

2022 Consumer Financial Services Year in Review & A Look Ahead

Consumer Financial
Services Practice

2022 Consumer Financial Services Year in Review & A Look Ahead

January 2023

Table of Contents

Executive Summary	3
About Us.....	4
Auto Finance	5
Background Screening	12
Bankruptcy.....	21
Consumer Class Actions	25
Consumer Credit Reporting	31
Cryptocurrency	42
Cybersecurity and Privacy.....	61
Debt Collection	83
Fair Lending	90
Fintech	100
Mortgage	110
Payment Processing and Cards	117
Small Dollar Lending	121
Student Lending	125
Telephone Consumer Protection Act.....	130
Tribal Lending	135
Uniform Commercial Code and Banking.....	138
Consumer Financial Services Law Monitor	143
Consumer Financial Services Podcasts	144
Contacts	145

The views and opinions expressed in these materials are solely those of the authors. While these materials are intended to provide accurate information regarding the subject matter covered, they are designed for educational and informative purposes only. Nothing contained herein is to be construed as the rendering of legal advice for specific cases, and readers are responsible for obtaining such advice from their own legal counsel. Use of these materials does not create an attorney-client relationship between the user and the authors.

EXECUTIVE SUMMARY

With active federal and state legislatures, consumer financial services providers faced a challenging 2022. Courts across the United States continued to issue rulings that will have both immediate and lasting impacts on the industry. Here at Troutman Pepper, we continued to help clients navigate large volumes of industry regulations, find successful resolutions, and stay ahead of the compliance curve. Being thoroughly entrenched in the consumer financial services industry enables us to produce the following collection of reports, with the hope that it will prove to be a helpful resource for you throughout the coming year.

In this compendium, we share developments on auto finance, background screening, bankruptcy, consumer class actions, consumer credit reporting, cryptocurrency, cybersecurity and privacy, debt

collection, fair lending, fintech, mortgage, payment processing and cards, small dollar lending, student lending, the Telephone Consumer Protection Act (TCPA), tribal lending, the Uniform Commercial Code (UCC), and banking. We hope you find the information in our report insightful and valuable for your business strategy, so you can focus less on the law and more on achieving your business goals.

We are honored that you continue to rely on us for the latest legal and regulatory developments in the industry. Please think of us as your trusted resource to help you understand and tackle today's challenges, while preparing you for what lies ahead.

I would appreciate your feedback on this year's publication. Please feel free to contact me at any time at michael.lacy@troutman.com with any questions, comments, or suggestions.

Michael Lacy
Practice Group Leader

ABOUT US

Troutman Pepper's Consumer Financial Services Practice Group consists of more than 120 attorneys and professionals nationwide, who bring extensive experience in litigation, regulatory enforcement, and compliance. Our trial attorneys have litigated thousands of individual and class action lawsuits involving cutting-edge issues across the country, and our regulatory and compliance attorneys have handled numerous 50-state investigations and nationwide compliance analyses.

Our multidisciplinary attorneys work together to bring a higher level of specialized knowledge, practical guidance, and valuable advice to our clients. This results-driven collaboration offers seamless legal services to resolve client issues effectively and efficiently. As such, we address the many perspectives that may arise in a single legal issue before it becomes a larger problem, or that may lead to compliance solutions and regulatory strategies developing out of contentious litigation.

Our nationwide reputation in consumer claims litigation derives from our attorneys' extensive experience representing clients in consumer class actions involving the pantheon of federal and state consumer protection statutes, including the following:

- Fair Credit Reporting Act (FCRA)
- Fair Debt Collection Practices Act (FDCPA)
- Telephone Consumer Protection Act (TCPA)
- Truth in Lending Act (TILA)
- Real Estate Settlement Procedures Act (RESPA)
- West Virginia Consumer Credit Protection Act (WVCCPA)
- Unfair and Deceptive Acts and Practices (UDAP)
- Unfair, Deceptive, or Abusive Acts or 2X Practices (UDAAP)
- Electronic Fund Transfer Act (EFTA)
- Electronic Signatures in Global and National Commerce Act (E-SIGN)
- Equal Credit Opportunity Act (ECOA) and state law equivalent statutes
- Fair and Accurate Credit Transactions Act (FACTA)

- Home Affordable Modification Program (HAMP)
- Home Owner's Equity Protection Act (HOEPA)
- Servicemembers Civil Relief Act (SCRA)
- Magnuson-Moss Warranty Act
- Federal and State Odometer Acts
- FTC Holder Rule
- Home warranties
- Mortgage foreclosures
- Mortgage lending and servicing
- Cybersecurity and privacy, and state law debt collection claims

Our regulatory enforcement team comes well prepared to respond to the Consumer Financial Protection Bureau's (CFPB) oversight inquiries, civil investigative demands (CIDs), audit, supervision, examination, and enforcement actions, including the request for production of privileged and highly confidential information routinely demanded by the CFPB to gauge compliance and procedures. Our enforcement team has spent years handling similar claims and CID, audit, supervision, examination, and enforcement proceedings. We also are well equipped to handle Federal Trade Commission (FTC) investigations concerning a variety of matters, including consumer privacy and data security breaches. At Troutman Pepper, we move seamlessly from negotiation to litigation, if and when requested, with a team of highly skilled litigators with extensive experience in regulatory enforcement litigation matters.

We regularly advise and prepare our clients proactively for compliance matters to avoid costly government audits, investigations, fines, litigation, or damage to brand and reputation. Our compliance attorneys have handled a variety of matters for our clients, including facilitating compliance audits (both on-site and off-site), performing due diligence reviews, drafting training and compliance manuals and policies, and conducting multistate analyses of state and federal laws.

Attorneys in each of our Consumer Financial Services team's core areas—litigation, regulatory enforcement, and compliance—work together to recommend creative approaches that efficiently address our clients' needs and achieve their goals.

AUTO FINANCE

Authors: Alan D. Wingfield, Chris J. Capurso, Brooke K. Conkle, Stephen J. Steinlight

Highlights From 2022

In 2022, the major stories for auto finance included new developments from regulatory agencies. The Federal Trade Commission (FTC) mirrored many of the initiatives of the Consumer Financial Protection Bureau (CFPB), targeting so-called “junk fees” and moving to require dealerships to include additional disclosures, both in advertisements and at the point of sale, regarding fees and add-on products. Fair lending and discrimination also remained high on regulators’ respective radars, with multiple enforcement actions seeking to curb what regulators viewed as unfair practices in auto lending. Finally, uncertainty reigned under the FTC’s Holder-in-Due-Course Rule (Holder Rule) where the FTC and California courts reversed the standard limits imposed by the rule, creating greater exposure for auto finance companies that would potentially be on the hook for attorney fee awards beyond consumers’ payments retail installment sales contracts.

FTC Keeps the Pressure on Dealers and Auto Finance Companies in the Motor Vehicle Dealers Trade Regulation Rule

In July 2022, the FTC announced a Notice of Proposed Rulemaking for the Motor Vehicle Dealers Trade Regulation Rule, which proposed a host of new requirements in advertising and selling motor vehicles. The rule shows the FTC working alongside the CFPB, targeting many of the same practices denounced by CFPB Director Rohit Chopra, including so-called “junk fees.”

The FTC rule will require significant changes to the ways that vehicles are advertised for sale, and it will require an “Offering Price” of each vehicle to be advertised that includes all dealer-required charges, excluding only those charges specifically required by the state or federal government. Add-on products are also a major target of the rule, and dealers must create a webpage and in-store signage, listing all add-on products offered, with a

range of prices the typical consumer can expect to pay and a disclosure formally stating that add-on products are not required for vehicle purchase.

The rule also will require significant changes to the ways that vehicles are sold. The rule requires multiple new forms in the sales process, including “Cash Price Offer” forms where consumers want to include add-on products in their vehicle purchase. The “Cash Price Offer” forms must provide a clear and conspicuous disclosure of the Cash Price of the vehicle, which the FTC defines as the Offering Price plus any government-mandated charges, but without any discounts, rebates, trade-ins, or add-ons, and the consumer must specifically *decline* to purchase the vehicle for that price. Notably, the rule would require both the consumer’s signature and a store manager’s signature, with the date and time also recorded.

Where consumers want to include add-on products in their vehicle purchase, the rule also would require the consumer to sign an Add-on Itemization form, which discloses the Cash Price of the vehicle, the charges for any optional add-ons separately itemized, and the sum of all charges. The form cannot include any preprinted check boxes. Finally, the rule prohibits the sale of “no benefit” add-on products defined by the FTC to include GAP products where a consumer would likely “price out” of the product with a low loan-to-value ratio and GAP products where a consumer would be subject to certain exclusions, such as a geographic exclusion from coverage or a vehicle-specific exclusion from coverage.

For auto finance companies, the rule could create additional exposure. Consumers may have additional defenses to retail installment sales contracts if the contracts are not executed under the requirements of the rule. And, combined with the ambiguity surrounding the Holder Rule, auto finance companies could wind up with significantly more exposure if their dealer partners have not abided by the myriad new obligations set forth by the FTC.



The comment deadline for the rule expired on September 12, 2022, after the FTC refused to extend the deadline, much to the chagrin of the industry.

CFPB and DOJ Remind Auto Finance Companies of SCRA Protections for Servicemembers

On July 29, 2022, the CFPB and the Department of Justice (DOJ) issued a joint letter¹ to auto finance companies, reminding them of the protections afforded by the Servicemembers Civil Relief Act (SCRA) to servicemembers and their dependents during periods of military service. These protections include several related to auto lending and leasing, which are particularly important given that recent CFPB research has shown that servicemembers tend to carry more auto loan debt at younger ages than their civilian counterparts, largely due to the need for transportation while living on a military base. The DOJ enforces the SCRA, which covers debts incurred before active duty, while the CFPB is authorized to address unfair, deceptive, or abusive practices related to auto financing for all members of the public, including servicemembers, under the Consumer Financial Protection Act. The agencies encouraged auto finance companies to review applicable SCRA provisions and ensure compliance,

including provisions related to vehicle repossession protections, early vehicle lease terminations, and auto loan interest rate caps. In December 2022, the CFPB kept up its SCRA focus by issuing a report claiming that only one in 10 servicemembers entitled to receive interest rate restrictions or auto financings under the SCRA actually receive the benefit.

FTC Seeks Public Comment on So-Called “Junk Fees”

On October 20, 2022, the FTC issued an Advance Notice of Proposed Rulemaking,² seeking public comment on the harms stemming from what it characterizes as “junk fees,” i.e., fees that are allegedly unnecessary, unavoidable, or unexpected and that inflate costs, while adding little value. The term also encompasses “hidden fees,” which are fees for goods or services that are deceptive or unfair, including fees only disclosed at the latter stage in the consumer’s purchasing process or not at all. While the FTC has been active in bringing enforcement actions against alleged “junk fees,” it generally lacks the authority to seek penalties against first-time violators or lacks the ability to obtain financial compensation for consumers in instances in which “junk fees” violate the FTC’s

¹ See <https://www.justice.gov/opa/press-release/file/1522946/download>.

² See https://www.ftc.gov/system/files/ftc_gov/pdf/R207011UnfairDeceptiveFeesANPR.pdf.

prohibition on unfair or deceptive practices. This new rule would change that.

Examples of fees that the FTC is questioning include “mobile cramming” charges, connection and maintenance fees on prepaid phone cards, account fees, fees that diminish the amount a borrower receives from a loan, miscellaneous fees levied on fuel cards, auto dealer fees, undisclosed fees for funeral services, hotel “resort” fees, hidden fees for academic publishing, poorly disclosed ancillary insurance products, and membership programs.

According to the FTC, it is considering regulating fees that fall into the following categories:

- Unnecessary charges for worthless, free, or fake products or services
- Unavoidable charges imposed on captive consumers and
- Surprise charges that secretly push up the purchase price

The FTC seeks comment on, among other things, the prevalence of each of the above practices and the costs and benefits of a rule that would require upfront inclusion of any mandatory fees whenever consumers are quoted a price for a good or service.

FTC Takes Action Against Dealership for Discrimination and So-Called “Junk Fees,” Highlighting Dual Aims of the FTC and the CFPB While Expanding the FTC Act’s Reach

The FTC announced a major settlement in October 2022 that simultaneously showed the agency working side by side with the CFPB to address allegations of discrimination and the assessment of purported “junk fees,” while also expanding the FTC Act to cover claims it previously never addressed. The FTC reached a \$3.38 million settlement with Passport Automotive Group (Passport) and two of its officers to resolve allegations that the automotive group violated the Equal Credit Opportunity Act (ECOA) and the FTC Act by adding “junk fees” onto the cost of its vehicles and discriminating against Black and Latino consumers by charging

them higher financing costs and fees than non-Latino white consumers. In addition to the fine, the proposed settlement order includes a remediation plan, changing how Passport, which operates nine car dealerships in the Washington, D.C. metropolitan area, will operate going forward. Specifically, those provisions include: (1) a broad prohibition on misrepresenting the costs or terms to buy, lease, or finance a car; (2) a requirement that the dealerships get consumers’ express, informed consent before charging them any fees; (3) a prohibition on dealerships charging different groups different markups; and (4) a requirement that all employees involved in the extension, renewal, or continuation of credit receive fair lending training.

The FTC complaint included allegations that:

- In numerous instances, when consumers attempted to purchase particular vehicles for the prices advertised, Passport charged them hundreds to thousands of additional dollars in fees
- Passport’s discretionary markup rate practice resulted in Passport charging, on average, Black and Latino consumers higher markups. These disparities were statistically significant. Passport charged Black consumers, on average, approximately 28 basis points (approximately \$291) and Latino consumers, on average, approximately 26 basis points (approximately \$235) more in finance charges than non-Latino white consumers. Black consumers received the maximum Passport-allowed markup approximately 47% more often and Latino consumers approximately 38% more often than non-Latino white consumers did and
- In addition to charging minority consumers higher interest rate markups, Passport charged Black and Latino consumers extra inspection, reconditioning, vehicle preparation, and certification fees more frequently and in higher amounts than similarly situated non-Latino white consumers. The FTC alleged that Black consumers paid, on average, approximately \$82 more and Latino consumers approximately \$81 more in fees

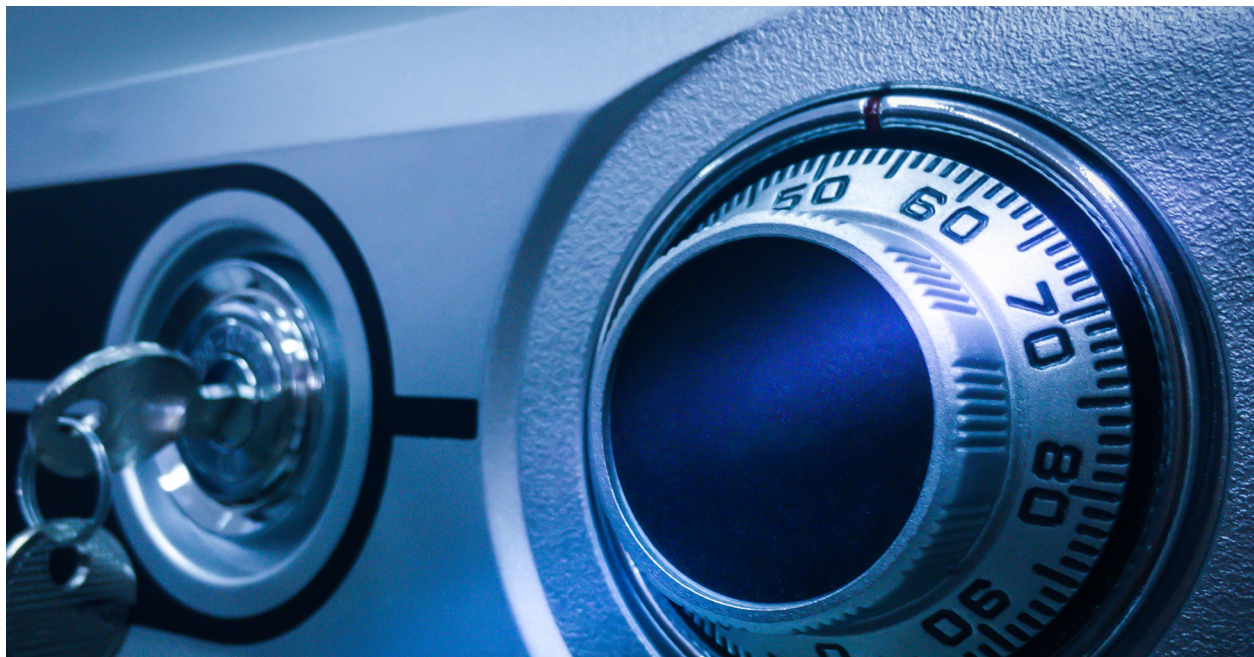
Notably, the complaint included a claim under the FTC Act for discrimination, covering ground that arguably was covered by the similar the ECOA claims in the complaint. Then-Commissioner Noah Phillips dissented from the enforcement action, citing the “novel interpretation of unfairness” espoused in the complaint by including a discrimination claim under the FTC Act. According to Commissioner Phillips, the FTC Act does not include antidiscrimination provisions, and furthermore, the agency had not shown a disparate treatment to support the claim. The FTC Act “is versatile, but it is not a Swiss Army knife,” Commissioner Phillips, who stepped down from the FTC on the day the complaint was released, wrote in dissent.

New Ambiguities Under the Holder Rule

One of the biggest stories from 2022 was the sudden ambiguity in the FTC’s stance on the Holder Rule. The Holder Rule permits consumers to bring any legal claims against the “holder” of a credit contract that the consumer could assert against the original seller of the good or service, even if the claim springs from the seller’s misconduct alone. The Holder Rule, however, states that a plaintiff’s “recovery hereunder” from the holder “shall not exceed amounts paid by the debtor” under the sales contract.

In 2019, under the Trump administration, the FTC issued a confirmation of the Holder Rule that appeared to expressly reject limitless attorney fee awards against holders. Yet, early 2022 saw the federal agency, under the Biden administration, reverse this long-held understanding by issuing an advisory opinion, suggesting that an automatic cap on attorney fees and costs is not proper.

California courts in particular have struggled with whether the Holder Rule’s recovery cap applies to a plaintiff’s recovery of attorneys’ fees and costs over and above the amount paid under the contract. In a 2018 decision, a California court of appeals held that the word “recovery” as used in the Holder Rule includes attorneys’ fees and, therefore, the cap prevents courts from awarding attorneys’ fees against the holder defendant over and above the amount paid on the contract. In response, the California Legislature passed California Civil Code Section 1459.5, a fee-shifting statute that purports to allow attorneys’ fees against the holder. In 2020, another California court of appeals held that the Holder Rule’s recovery cap applied to attorneys’ fees and, citing the 2019 rule confirmation, that the Holder Rule preempted Section 1459.5.



California's Second District Court of Appeals, however, issued recent decisions retreating from its previous position, including *Pulliam v. HNL Automotive, Inc.*, 60 Cal. App. 5th 396 (2021). *Pulliam* held that the term "recovery" as used in the Holder Rule does not include attorneys' fees, the FTC's 2019 rule confirmation is not entitled to deference, and attorneys' fees above and beyond the amount paid under the sales contract are therefore recoverable by a plaintiff from the holder defendant. Also, in early 2022, California's Fifth District Court of Appeals allowed recovery of attorneys' fees, ruling that while attorneys' fees are part of "recovery" and are generally precluded by the Holder Rule, the Holder Rule did not preempt an attorneys' fee award under Section 1459.5. *Reyes v. Beneficial State Bank*, 2022 Cal. App. LEXIS 233 (Cal. Ct. App. Mar. 22, 2022).

Deviating from the logic of the lower courts' prior decisions, the California Supreme Court charted its own course in its review of the *Pulliam* decision, allowing unlimited attorney fee awards under the Song-Beverly Act. *Pulliam v. HNL Automotive, Inc.*, 13 Cal. App. 5th 127 (2022). The court began by ruling that the phrase "recovery hereunder by the debtor" as used in the Holder Rule was ambiguous because it could refer only to money the debtor keeps (like damages) or also to money the debtor receives and passes along to its counsel (like attorneys' fees). Looking to extrinsic sources, the court noted that the FTC did not mention attorneys' fees until its 2019 rule confirmation, indicating that it was only intended to apply to limit damages awards. From there, the court noted that California law, including the Song-Beverly Act, does not consider attorneys' fees to be an element of damages, treating them as "costs" instead. The court concluded that the FTC, aware of these state laws at the time it created the Holder Rule, did not intend to preempt state laws allowing attorneys' fee awards.

The court also addressed the purpose of the Holder Rule, framing it as a consumer protection rule designed primarily to shift costs away from consumers. It reasoned that the FTC was concerned about consumers' ability to afford litigation, as well as consumers' ability to recover from sellers, but nonetheless expected that consumers would be able to afford to bring "affirmative claims." In the

court's view, the Holder Rule acted as a "national floor," but did not "restrict the application of state laws authorizing additional awards of damages or attorney's fees against a seller or holder."

Finally, the court ruled that regardless of whether deference to the FTC's most recent interpretive guidance is warranted, the FTC's interpretation is consistent with its own. The court stated that claims for attorneys' fees by a prevailing party under Section 1794 are distinct from claims against a seller that are extended to a creditor solely by the Holder Rule because Section 1794 applies to all defendants, not just to sellers. Notably, the court did not provide any analysis of the more recent Section 1459.5, although its brief references were generally favorable, relying instead on Section 1794 to authorize unlimited attorneys' fee awards.

The California Supreme Court's *Pulliam* decision, however, may not be the final word on this issue. The defendant in *Pulliam* has filed a petition for a writ of certiorari to the U.S. Supreme Court, highlighting the state split created by the *Pulliam* opinion and noting that the decision ignores or misunderstands the text, purpose, and history of the Holder Rule. Given the current Supreme Court's disfavor for agency deference, the *Pulliam* decision may be reviewed by the highest court in the land.

Enforcement Actions Continue Apace, Targeting Fair Lending Initiatives

Federal and state agencies remained active in enforcement actions, highlighting many of the initiatives set forth by the CFPB, with emphasis on fair lending, discrimination, and fees.

On February 24, 2022, the CFPB released a blog post, outlining multiple auto lending topics in the wake of rising vehicle prices. It identified three primary ways the CFPB seeks to ensure a fair, transparent, and competitive auto lending market in the wake of the significant price changes: ensuring affordable credit for auto loans; monitoring practices in auto loan servicing and collections; and fostering competition among subprime lenders.

Just a few days later, the CFPB issued a bulletin and accompanying press release, highlighting one of its increased priorities in auto finance, particularly,

inadvertent repossessions. These inadvertent repossessions are those that occur in error—when a consumer has made a payment or promise sufficient to avoid the repossession, but it occurs nonetheless. The CFPB noted that these errors can occur by a lender applying a payment to the wrong account; failure to process an extension/deferment; failure to cancel a repossession order (or all orders, if the account is placed with more than one repossession vendor); or vendor failures (i.e., the recovery of the vehicle by a vendor, even though the order had been put on hold or canceled by the lender). In its bulletin, the CFPB provided a list of recommended compliance steps to avoid inadvertent possession. These steps include typical measures like policies, procedures, review of customer communications and payment application processes, monitoring of repossessions and complaints, logging and root cause analysis of inadvertent repossessions, and vendor monitoring of repossession agents.

In July 2022, the CFPB ordered Hyundai Capital America (Hyundai) to pay \$19.2 million for allegedly providing inaccurate information to consumer reporting agencies in violation of the Fair Credit Reporting Act (FCRA). The CFPB stated that Hyundai violated the FCRA by failing to report complete and accurate loan and lease information, including but not limited to failing to have reasonable identity theft and related blocking procedures and continuing to report such information that should have been blocked on a consumer's report.

On October 6, 2022, the New York State Department of Financial Services (NYDFS) announced a consent order³ with a bank to resolve allegations that, in violation of New York Executive Law Section 296-a, the bank instituted discretionary dealer markup policies that resulted in a disparate impact negatively affecting members of minority groups.

As part of the bank's indirect automobile lending operations, the bank sets a specified risk-based interest rate (buy rate) for approved applications. However, the bank has a policy that allows automobile dealers to mark up prospective

borrowers' interest rates above the buy rate. According to NYDFS, its investigation revealed that between 2017 and 2020, Black or African American and Hispanic consumers were charged over 30 basis points more in discretionary dealer markups than non-Hispanic white borrowers. Further, between 2018 and 2020, Asian borrowers were charged approximately 15 basis points more in discretionary dealer markups than non-Hispanic white borrowers. Although the NYDFS did not find evidence of any intentional discrimination, it found the bank's policies and practices allowed automobile dealers to mark up a consumer's interest rate above the established buy rate, which resulted in a disparate impact.

In addition to a \$950,000 fine and mandatory restitution to impacted borrowers, the consent order includes remediation, requiring the bank to develop a compliance plan providing for updates to its automobile lending policy to limit dealer markups on retail installment contracts purchased by the bank. This consent order is a continuation of the pattern of dealer reserve actions by the NYDFS, similar to two previous consent orders entered into in July 2021, both with smaller New York-chartered banks. All of these consent orders followed a 2018 announcement by the NYDFS that it planned to take actions against indirect auto finance companies relating to dealer reserve, similar to those taken by the CFPB starting in 2013.

Federal and state agencies remained active in enforcement actions, highlighting many of the initiatives set forth by the CFPB, with emphasis on fair lending, discrimination, and fees.

³ See https://www.dfs.ny.gov/system/files/documents/2022/10/ea20221005_co_rhinebeck.pdf.



Outlook for 2023

We will look for the FTC to continue its partnership with the CFPB to address many of the initiatives championed by CFPB Commissioner Chopra. Look for enforcement actions, targeting dealerships that engage in discriminatory practices or that engage in bait-and-switch tactics, with a special emphasis on

add-on products. Should the Motor Vehicle Dealers Trade Regulation Rule be passed, and we anticipate that it will, industry stakeholders likely will have very little time to get their compliance strategies up to speed. Auto finance companies may want to consider additional vetting for its dealer partners to ensure that they have the capabilities to meet the new prerequisites of the rule.

BACKGROUND SCREENING

Authors: Cindy D. Hanson, Jack F. Altura, Elizabeth Andrews, Noah J. DiPasquale, Jessica Lohr

Introduction

Following a trend from previous years, the last year included a significant number of initiated actions and court decisions involving violations of the Fair Credit Reporting Act (FCRA) and state law equivalents, including substantial developments in the area of background screening. In a standing decision, the Eighth Circuit held a consumer lacked Article III standing after failing to receive a required adverse action notice concerning an employment application where she did not dispute any of the negative information in her report. Further, a California district court judge interpreted the California Investigative Consumer Reporting Agencies Act's (ICRAA) statutory damages scheme, holding that the statute allows for only one statutory penalty per background report, not per alleged violation. The background screening industry continues to face uncertainty in California due to an appellate court opinion making online searches for criminal records slow, difficult, or impossible, which was followed by a gubernatorial veto of a proposed legislative solution. Also, on a state and local level, the recent trend has continued in the enactment of new "fair chance" laws and ordinances to prevent the use of criminal screening for employees and housing applicants.

FCRA Does Not Create a Right to Explain Negative but Undisputed Background Information to Employer Prior to Adverse Action, Says Eighth Circuit

In a unanimous decision issued in May 2022, a three-judge panel of the Eighth Circuit Court of Appeals held a plaintiff lacked standing for a claim her employer violated the FCRA by not providing her a copy of her consumer report before taking adverse action. Although Section 1681b(b)(3)(A) of the FCRA does require employers to provide a copy of a consumer report before taking adverse action based on negative information in that report, the plaintiff suffered no injury because she did not dispute any of the negative information contained

in her report. Instead, she asserted she was injured because the employer's failure to provide her with a copy of the report prevented her from explaining or contextualizing the negative information directly to her employer. The Eighth Circuit, however, held the FCRA does not create a right to simply explain negative but undisputed consumer report information to an employer before an adverse action, and thus, the plaintiff was not injured by being deprived of the opportunity to do so.

Plaintiff Ria Schumacher was arrested in the late 1990s at the age of 17 when she was implicated in a murder case involving a drug deal gone bad. She was ultimately tried as an adult, convicted of murder and armed robbery, sentenced to 25 years in prison, and served 12 years before being released. In 2015, Schumacher applied for employment with defendant SC Data Center, Inc. In response to a question on the application about whether she had ever been convicted of a felony, she answered "no," but included a handwritten explanation: "was once arrested in 1996 at age 17 and then found Not guilty." SC Data offered her a position but required her to consent to a criminal background check by Sterling Infosystems, which she did. When the background check revealed her 1996 felony convictions, SC Data rescinded its offer of employment due to the undisclosed convictions. SC Data did not provide a copy of the report and statement of her rights under the FCRA, however, until two weeks after the offer was rescinded and a week after her original start date had passed.

The plaintiff filed suit on behalf of a putative class, claiming SC Data violated the FCRA by not providing her a copy of her report prior to the adverse action (as well as claims SC Data's background check disclosure form was not in compliance with the FCRA, and the background check exceeded the scope of her authorization). The parties reached a tentative class settlement in May 2016, but after the U.S. Supreme Court issued its opinion in *Spokeo, Inc. v. Robins*, 578 U.S. 330

(2016), SC Data moved to dismiss the case for lack of Article III standing. The district court ultimately found Schumacher had standing for all three claims, and SC Data appealed to the Eighth Circuit.

In concluding Schumacher did not have standing for her adverse action claim, the Eighth Circuit noted Schumacher had never disputed the accuracy of the background check information, but only asserted she was deprived of a right to explain that information to SC Data by its failure to provide her a copy of her report before the adverse action. The court noted other courts, including the Third Circuit and the Seventh Circuit, have held that taking an adverse employment action without first providing the consumer report to the employee is a sufficiently concrete harm to confer standing. By contrast, the court noted the Ninth Circuit has concluded that no standing exists when a plaintiff fails to show the failure to provide the consumer report caused actual harm or a material risk of harm.

Analyzing the issue further, the court noted the only injury that could be asserted by Schumacher would be premised on “a prospective employee’s right to discuss with an employer the information in the consumer report prior to the employer taking an adverse action.” The court concluded neither the text of the FCRA nor its legislative history supported the existence of any such right. Instead, the court found the right protected by the relevant provisions of the FCRA was the right to dispute information in the consumer report. Because Schumacher never claimed the background check information was inaccurate or she would have disputed the information had she received a copy of the consumer report, the court found she had no standing.

The court further disposed of Schumacher’s improper disclosure and scope of authorization claims as well. With regard to the alleged improper disclosure, Schumacher failed to allege any harm caused by the allegedly improper disclosure form, and thus lacked standing for that claim. Regarding the scope of authorization claim, the court held the background check was properly conducted within

the scope of her authorization and that she also lacked standing because she failed to allege a specific harm beyond a general invasion of privacy.

The *Schumacher v. SC Data Center, Inc.*, 33 F.4th 504 (8th Cir. 2022) decision has significant implications for employers conducting background screening checks of employees and potential employees. While employers are clearly required under the FCRA to provide a copy of the consumer report to the consumer prior to taking an adverse action based on the report, this decision confirms that applicants and employees do not have a right under the FCRA to simply explain or contextualize negative but accurate information contained in their consumer report. More broadly, this decision adds to the growing body of case law defining Article III standing under the FCRA and other consumer protection statutes, particularly for alleged informational injuries.

While employers are clearly required under the FCRA to provide a copy of the consumer report to the consumer prior to taking an adverse action based on the report, this decision confirms that applicants and employees do not have a right under the FCRA to simply explain or contextualize negative but accurate information contained in their consumer report.

Federal Court Holds ICRAA Statutory Damages Limited to One Penalty Per Background Report

In January 2022, a federal judge granted plaintiff Maria Garcia's (Garcia) motion to remand on the basis that the amount in controversy was below the required threshold. The order was based on the court's interpretation of the California Investigative Consumer Reporting Agencies Act's (ICRAA) statutory damages scheme and its finding that the statute allows for one statutory penalty per background report, not per violation.

In the case, Garcia alleged ICRAA violations against Quest Group Consulting LLC, Quest Group Search LLC, Douglas Shaener, and Jason Hanges (defendants). Garcia also asserted claims under the California Private Attorneys General Act (PAGA) for alleged violations of the California Labor Code. Garcia alleged she was hired by the defendants as a youth care worker to supervise unaccompanied migrant children temporarily housed in California. Garcia alleged during her employment, the defendants violated various sections of the California Labor Code and procured an investigative consumer report after requiring her to sign a deficient disclosure form.

The defendants originally removed the case to federal court based on diversity jurisdiction, which requires an amount in controversy of \$75,000. The parties agreed Garcia's PAGA claims only totaled

\$2,125. However, the parties disagreed on the potential monetary liability for the ICRAA claim, which formed the basis of the motion to remand.

The ICRAA damages provision provides that a user who fails to comply with ICRAA is liable for any damages sustained by the consumer as a result of the failure or, except in the case of class actions, \$10,000, whichever sum is greater. Cal. Civ. Code § 1786.50(a).

The defendants argued the amount in controversy was \$120,000 because Garcia alleged multiple separate statutory violations of the ICRAA against two of the defendants. On the other hand, Garcia argued the amount in controversy for the ICRAA claim was only \$20,000 (or \$10,000 per defendant) because, although she alleged multiple technical ICRAA violations, there was only one potential statutory penalty per background report. The court agreed with Garcia's interpretation, focusing on the plain language of Section 1786.50(a), which provides that a defendant that fails to comply with "any requirement ... with respect to an investigative consumer report" is liable to the consumer for actual damages, or \$10,000, whichever sum is greater. Therefore, the court held, at most, the plaintiff would be entitled to one \$10,000 ICRAA penalty per background report.



Although remanded, the decision can be used as a helpful tool for defendants to argue that statutory damages should be limited in ICRAA cases. This is especially true given the lack of case law discussing how ICRAA's statutory damages scheme should be interpreted, and given that in practice, the plaintiff's bar often takes the position that statutory damages should be recoverable for each distinct technical violation of the ICRAA.

Background Screening in California Affected by Court of Appeal Decision in *All of Us or None v. Hamrick* and Subsequent Defeat of Senate Bill 1262

The background screening industry has experienced considerable turmoil in California over the last year and a half. First, in the summer of 2021, an intermediate appellate court in San Diego interpreted a long-standing California Rule of Court in a novel manner that made online searches for criminal records slow, difficult, or impossible. Background screening came to a virtual halt across the state. Efforts by various companies and industry groups to persuade the California Supreme Court to remedy the situation ultimately proved unsuccessful. Finally, after vigorous lobbying, a legislative solution seemed within grasp. However, after sailing through both houses of the California Legislature, a key bill fell to a surprise, late-night gubernatorial veto in autumn 2022. As of this writing, employers, landlords, and other customers of the background screening industry continue to face long delays and uncertain outcomes as they try to conduct routine criminal background checks on individuals seeking to be placed in places of trust.

All of Us or None v. Hamrick

In May 2021, the California Court of Appeal, Fourth District, Division One, sitting in San Diego, dealt the background screening industry in California a significant blow in *All of Us or None – Riverside Chapter v. Hamrick*, 64 Cal. App. 5th 751, 279 Cal. Rptr. 3d 422 (2021). In a 67-page

unanimous opinion authored by Associate Justice Cynthia Aaron, *Hamrick* embraced a heretofore novel interpretation of California Rule of Court 2.507. That relatively obscure rule, which has been in effect for many years, provides that certain items of personally identifiable information (PII), such as Social Security numbers, dates of birth, and driver's license numbers, "must be excluded from a court's electronic calendar, index, and register of actions." Cal. Rule of Court 2.507(c). For the first time, *Hamrick* construed Subsection (c) not only to prevent accidental encounters with the PII of criminal defendants in the normal course of court business (as the rule had generally been applied in the past), but also to prohibit members of the public from using these items of PII as *search filters* when conducting online searches on superior court websites using first and last names.

This decision had—and continues to have — outsized implications for the background screening industry. When reviewing online records to determine if the subject of a search has any criminal convictions or other relevant criminal history, researchers routinely use PII (usually dates of birth or driver's license numbers) to narrow their search results. Before *Hamrick*, a researcher could easily determine whether an online criminal record was relevant to that individual by filtering voluminous search results using (for example) the date of birth the subject provided with his/her consent to the background screening process. After *Hamrick*, superior courts across California began removing date of birth, driver's license numbers, etc. as available search filters on their websites, leaving the public to conduct online searches for criminal records using first and last names only (and sometimes, not even that).

Data collected by the Professional Background Screening Association (PBSA) shows that as of 2020, 94% of American employers conduct one or more types of employment background screening, and 73% of employers have a documented screening policy.¹ Yet given the huge size of many counties in California—Los Angeles County alone

¹ Professional Background Screening Association, Background Screening: Trends and Uses in Today's Global Economy (2020), available at <https://pubs.thepbsa.org/pub.cfm?id=459B8AB7-OCEA-625E-0911-A4A089DE5118>.



has nearly 10 million residents—it can be virtually impossible to meaningfully search online criminal court records for an individual when the only two data points are first name and last name.

The California Supreme Court Declines to Get Involved

The interest groups funding the impact litigation that resulted in *Hamrick* were careful to sue only court officials in their official capacity, thereby affording no seat at the table for the background screening industry and its entire customer base—including nearly all employers in California and beyond. This tactic left few options for the business sector to challenge *Hamrick* in the California Supreme Court since the court typically only entertains petitions for review from parties to the action below.

Nonetheless, a coalition of companies and industry groups represented by Troutman Pepper including the California Chamber of Commerce, the California Hospital Association, the California Hotel & Lodging Association, and numerous prominent companies in the gig economy, launched an effort to persuade

the California Supreme Court to take up *Hamrick* and overturn it. Seeking to proceed in an amicus curiae capacity, the coalition filed a letter in July 2021, urging the court to grant review. In September 2022, however, the court declined.

Although the California Court of Appeal is divided into six districts based on geography, and these districts are not horizontally bound to agree with one another, the Court of Appeal is technically a single unitary court. As a result, although *Hamrick* issued from the appellate court sitting in San Diego, the state supreme court’s decision not to take it up caused it to become binding law throughout the entire state of California. Unless a sister appellate district elects to part ways from *Hamrick*, or the state Supreme Court overrules it, trial courts in all 58 counties were (and remain) bound to follow *Hamrick*’s prohibition on the use of search fields, such as date of birth, on their public websites.

Together, these trial courts have jurisdiction over 40 million Californians—and that number does not include former California residents who list the state in their residential history on job applications nationwide and even globally.

In a Surprise Last-Minute Move, Governor Newsom Vetoes a Promising Legislative Fix

Seeking a solution, the background screening industry and its customers turned to the California Legislature.² With their support and lobbying efforts, California State Senator Steven Bradford of Senate District 35 in Los Angeles County introduced Senate Bill (SB) 1262 in February 2022. In SB 1262, Senator Bradford, who chairs the Senate Committee on Public Safety, proposed a short amendment to California Government Code Section 69842, providing: “Publicly accessible electronic indexes of defendants in criminal cases shall permit searches and filtering of results based on a defendant’s driver’s license number or date of birth, or both.” This new language would have ensured that researchers conducting background checks on individuals—who had consented to the check and voluntarily provided their driver’s license number or date of birth—could use those two items of PII to confirm if a search hit on the subject’s name lined up with those identifiers.

In the wake of this unexpected and unwelcome development, the background screening industry and its customers must once again regroup to determine the best way to conduct business in a post-Hamrick world, while also seeking solutions through every avenue possible to mitigate or reverse the real-world effects of the decision.

The bill proved popular in both houses of the Legislature, passing by a unanimous Senate vote of 37-0 and then a vote of 53-9 in the Assembly. However, in a surprise late-night move in September 2022, Governor Newsom vetoed the bill. His office issued a veto message stating: “This bill would change superior court rules to allow publicly accessible electronic court criminal indexes to be searched with a subject’s driver’s license number or date of birth. This bill would override a 2021 appellate court decision and current court rules that strike a fair balance between public access to court records, public safety, and an individual’s constitutional right to privacy. While this bill may provide for a more convenient process for companies conducting commercial background checks, it would also allow any member of the public to easily access individuals’ sensitive personal information online.”

In the wake of this unexpected and unwelcome development, the background screening industry and its customers must once again regroup to determine the best way to conduct business in a post-*Hamrick* world, while also seeking solutions through every avenue possible to mitigate or reverse the real-world effects of the decision. Troutman Pepper has been heavily involved with industry group efforts to address the problems that *Hamrick* created and will continue to track the situation closely.

Update on New State and Local Laws Requiring or Restricting Background Screening

The use of background screening for employment and housing applicants is a controversial issue that has generated significant debate in recent years. While some advocacy groups and policymakers have sought to impose various limits on the preparation and use of background screening reports, including through promotion of “fair chance” laws and ordinances to prevent the use of criminal screening for employees and housing applicants, others have recognized the important public safety and economic interests served by the background screening industry.

² Efforts by industry groups and associations to intervene in related litigation, including rule change requests to the California Judicial Council, proved unsuccessful.

In 2021, multiple states and localities enacted laws favoring both sides of the debate, with some jurisdictions affirmatively requiring more robust background screening in certain industries, while other jurisdictions have sought to limit it. Troutman Pepper has compiled the following update on some of the laws affecting background screening.

New York City Law Restricts Use of Automated Employment Screening Tools

In February 2022, New York City passed its Automated Employment Decision Tools law, which prohibits employers and employment agencies in New York City from using an “automated employment decision tool” (AEDT) to screen applicants or employees unless the tool first passes an independent bias audit to assess the disparate impact the tool may have on protected classes, and the employer or agency provides specified notices to the applicant or employee. The law defines an AEDT as a tool that uses machine-learning, statistical monitoring, data analytics, or artificial intelligence to issue a score, classification, or recommendation used to either substantially assist or replace discretionary decision-making in hiring decisions. The law will go into effect on January 1, 2023.

The law specifically requires employers and employment agencies to provide notice to job applicants and employees who reside in New York City and who will be subject to the AEDT that: (1) an AEDT is being used as part of the evaluation, and the candidate or employee may request an alternative selection process; and (2) the AEDT will reference a specified list of job qualifications or characteristics at least 10 business days before use of the AEDT. It further requires that the employer provide information about the types of data collected, the source of the data, and the data retention policy to an applicant or employee within 30 days of a written request or make this information available on its website.

The Department of Consumer and Worker Protection (DCWP) issued new proposed regulations to effectuate the AEDT law.

Arizona Background Screening Law for Nursing Care Workers

In March 2022, Arizona Governor Doug Ducey signed into law a bill that bolsters the background screening requirements for licensure of nursing care workers through the Arizona Board of Nursing Care Institution Administrators and Assisted Living



Facility Managers (NCIA). In a press release, Governor Ducey stated: Arizona’s “nursing homes and assisted living facilities deserve accountability and leadership from their supervisors. ... [The new law] accomplishes this. Our seniors—grandmothers, grandfathers and family members—deserve nothing less to ensure their safety, happiness and health.”

The new law amends an existing law requiring background checks as a condition for licensure for most employees and owners of residential care institutions, nursing care institutions, and home health agencies. The existing law also applies to contractors or volunteers providing medical services, nursing services, behavioral health services, health-related services, home health services, or supportive services through those institutions.

The amended law imposes additional background screening procedures, including requiring applicants for licensure to submit a full set of fingerprints for a state and federal criminal check, which will go into effect beginning January 1, 2023. It also prohibits from licensure any individuals with a felony conviction for any of 46 specific offenses involving violence or financial fraud, including homicide, sexual assault, sexual abuse, child abuse, neglect of a vulnerable adult, theft, forgery, welfare fraud, kidnapping, and others.

Florida Background Screening Law for Apartment Complex Employees

In July 2022, Florida Governor Ron DeSantis signed into law an act known as “Miya’s Law,” intended to strengthen residential tenant safety by, among other things, requiring background checks for employees of apartment complexes. The law’s namesake was Miya Marcano, a young woman who was tragically killed in her own apartment in 2021 by a maintenance worker who entered her unit with a master key maintained by the complex. The law passed unanimously in the Florida House and Senate.

Governor DeSantis stated in a press release: “Every tenant deserves to be safe in their home. By signing this legislation, we are making it safer to live in a rental unit and giving renters more peace of mind in their homes. ... I am proud to act on [Miya Marcano’s family’s] behalf to help prevent a tragedy like that from happening to another Florida tenant.” Florida State Representative Robin Bartleman, the Florida House sponsor for the bill, referred to it as “potentially lifesaving legislation” and stated it “will bring a greater sense of security for Florida’s 2 million renters.”

The law requires employees of an apartment building to undergo, as a condition of employment, a background check that includes criminal history and sex offender registration screening for all 50 states and the District of Columbia. The law further allows landlords to deny employment to any individual who has been convicted of, pled guilty to, or pled *nolo contendere* to: (1) any felony or first-degree misdemeanor offense involving disregard for the safety of others, or (2) a criminal offense involving violence, including murder, sexual battery, robbery, carjacking, home invasion-robbery, and stalking.

Policymakers in other states and industries should carefully consider the benefits of screening in general and the potential risks of limiting or de-incentivizing background screening.

In addition to mandating background screening, the law also requires apartment complexes to implement procedures for controlling the issuance and use of master keys and requires the landlord to provide a tenant with notice of any entry to their unit for maintenance or repairs 24 hours in advance of the entry, instead of the previously required 12-hour notice.

Conclusion

Although it does not prohibit background screening, New York City's AEDT law will place significant restrictions upon the use of automated screening products for employment decisions. Those restrictions will certainly increase the cost of compliance for employers and background screeners, and thus may have the indirect result of reducing the use of background screening in employment.

By contrast, both the Arizona nursing care licensing law and Florida's Miya's Law bolster background

screening in their respective states and industries of focus, motivated by a desire to promote public safety and accountability. The lawmakers and advocates for these laws recognized certain specific dangers that background screening can help prevent and took action to promote the use of screening in those particular contexts. More broadly, however, these laws highlight only a small fraction of the societal benefits derived from background screening and respond to only a few specific examples of dangers to public order or hindrances to business that can often be prevented by screening. Policymakers in other states and industries should carefully consider the benefits of screening in general and the potential risks of limiting or de-incentivizing background screening.

Employers and background screeners operating in each of these jurisdictions and within the industries affected by these laws should also take careful note of the new laws' requirements and review their hiring and screening policies to ensure compliance.



BANKRUPTCY

Authors: Andrew B. Buxbaum, Jared D. Bissell, Joseph M. DeFazio, Peter B. Yould

Taggart Standard Applies Beyond Bankruptcy Discharge Injunction Violations

Recently, the Fourth Circuit expanded the reach of *Taggart v. Lorenzen*, 139 S. Ct. 1795 (2019), beyond the Supreme Court's standard for the imposition of contempt sanctions due to a bankruptcy discharge violation. See *Beckhart v. Newrez LLC*, 31 F.4th 274 (4th Cir. 2022).

In *Beckhart*, the Fourth Circuit ruled that “*Taggart* also applies when a court is considering whether to hold a creditor in civil contempt for violating a plan of reorganization of debts entered under Chapter 11.” It further offered that “[n]othing about the Supreme Court’s analysis in *Taggart* suggests it is limited to violations of Chapter 7 discharge orders ... or that the Court’s decision turned on considerations unique to the Chapter 7 context.”

This decision follows the Second Circuit’s ruling in *PHH Mortgage Corp. v. Sensenich (In re Gravel)*, 6 F.4th 503 (2d Cir. 2021), *reh’g en banc denied*, No. 20-1 (2d Cir. Nov. 1, 2021), petition for cert. denied, No. 21-1322 (U.S. June 13, 2022), which extended *Taggart* to apply to contempt sanctions imposed for repeated violations of bankruptcy court orders, declaring a home mortgage current.

In *Taggart*, the Supreme Court found that a bankruptcy court may hold a creditor in contempt for attempting to collect on a debt discharged in bankruptcy “if there is no fair ground of doubt as to whether the [discharge] order barred the creditor’s conduct.” *Taggart*, 139 S. Ct. at 1801. *Taggart* did not address whether the standard applied to other court orders or bankruptcy codes.

Several courts have reached mixed results when using the *Taggart* standard. See, e.g., *Deutsche Bank Trust Co. Americas v. Gymboree Group, Inc.*, 2021 WL 3618229, *11 (E.D. Va. Aug. 16, 2021)

(“Because there is fair ground for doubt concerning the requirements of the 2017 Plan and related disbursements, the record does not warrant a finding of contempt.”); *Tate v. Fairfax Village I Condominium*, 2020 WL 634293 (Bankr. D.D.C. Feb. 10, 2020) (citing *Taggart* in finding a willful violation of the stay in a Chapter 13 case and imposing sanctions under Section 362(k)(1) of the Bankruptcy Code).

In *Beckhart*, the debtors filed for Chapter 11 bankruptcy, seeking to reinstate their mortgage loan. The lender objected because the plan did not include the payment of the prepetition debt or the application of post-petition principal and interest payments. The bankruptcy court approved the plan over the lender’s objection. The debtors continued making payments according to their Chapter 11 plan, but nearly four years later, the loan servicer informed the debtors that their account was past due by approximately \$50,000. After some attempts to resolve the issue, the lender served the debtors with a foreclosure notice in January 2020. The debtors then filed a motion in the bankruptcy court for civil contempt and sanctions against the loan servicer and the lender (collectively, the defendants). After an evidentiary hearing, the bankruptcy court entered an order to find the defendants in contempt and directed them to pay monetary sanctions of approximately \$115,000 to the debtors. On appeal, the district court reversed and remanded, finding the confirmation order confusing because it did not expressly address what amount the debtors would owe as of the confirmation date or how the pre- and post-petition arrearages would be repaid, if at all.

The Fourth Circuit held neither the bankruptcy nor the district court correctly applied the *Taggart* standard to the facts. According to the decision, the bankruptcy court did not use the *Taggart* standard, but instead a four-factor test for civil

contempt standards articulated in a Fourth Circuit non-bankruptcy decision that long predated *Taggart*. It further held that the district court erroneously granted controlling weight to the defendant's reliance on the advice of counsel as a sufficient defense to civil contempt. Therefore, having concluded that both lower courts "erred in analyzing the threshold question of whether [the defendants] may be held in civil contempt at all," the Fourth Circuit held that the district court's ruling should be vacated, and the case should be remanded to the bankruptcy court "to reconsider the contempt motion under the correct legal standard."

In *Gravel* and *Beckhart*, two appellate courts have answered an important question *Taggart* left unanswered. That is, whether the "fair ground of doubt" standard applies to contempt for violating bankruptcy court orders other than orders discharging Chapter 7 debtors. In ruling it does, the Second and Fourth circuits have expanded the *Taggart* decision beyond its original application. Some lower courts have already embraced this expansive interpretation of *Taggart*.

The Sun Goes Down on Section 1329(d) Plans

Congress has allowed the seven-year Chapter 13 plans it permitted under the CARES Act to expire, and bankruptcy courts are tending to hold that any new modifications are required to comply with the historical maximum plan duration of five years. See *In re Nelson*, 71 Bankr. Ct. Dec. 269 (Bankr. E.D. Wisc. 2022).

Historically, the duration of a plan modified post-confirmation is limited to a maximum of five years. 11 U.S.C. § 1329(c). Specifically, "a court may not approve a period that expires after five years." 11 U.S.C. § 1329(c). Congress, with the CARES Act, added temporary provision 11 U.S.C. § 1329(d), which allowed qualifying debtors to modify their confirmed Chapter 13 plans to a maximum duration of seven years. However, this legislation included a sunset date of March 27, 2022. See Public Law 117-5 (COVID-19 Bankruptcy Relief Extension Act of 2021).

Based on this sunset provision, any attempts after March 27, 2022 to modify a previously modified plan may run afoul of the five-year plan limit of Section 1329(c), despite the prior modified plan lawfully extending up to seven years. Courts have handled this issue two ways. Either disapprove any post-sunset modification if the proposed modified plan has a duration of greater than five years, OR alternatively, approve post-sunset modifications, permitting the plan duration to be greater than five years so long as the proposed modified plan is unopposed by creditors.

The first approach of disapproving any post-sunset modifications if the plan extends beyond five years stems from a strict statutory interpretation and the separation of powers doctrine. In *Nelson*, the court interpreted the Section 1329(c) five-year limitation to apply to the entire "plan," not simply the modified provision of the plan. 2022 WL 6795096, at 5. The court in *Nelson* also expressed hesitancy to "fix the mistake" of Congress because doing so may "interfere with the legislative power to fashion the



rules.” *Id.* at 8. Accordingly, the court disapproved the modified plan because it extended beyond the five-year limit.

At least one court has taken the alternate approach of approving post-sunset modifications of plans that extend beyond five years. *In re Mercer*, 640 B.R. 577, 581 (Bankr. D. Colo. 2022). The court in *Mercer* reasoned that any plan extension beyond five years that had been approved pre-sunset “should remain in effect despite a subsequent modification to the plan after the sunset date.” *Id.*

The *Nelson* decision specifically criticized the *Mercer* decision for its lack of reasoning and follows two other opinions from the same judge. *Nelson*, 2022 WL 6795096 (citing *In re Sykes*, 638 B.R. 578 (Bankr. E.D. Mich. 2022); *In re Bohinski*, 638 B.R. 870 (Bankr. E.D. Mich. 2022)). Although *Mercer* appears to be an outlier, there may be other unpublished decisions of bankruptcy courts, approving post-sunset modifications of plans that extend beyond five years. Nevertheless, it appears the trend seems to be leaning toward disapproval of post-sunset modifications of plans that extend beyond five years.

Without a clear answer whether post-sunset modifications of seven-year plans will be approved or denied, parties seeking to modify the plan, such as debtors, Chapter 13 trustees, and unsecured creditors, should proceed with caution. Secured creditors may use the sunset of Section 1329(d) as a reason to object to modification of plans that extend beyond five years. The strange consequence of the sunset of Section 1329(d) is that even if the proposed modified plan would increase payment to creditors, and the creditors consent to the modification, the court may disapprove the modification. See e.g., *In re Nelson*, 71 Bankr. Ct. Dec. 269 (Bankr. E.D. Wisc. 2022). Since it is unlikely that Congress will at any time in the near future clarify whether plans that previously obtained the benefit of a seven-year duration will be permitted to remain seven-year plans despite modifications to other terms, parties in Chapter 13 bankruptcy proceedings must navigate the differing approaches of bankruptcy courts across the nation. It remains to be seen whether circuit courts will weigh in on this issue.

Without a clear answer whether post-sunset modifications of seven-year plans will be approved or denied, parties seeking to modify the plan, such as debtors, Chapter 13 trustees, and unsecured creditors, should proceed with caution. Secured creditors may use the sunset of Section 1329(d) as a reason to object to modifications of plans that extend beyond five years.

Continued Litigation Surrounding U.S. Trustee’s Fees

Congress may only establish “uniform Laws on the subject of Bankruptcies throughout the United States.” U.S. Const. art. I, § 8, cl. 4 (the bankruptcy clause). However, in 2017, Congress enacted legislation (2017 Act) that temporarily increased fees that Chapter 11 debtors had to pay in only 88 of the 94 judicial districts in the United States, seeking to offset the costs of the U.S. Trustee Program, especially in large bankruptcy cases, after the U.S. Trustee Fund faced an ongoing shortfall.

This increase ran from fiscal year 2018 through fiscal year 2022, with the new quarterly fee increasing from a prior maximum of \$30,000 to the lesser of 1% of disbursements or \$250,000. In September 2018, the Judicial Conference applied the increase to the remaining six districts—districts in North Carolina and Alabama that utilize the Administrator Program as opposed to the U.S. Trustee Program to serve the function of impartial case monitoring and supervision—to bankruptcy cases filed on or after October 1, 2018.



The 2017 Act met with legal challenges—most notably in the Circuit City Chapter 11 bankruptcy filed in the Bankruptcy Court for the Eastern District of Virginia—because it did not apply in the bankruptcy administrator districts. A split between the First, Fifth, and Eleventh circuits on one side and the Second and Tenth circuits on the other developed over the constitutionality of the 2017 Act, and the Supreme Court sought to resolve the split when it granted certiorari. See *Siegel v. Fitzgerald*, 142 S. Ct. 1770 (2022).

In *Siegel*, a U.S. trustee argued that the fees aspect of the 2017 Act did not fall under the uniformity requirement of the bankruptcy clause because the increase was an “administrative law” rather than a “substantive law,” and, even if the clause applied, it forbade “only ‘arbitrary’ geographic differences.” *Id.* at 1778.

The Supreme Court rejected both arguments and unanimously held “that the 2017 Act falls within the ambit of the Bankruptcy Clause,” *Id.* at 1780, and that the 2017 Act was not a “permissible exercise” of the law because the 2017 Act was “not geographically uniform” without the requisite justification for such disparate treatment. *Id.* at 1781-82.

The Supreme Court concluded that “[n]othing in the language of the Bankruptcy Clause itself ... suggests a distinction between substantive and administrative laws” and highlighted the fact that the “Bankruptcy Clause’s language, embracing ‘laws on the subject of Bankruptcies,’ is broad.” *Id.* at 1779. Indeed, the Supreme Court noted that it had never distinguished between substantive and administrative bankruptcy laws. *Id.*

The Supreme Court remanded the matter to the Fourth Circuit, which then remanded to the Bankruptcy Court for the Eastern District of Virginia to consider appropriate remedies. *Ventoux Int’l, Inc. v. Fitzgerald (In re Circuit City Stores, Inc.)*, No. 19-2240 (L), 2022 U.S. App. LEXIS 20018 (4th Cir. July 20, 2022).

At this time, what the ultimate course of action will be for fees paid under the 2017 Act remains uncertain. Although the dollar amount at issue may be large, this decision will likely affect only a small percentage of Chapter 11 cases pending during the at-issue time period. However, the one thing that is for certain is that debtors will seek to recoup fees paid into the Trustee Program under the 2017 Act now that the Supreme Court has ruled that it is unconstitutional.

CONSUMER CLASS ACTIONS

Authors: Tony Kaye, Timothy J. St. George, Julie Diane Hoffmeister, Mary Kate Kamka, Kathleen M. Knudsen, Nathan R. Marigoni

2022 was an interesting year of class action developments. Several key highlights are explored below.

Circuit Split on Class Action Standing

In *TransUnion v. Ramirez*, 141 S. Ct. 2190 (2021), the U.S. Supreme Court held that all class members must have standing – and therefore be “injured” – in order to recover individual damages in a class action. However, the *TransUnion* Court did not address the related question of whether every member of the class must show standing and injury at the class certification stage. Before and after *TransUnion*, circuit courts remain divided over this issue. In 2022, this split became more evident based on two differing decisions by the Ninth and Eleventh Circuits.

In *Olean Wholesale Grocery Cooperative, Inc. v. Bumble Bee Foods LLC*, 31 F.4th 651 (9th Cir. 2022), the Ninth Circuit approved the certification of a class containing more than a *de minimis* number of uninjured class members. In that case, plaintiff alleged that tuna suppliers engaged in a conspiracy to fix the price for canned tuna, thereby violating antitrust laws. The district court certified classes and subclasses that included all purchasers of defendant’s canned tuna during the relevant time period. At class certification, the parties disputed the number of uninjured persons included in the proposed class definition. Defendant put forth expert evidence suggesting that as much as 28% of the class did not experience a statistically significant price difference in their tuna purchase, and so did not suffer any resulting injury. In certifying the class, the majority acknowledged that plaintiff had not proven that 28% of the class members had suffered an actual injury, but found that plaintiff did not need to do so at this stage of the litigation. In other words, the Ninth Circuit refused to adopt a *per se* rule precluding certification of Rule 23(b)(3) classes containing more than a *de minimis* number of injured members.

The Eleventh Circuit, on the other hand, came to a different conclusion in *Drazen v. Pinto*, 41 F.4th 1354 (11th Cir. 2022). There, the plaintiff alleged that defendant GoDaddy violated the Telephone Consumer Protection Act (TCPA) when it allegedly called and texted the plaintiff to market its services and products through a prohibited automatic telephone dialing system. The parties reached a \$35 million class settlement, and the district court certified the settlement class, acknowledging that the alleged class contained uninjured class members, but finding that only the named plaintiff must have standing to certify the class. On appeal, the Eleventh Circuit held “that the class definition does not meet Article III standing requirements.” Citing *TransUnion*, the court explained that “when a class seeks certification for the sole purpose of a damages settlement under Rule 23(e), the class definition must be limited to those individuals who have Article III standing. If every plaintiff within the class definition in the class action in *TransUnion* had to have Article III standing to recover damages after trial, logically so too must be the case with a court-approved class action settlement.” The Eleventh Circuit ultimately vacated the class settlement, finding that the class settlement definition – which included all persons who received a voice or text message from GoDaddy – “cannot stand.”

The Fifth Circuit is set to decide a similar standing-related issue in *Earl, et al. v. The Boeing Co., et al.*, No. 21-40720 (5th Cir.). On July 5, 2022, the Fifth Circuit heard oral argument in the *Boeing* appeal and questioned whether Boeing and Southwest Airlines must face certified class allegations that they overcharged passengers for flights. The underlying case involves claims under the Racketeer Influenced and Corrupt Organizations Act (RICO) alleging that Boeing and Southwest Airlines conspired to defraud the public by concealing safety defects on the Boeing 737 MAX 8 aircraft. The plaintiffs all safely reached their destinations, and the majority never even flew on



a 737 MAX 8, but they claim they would not have purchased tickets or would have paid less for routes that use the 737 MAX 8 if they knew about the defects. The district court granted class certification, but the Fifth Circuit subsequently granted the defendants' Rule 23(f) petition. Standing was a key issue at the July 5 hearing before the Fifth Circuit. Defendants argued that the plaintiffs do not have standing because their claims are based on an increased risk of harm that never materialized and each plaintiff received the benefit of his or her bargain (i.e., a safe flight to desired destination). If the Fifth Circuit finds the plaintiffs lack standing, that decision could potentially have a direct impact on other cases, including many data breach cases that are likewise based on a risk of future harm that has never materialized.

These decisions make clear that whether a class containing uninjured class members can be certified depends on the circuit in which it was filed. In 2023, we look forward to seeing if the Supreme Court will resolve this deepening circuit split.

Data Breach Class Developments

In 2022, as a consequence of the increasing frequency of security breaches, we saw an expected increase in consumer data breach class action litigation. Plaintiffs have historically struggled to certify Rule 23(b)(3) damages classes given that injury *caused* by a data breach can be difficult to prove through common evidence. For that reason,

defendants have, for the most part, avoided class certification by demonstrating that class representatives or class members cannot establish Article III standing.

However, on May 3, 2022, Judge Grimm of the U.S. District Court for the District of Maryland issued a class certification decision in a consumer data breach multidistrict litigation case against an international hotel and resort management company, becoming one of the few district courts to certify Rule 23(b)(3) classes in this type of case. See *In re Marriott International, Inc. Customer Data Security Breach Litigation*, MDL No. 19-md-2879 (D. Md.). The litigation arises out of a data breach of one of the company's guest reservation databases that allegedly exposed guests' reservation details, contact information, and some payment information.

The decision granted in part and denied in part the plaintiffs' motion for class certification. More specifically, the court denied certification of: (1) a state data breach notification statute class because the asserted damages were not tied to the plaintiffs' damages theory; (2) injunctive and declaratory relief classes because the plaintiffs failed to describe the contours of their requested relief and because the record showed that there was no continuing risk of future data breaches; and (3) damages class based on a rejected "loss of market value of PII" theory. The court did certify multiple state-specific Rule 23(b)(3) damages classes for the plaintiffs' contract and statutory claims, but substantially modified and

narrowed the classes, including to: (1) only those class members who were members of the hotel's "preferred guest" program, resulting in all class members having identical contractual relationships with the defendant; and (2) only those guests who bore the economic burden for a hotel stay since the plaintiffs' damages theory relied in part on overpayment for each stay.

The class certification decision is currently on appeal to the Fourth Circuit. We will continue to monitor the case for developments and potential impacts on other data breach litigation.

Supreme Court's Focus on Arbitration and Impact on Class Actions

In its 2021 term, the Supreme Court took a close look at arbitration, issuing four merits decisions on arbitration issues.

Two of those decisions, *Morgan v. Sundance, Inc.*, 142 S. Ct. 1708, and *Viking River Cruises, Inc. v. Moriana*, 142 S.Ct. 1906, impact strategies for managing class action risk.

***Morgan v. Sundance* Eases Burden to Show Waiver of Arbitration Provision**

The inclusion of an arbitration agreement and class action waiver in consumer agreements is an important component of managing class action exposure. Because a consumer bound by an enforceable arbitration agreement has agreed to forgo bringing claims in court, the consumer generally cannot represent a class or otherwise participate in class actions. However, due to costs or administrative requirements of arbitration, some companies attempt to resolve putative classes—by settlement or, in some cases, seeking dismissal of the claims—before moving to compel arbitration.

The Supreme Court's *Morgan v. Sundance* decision increases the risk that such a course of action will result in a finding that the right to arbitrate has been waived. Because the right to demand arbitration is a contractual right, courts concluded that it may be

waived by a party taking actions inconsistent with the right to arbitrate. However, a split of authority developed regarding whether there was an additional requirement of prejudice—i.e., that the delay by the party seeking to compel arbitration had harmed the rights of the party opposing arbitration. Most federal circuits adopted this "prejudice" requirement, reasoning that "mere delay" did not justify depriving a party of its contractual right to insist a claim be arbitrated.

The inclusion of an arbitration agreement and class action waiver in consumer agreements is an important component of managing class action exposure. Because a consumer bound by an enforceable arbitration agreement has agreed to forgo bringing claims in court, the consumer generally cannot represent a class or otherwise participate in class actions.

However, in a unanimous decision, the Supreme Court rejected the majority rule, concluding it had no basis in the common law of waiver and was otherwise inconsistent with the Federal Arbitration Act's (FAA) policy favoring arbitration. The Supreme Court held that where the waiver inquiry is governed by federal law, a party attempting to avoid arbitration need only show that the other party knowingly relinquished the right to arbitration by acting inconsistently with that right; no showing of prejudice is required.

Morgan v. Sundance will inevitably impact litigation strategy decisions when faced with arbitration agreements. The decision left open several important questions about the reach of this rule, however. Chief among them is whether waiver should be governed by state-law waiver rules—many of which retain the prejudice requirement for arbitration agreements—rather than federal law. Defendants faced with a waiver argument must carefully consider whether state-law waiver or other principles such as forfeiture, estoppel, or laches provide a more favorable standard. We expect significant interest in and development of such state-law alternatives to the waiver inquiry in light of this decision.

Viking River Cruises v. Moriana Approves Some State-Law Limits on Pre-Suit Waiver of Collective Actions

In its 2011 decision in *AT&T Mobility LLC v. Concepcion*, the Supreme Court held that the FAA preempts state laws prohibiting class action waivers in pre-suit arbitration agreements. However, some state laws, like California's Private Attorneys General Act (PAGA), allow plaintiffs to use a class-like mechanism to aggregate claims in certain circumstances, and also bar the pre-suit waiver of the right to bring such claims. *Viking River* addressed whether the bar on pre-suit waiver of the right to bring a PAGA claim was preempted by federal law.

PAGA itself permits an aggrieved employee to file a private suit on behalf of California's Labor and Workforce Development Agency to challenge certain labor practices. The law permits a plaintiff to seek any civil penalties the state could bring, with the proceeds split between the plaintiff and the labor agency. The law also permits a plaintiff to seek penalties for violations involving employees other than the plaintiff, allowing a PAGA litigant to join the claims of multiple aggrieved employees into a single aggregate, quasi-class action. The California Supreme Court had concluded that contractual provisions waiving the right to file a PAGA suit—either by waiving the right to bring PAGA claims at all or by agreeing to “split” the plaintiff's individual claim out for separate arbitration—were void as a matter of public policy.

The Supreme Court concluded that California's bar on agreements to arbitrate a plaintiff's individual claim was preempted by the FAA, but allowed the state's prohibition on wholesale waiver of PAGA claims to stand. The Court ruled that the “claim splitting” prohibition effectively required a contracting party to either agree to arbitrate the plaintiff's claims plus those of any number of aggrieved claimants the plaintiff sought to join or forgo arbitration altogether. The Supreme Court concluded this rule conflicted with the FAA by unduly burdening the freedom of parties to determine by contract what claims will be subject to arbitration. However, the Court had no such trouble



with the bar on waiving PAGA claims in their entirety, concluding that such claims only truly involved the claims of one party—the state through its labor agency—and therefore did not present defendants with the same untenable dilemma between undertaking “class” arbitration and forgoing arbitration entirely.

Thus, *Viking River* allows states to create class-like enforcement mechanisms that allow private plaintiffs to aggregate claims that could otherwise be brought on behalf of the state, and also prohibits pre-suit waiver of such claims. While PAGA itself applies only to violations of the California labor code, states could adopt similar provisions that apply to an array of consumer protection statutes, including broad and flexible unfair and deceptive practice laws. However, states cannot prohibit agreements to arbitrate an individual’s own claims separately from any “private attorney general” claims the plaintiff may bring.

After *Viking River*, companies and counsel drafting arbitration and waiver provisions relating to “representative” or aggregated claims under state laws like PAGA must consider whether waiver is permissible under state law. If not, drafters should avoid wholesale waivers of such representative actions, ensure individual claims are within the scope of the arbitration clause, and include a severability clause to ensure any partial invalidation of a waiver does not strike the entire agreement to arbitrate. Any strategy to mitigate class action risk must also include carefully monitoring any developments in state consumer-protection laws to watch for the adoption or recognition of any right to bring such “representative” private-attorney-general actions on behalf of the state, and take appropriate action to update arbitration and waiver agreements appropriately.

In 2022, Appellate Courts Looked at Attorney’s Fee Claims in Class Cases

In a consumer class action settlement, plaintiff’s counsel often receives a fee award that is calculated based off a percentage of the total

settlement amount. For larger class action settlements, this fee award can be significant. In 2022, we saw the circuit courts increase their scrutiny of attorney fee claims in consumer class actions.

For example, in *Fessler v. Porcelana Corona De Mex., S.A.*, 23 F.4th 408 (5th Cir. 2022), the Fifth Circuit held that an award of attorney’s fees to class counsel must consider the time spent on unsuccessful claims. The consumer class had sought injunctive relief and monetary damages against a manufacturer of toilet tanks for alleged defects in seven models produced over nine years. After substantively litigating the case, in two steps, the redefined, narrower class settled for monetary damages for a single year with only two tank models. The class obtained injunctive relief for only four of the nine model years.

Following settlement, class counsel sought over \$12 million in fees. The district court found it too difficult to separate time spent on successful claims from time spent on unsuccessful claims. The district court ultimately awarded \$4.3 million to class counsel. The Fifth Circuit vacated and remanded. The Fifth Circuit held that “[t]he district court’s failure to make any factual findings regarding the nature of the class’s unsuccessful claims is an abuse of discretion.” 23 F.4th at 417. Further, the Fifth Circuit noted that “it appears that [c]lass [c]ounsel achieved little beyond Porcelana’s self-imposed replacement program, which the defendant instituted following its admission in 2016 that there were problems in the 2011 manufacturing runs for two tank models” *Id.* at 419.

Because “the district court failed to account for counsel’s time spent on unsuccessful claims and failed to compare the relief sought to that actually awarded,” the attorney fee award was improper. *Id.* at 413. The Fifth Circuit remanded with a word of caution to the district court: “On remand, the court must consider the amount of damages and non-monetary relief sought compared to what was actually received by the class. But in doing so, the court’s scrutiny should ‘guard[] against the public perception that attorneys exploit the class action device to obtain large fees at the expense of the class.’” *Id.* at 419-20 (citation omitted).



In contrast, the Fourth Circuit was more supportive of a sizable award of class attorney's fees. In *In re Lumber Liquidators Chinese-Manufactured Flooring Products Marketing, Sales Practices and Products Liability Litigation*, 27 F.4th 291 (4th Cir. 2022), the Fourth Circuit affirmed an award of \$10.08 million in attorney's fees as reasonable and consistent with the value of the settlement to class members, which included store vouchers qualifying as "coupons" under the Class Action Fairness Act (CAFA). *Id.* at 295. The Fourth Circuit had vacated a prior fee award for failing to "calculate the attorney's fees in accord with the 'coupon' settlement provisions of [CAFA]." *Id.* at 294. On remand, the district court awarded class counsel \$10.08 million in fees from the \$22 million settlement fund. The objectors to the class once again appealed the fee award.

In denying the objectors' appeal, the Fourth Circuit held the class "settlement agreement authorized an award of fees of no more than 33.33% of the 'Settlement Fund,' which the settlement agreement defined as 'a total of \$22 million [] in cash and \$14 million [] in [s]tore-credit [v]ouchers.'" *Id.* at 296. Based on these numbers, "the settlement permitted a maximum of \$11,998,800 in attorney's fees, or one-third of \$36 million." *Id.*

The CAFA "coupon" provision states that "[i]f a proposed settlement in a class action provides for a recovery of coupons to a class member, the portion of any attorney's fee award to class counsel that is attributable to the award of the coupons shall be based on the value to class members of the

coupons that are redeemed." 28 U.S.C. § 1712(a). CAFA also states that "[n]othing in this subsection shall be construed to prohibit application of a lodestar with a multiplier method of determining attorney's fees." 28 U.S.C. § 1712(b)(2).

Based on this provision, an objector argued that because the vouchers were "coupons" under CAFA, their use "required greater judicial scrutiny." 27 F.4th at 296. Further, "the vouchers were not worth their stated \$14 million face value when held as 'coupons,' and should not be valued as such in calculating attorney's fees for [c]lass [c]ounsel." The Fourth Circuit saw things differently, and held award was consistent with the lodestar analysis of attorney's fees regardless of any coupon value of the settlement. *Id.* at 306. It also ruled that the fact that the fee award represented 45.8% of the \$22 million settlement fund and was more than the \$9.9 million cash to be distributed to the putative class members was not unfair. To the contrary, the Fourth Circuit held it was improper to compare the fee award with only the cash portion of the settlement because, even if the vouchers were coupons for purposes of CAFA, "the vouchers remain a fully valuable part of the underlying settlement agreement." *Id.* at 307.

Together, these decisions reflect that in 2022, appellate courts were closely considering fee awards for class counsel. Of course, the ultimate decision on whether the fee is reasonable will continue to vary by court.

CONSUMER CREDIT REPORTING

Authors: Ethan G. Ostroff, Kim Phan, Justin T. Golart, Carter R. Nichols, Sarah T. Reise, Derek M. Schwahn

CARES Act

For nearly three years, we have written about the impact of COVID-19 on credit reporting. Even as the world re-opens, we continue to see its ongoing impact. The Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 amended the federal Fair Credit Reporting Act (FCRA) to establish specific reporting requirements for loans and other credit obligations where an “accommodation” is provided to a consumer as a result of a COVID-19-related hardship.

Some benefits created by the CARES Act, in particular with regard to payment forbearances for borrowers with federally backed mortgages, still remain available. The U.S. Department of Health and Human Services (HHS) most recently extended the PHE on October 13, 2022, making it effective through January 11, 2023. The existence of the PHE and availability of benefits, such as the mortgage payment forbearance, has long-term credit reporting implications for loan servicers. For example, borrowers with federally backed mortgages that took advantage of a payment forbearance were allowed to defer repayment of the forbearance amounts until the end of their mortgages. As a result, the reporting of these outstanding amounts is a particularly important issue for data furnishers to consider since the CARES Act makes clear that reporting related to an accommodation under the CARES Act cannot negatively affect a borrower. Mortgage servicers furnishing data to consumer reporting agencies (CRAs) must take particular care to ensure that amounts covered during an accommodation period are not reported in a way that could be considered derogatory to a consumer’s credit.

Another lasting impact of the CARES Act and COVID-19 is the continuing moratorium on federal student loan repayment. While the Biden administration had planned for payments to resume after it announced a series of loan reduction/cancellation plans, litigation over the debt reduction/forgiveness has put the Biden

administration’s plans in limbo. As a result, the Department of Education announced that repayment of federal student loans would remain paused until 60-days after the litigation is resolved or 60-days after June 30, 2023, whichever is earlier. As a result, data furnishers who service federal student loans must continue to adhere to the reporting requirements that have been in effect since the start of the student loan pause.

Litigation Updates

Furnishers

During this past year, the expectations relating to a furnisher’s duty to reasonably investigate consumer disputes continued to expand. The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) have led the way on this issue by filing amicus briefs, advocating higher standards for the duties of furnishers to investigate indirect disputes. The agencies have focused on two primary areas: (1) the distinction between legal and factual disputes; and (2) furnishers’ investigation of indirect disputes deemed “frivolous.”

Legal Disputes

Prior legal precedent had established that consumer reporting agencies (CRAs) are generally not required to resolve legal disputes made by consumers. In some circuits, such as the First and Eleventh circuits, courts have extended this reasoning to the investigation duties of furnishers, holding that “a plaintiff must show a factual inaccuracy rather than the existence of disputed legal questions.” *Hunt v. JPMorgan Chase Bank, N.A.*, 770 F. App’x 452, 458 (11th Cir. 2019). Where the dispute “turns on questions that can only be resolved by a court of law,” a furnisher can escape liability under Section 1681s-2(b) of the FCRA. *Chiang v. Verizon New England*, 595 F.3d 26 (1st Cir. 2010).



The CFPB has filed several amicus briefs this year, including in the Second, Ninth, and Eleventh circuits, arguing that the FCRA makes no distinction between a legal and a factual dispute. The CFPB argues that even if the dispute is of a legal nature, a furnisher is still required to conduct a reasonable reinvestigation, including resolving questions of legal significance. According to the CFPB, furnishers are uniquely qualified to resolve disputes implicating legal questions because of their relationship to the consumer and access to relevant information.

In April 2022, the CFPB filed an amicus brief with the Eleventh Circuit in *Milgram v. JPMorgan Chase*, Docket No. 22-10250, a case that involves the duty of furnishers to reasonably investigate the accuracy of the information they furnish after it is disputed by a consumer. In its brief, the CFPB argues that a furnisher has the same duty to reasonably investigate disputed information regardless of whether the underlying dispute could be characterized as “legal” or “factual.” The case remains pending before the Eleventh Circuit.

In May 2022, the Ninth Circuit weighed in on this issue in *Gross v. CitiMortgage, Inc.*, 33 F.4th

1246 (9th Cir. May 16, 2022). The case concerned a furnisher’s investigation of the plaintiff’s dispute related to the reporting of a junior mortgage’s late payments and a past due balance. The undisputed facts were that the plaintiff had previously gone into foreclosure, but the funds were inadequate to satisfy all mortgages on the property. Under Arizona’s anti-deficiency statute, the junior mortgagee could not recover a deficiency judgment, and the plaintiff was not required to pay the debt. Therefore, as a matter of law, the reporting and the failure to correct the reporting was improper.

Citing the CFPB’s amicus brief, the Ninth Circuit described the distinction between “legal” and “factual” disputes as “ambiguous, potentially unworkable,” and inviting furnishers to evade investigative duties. Echoing the CFPB’s positions, the opinion noted that furnishers are in a far better position to investigate consumer disputes involving a legal question than consumer reporting agencies. The Ninth Circuit concluded the “FCRA will sometimes require furnishers to investigate, and even to highlight or resolve, questions of legal significance.”

Frivolous Disputes

With respect to investigating “frivolous” disputes, the CFPB and the FTC are making similar efforts to redefine the scope of a furnisher’s investigation duties. Some courts have held that a furnisher need not investigate an *indirect* dispute it deems frivolous, such as when a consumer fails to provide all necessary supporting documentation. See, e.g., *Palouian v. FIA Card Services*, No. 13-cv-293, 2013 WL 1827615 (E.D. Pa. May 1, 2013). These courts have relied on the requirements of Section 1681s-2(a) and case law related to consumer reporting agencies’ ability to categorize disputes as “frivolous” under Section 1681i and applied this reasoning to conclude that furnishers are not required to investigate frivolous indirect disputes. CFPB regulations even provide a procedure for designating *direct* disputes as frivolous. 12 C.F.R. § 1022.43(f).

However, as the agencies have argued in their amicus briefs, there is nothing in the text of the FCRA that suggests that a furnisher can choose not to investigate an *indirect* dispute it deems to be frivolous. The agencies contend the statutory text is unambiguous: furnishers must investigate all indirect disputes. The agencies refer to the case law permitting furnishers not to investigate frivolous indirect disputes as an “atextual, judge-made exception” that is unnecessary because the FCRA requires consumer reporting agencies to determine if a dispute is frivolous before forwarding a dispute to the furnisher. The Third Circuit is currently considering a pending appeal on this issue in *Ingram v. Waypoint Resource Group, LLC*, No. 21-2430 (3d Cir.), in which the CFPB and the FTC filed a joint amicus brief to argue that a furnisher is required to investigate any dispute forwarded to it by a CRA and cannot avoid that obligation by claiming a dispute is “frivolous.”

Consumer Reporting Agencies

Reasonable Reader

In August 2022, the Third Circuit adopted an objective “reasonable reader” standard to evaluate whether information on a consumer report is inaccurate or misleading. In *Bibbs v. TransUnion, LLC*, 43 F.4th 331 (3d Cir. Jan. 20, 2022), the

Third Circuit analyzed whether certain pay status notations were inaccurate or misleading. The Third Circuit rejected the plaintiffs’ contention that it is misleading to report a negative pay status notation of “Account 120 Days Past Due” in conjunction with reporting that the account has been closed, transferred, and had an account balance of zero. The Third Circuit characterized Section 1681e(b)’s “maximum possible accuracy” as an “elusive” idea. Applying the “reasonable reader” standard to find the negative pay status notations were not misleading, the *Bibbs* court noted, “the possibility of further clarity is not an indication of vagueness.”

The Third Circuit determined that the “reasonable reader” standard was consistent with the FCRA’s broad definition of “creditor” that “encompasses sophisticated and unsophisticated individuals and entities,” which “run the gamut to include sophisticated entities like banks and less sophisticated individuals such as local landlords.”

The “reasonable reader” standard requires reading the report as a whole—not in isolation—to determine if the information is inaccurate or ambiguous. Under the “reasonable reader” standard, “if an entry is inaccurate or ambiguous when read both in isolation and in the entirety of the report, that entry is not accurate under § 1681e(b).”

Article III Standing

In June 2021, the U.S. Supreme Court issued its opinion in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), articulating its most recent interpretation of the “concrete injury” standard required for Article III standing. The Supreme Court clarified that disclosing inaccurate information in a consumer report to a third party constitutes a concrete injury sufficient to confer Article III standing, whereas the mere existence of undisclosed inaccurate information in a consumer’s file does not.

Since then, lower courts have sought to apply and interpret *Ramirez* in actions filed against CRAs. In November 2022, the Sixth Circuit applied *Ramirez* when determining whether the plaintiff had alleged a concrete injury in *Hammoud v. Equifax Information Services, LLC*, 52 F.4th 669 (6th Cir. Nov. 4, 2022).

The court concluded that, consistent with *Ramirez*, a third-party disclosure of allegedly inaccurate information is likely to be sufficient for Article III standing, unless the inaccuracy is innocuous. The Sixth Circuit reiterated that a plaintiff has a concrete injury where the CRA actually disclosed inaccurate information in his credit report to a third party.

However, other federal courts of appeals have distinguished *Ramirez*, especially regarding informational injuries. In *Tailford v. Experian Information Solutions, Inc.*, 26 F.4th 1092 (9th Cir. March 1, 2022), the Ninth Circuit distinguished the plaintiffs' file disclosure claim under Section 1681g from the disclosure claims that the Supreme Court decided lacked standing in *Ramirez*. Unlike *Ramirez*, where the plaintiff merely alleged that they received information in the wrong format, the plaintiffs in this case alleged that they were unable to opt out of certain disclosures to other parties without the complete information required under Section 1681g. The Ninth Circuit concluded the plaintiffs alleged a concrete informational injury.

Ramirez will undoubtedly remain at the forefront of Article III standing cases for the foreseeable future, both in CRA litigation and elsewhere.

End Users

Courts grappled with issues of standing in the context of claims against end users. For example, in *Schumacher v. SC Data Center, Inc.*, 33 F.4th 504 (8th Cir. May 3, 2022), the Eighth Circuit initially reversed the district court's order, finding that the plaintiff had sufficiently pleaded an injury-in-fact to support Article III standing. The plaintiff alleged, among other things, that the defendant-employer violated the FCRA's requirement to provide her with an opportunity to review her consumer report before taking adverse employment action, as well as by failing to provide an adverse action notice

that complied with the "clear and conspicuous" requirement of the FCRA.

The Eighth Circuit's panel decision held that the failure to comply with the FCRA's requirement to provide a prospective employee a copy of his/her consumer report prior to taking adverse employment action is a bare procedural violation that does not constitute a sufficient Article III injury-in-fact. Specifically, the court reasoned the express language of the FCRA does not afford a prospective employee the right to discuss accurate but negative information within a consumer report directly with the employer, as opposed to with the CRA, prior to the employer taking an adverse employment action. With respect to the format of the adverse action notice, the court held that the plaintiff alleged a technical violation only, which was also considered insufficient to confer standing. However, shortly after issuing this decision, the Eighth Circuit granted a motion for rehearing by the panel and vacated its decision. The case remains pending.

The Supreme Court clarified that disclosing inaccurate information in a consumer report to a third party constitutes a concrete injury sufficient to confer Article III standing, whereas the mere existence of undisclosed inaccurate information in a consumer's file does not.

By contrast, in *Scott v. Full House Marketing*, 2022 U.S. Dist. LEXIS 38999 (M.D.N.C. March 4, 2022), the District Court for the Middle District of North Carolina found that by alleging “downstream consequences” caused by the defendant-employer’s alleged failure to provide an adverse action notice, a plaintiff alleged a concrete and particularized injury-in-fact to establish Article III standing. Specifically, the plaintiff alleged that the defendant-employer provided an adverse action notice but did not include a copy of the consumer report as required by the FCRA. Five weeks after the defendant declined the plaintiff’s application for employment, the plaintiff learned the consumer report contained inaccurate information. The plaintiff alleged as a result of the defendant’s actions, he lost an employment opportunity and suffered damages in the form of wage loss and emotional distress. The court held that the plaintiff’s “ability to correct erroneous information” was “hindered,” and the plaintiff therefore had standing to pursue his claim.

The Northern District of Indiana reached a similar decision in *Reed v. United States Postal Service*, 2022 U.S. Dist. LEXIS 160155 (N.D. Ind. Sept. 6, 2022). The plaintiff alleged that the defendant committed violations of the FCRA in the process of telling her that she was ineligible for hire because of the results of a background check. The plaintiff alleged that she did not receive any notice of the contents of the background check or her rights to contest them prior to adverse action being taken against her. The defendant argued that even if the plaintiff did not receive notice of her rights before the adverse action, she was not injured by the lack of notice and therefore does not have standing to bring her claim.

The court disagreed, and it held that the plaintiff’s alleged preclusion from discussing or disputing her background report before an adverse action was taken is an informational injury sufficient to give her standing since “what matters is that the plaintiff was denied information that could have helped her craft a response to the defendant’s concern.” The court further explained that Article III’s strictures are met not only when a plaintiff complains of being deprived of some benefit, but also when a plaintiff complains that she was

deprived of a chance to obtain a benefit. According to the court, an informational injury can be concrete when the plaintiff is entitled to receive and review substantive information.

These cases illustrate that, like many statutory claims, courts frequently disagree about what is sufficient to establish an injury-in-fact in connection with claims that an end user failed to comply with the FCRA’s adverse action notice requirement.

Trade Association Litigation

In 2019, Maine passed amendments to the Maine Fair Credit Reporting Act to prohibit the reporting of certain medical debts and other debts arising from economic abuse. The Consumer Data Industry Association (CDIA) filed suit against the Maine Attorney General and the superintendent of the Maine Bureau of Consumer Credit Protection, seeking declaratory judgment that both laws were preempted by the FCRA. In October 2020, the U.S. District Court for the District of Maine ruled in favor of the CDIA, holding that the Maine amendments were preempted. The court concluded that Section 1681t(b)(1)(E) of the FCRA preempted any state regulation of information contained in consumer reports. The Maine defendants filed an appeal to the First Circuit.

In February 2022, the First Circuit vacated the trial court’s order and held that Section 1681t(b)(1)(E) did not entirely preempt the amendments to the Maine Fair Credit Reporting Act. The opinion includes a lengthy textual analysis of the preemption statute rejecting the CDIA’s contention that Section 1681t(b)(1)(E) preempts all state laws “relating to information contained in consumer reports.” The First Circuit went on to hold that “the preemption clause necessarily reaches a subset of laws narrower than those that merely relate to information contained in consumer reports.” The court remanded the case for consideration of whether the medical debt reporting amendments were partially preempted under Section 1681t(b)(1)(E) and whether Section 1681t(b)(5)(C) preempted the economic abuse debt amendments. In September 2022, the district court stayed this case, pending resolution of the CDIA’s petition for writ of certiorari to the Supreme Court.

Regulatory Updates

Furnishers

On January 13, 2022, the CFPB published a compliance bulletin, reminding debt collectors who furnish information to CRAs of their obligations under the FCRA and the Fair Debt Collection Practices Act (FDCPA) when dealing with medical debts covered by the newly effective No Surprises Act, which was designed to protect individuals from surprise medical bills, including by capping amounts consumers must pay for certain types of medical bills. Namely, the bulletin warns furnishers that reporting medical debt charges in excess of those permitted under the No Surprises Act could amount to violations of the FCRA and FDCPA. In light of this, the CFPB asserts that maintaining reasonable written policies and procedures regarding the accuracy of information reported, including medical debt, is of the utmost importance.

The CFPB noted in its *Spring 2022 Supervisory Highlights* that a number of issues were identified during its examinations of furnisher practices. The CFPB found that many furnishers lacked “reasonable written policies and procedures regarding the accuracy and integrity of the information relating to consumers.” In addition, the CFPB observed that when disputes are forwarded to furnishers by CRAs, the FCRA does not provide the furnisher with discretion to deem such disputes frivolous; for indirect disputes, only the CRA has discretion to determine that disputes are frivolous or irrelevant.

The CFPB also issued an interpretive rule on June 28, 2022, stating that states play an important role in the regulation of consumer reporting and articulating its view that state laws that are not “inconsistent” with the FCRA are generally not preempted by that statute. While the FCRA expressly preempts certain categories of state laws, the CFPB’s interpretive rule (Billing Code 4810-AM-P) clarifies the CFPB’s position that FCRA’s express preemption provisions should be interpreted to have a “narrow and targeted” scope, specifically noting that nothing in the FCRA preempts state laws relating to the content or information contained in credit reports. The CFPB affirmed states’ abilities to enact their own credit reporting laws “to tackle credit reporting problems related to medical debt,

tenant screening, and other consumer risks.”

Relating to furnishers, the CFPB stated that “if a State law were to prohibit furnishers from furnishing such information to consumer reporting agencies, such a law would also not generally be preempted.” The CFPB characterized the FCRA’s preemption provisions as “narrow and targeted.” The CFPB paired its interpretive rule on the FCRA’s preemption with a call to arms for state attorneys general to take a more active role in enforcing the Consumer Financial Protection Act, including the FCRA.

Consumer Reporting Agencies

Medical Debt Reporting

Medical debt reporting became a key focus of the CFPB during 2022. According to the CFPB’s March 2022 report, “Medical Debt Burden in the United States,” 58% of all third-party debt collection tradelines were for medical debt, which totaled over \$88 billion as of June 2021. The CFPB views medical debt collection as less predictive of a consumer’s future payments in part because medical debt is usually not a consumer’s choice, there is often no upfront disclosure as to cost, and there is limited ability to compare services.

The three CRAs have responded to the CFPB’s position that medical debt and collection are not predictive of a consumer’s creditworthiness by updating their reporting practices with regard to this type of tradeline. On March 18, 2022, Equifax, Experian, and TransUnion announced significant changes to how medical debts are reported. After July 1, 2022, paid medical collection debts no longer appeared on a consumer’s credit report. Further, the period of time before an unpaid medical bill can be reported was extended from six months to one year. Starting in 2023, the three nationwide CRAs will not include any unpaid medical debt less than \$500 on consumers’ credit reports. The changes resulted in the removal of nearly 70% of medical debt tradelines from consumers’ credit reports.

In August 2022, it was announced that VantageScore, founded by Experian, Equifax, and TransUnion, would update its 3.0 and 4.0 scoring models to no longer use medical collection accounts in the calculation of a consumer’s credit score, regardless of the amount owed or the age

of the collection. According to VantageScore, this resulted in as much as a 20-point increase in affected consumers' credit scores.

Following the announced changes to how medical debt is reported, the CFPB conducted an analysis to determine the impact for consumers. In its report, "Paid and Low-Balance Medical Collection on Consumer Credit Reports," the CFPB reviewed a sample of approximately 5 million de-identified credit reports from one of the three major nationwide CRAs. The CFPB acknowledged that the changes will result in the majority of individual medical collection tradelines being removed from credit reports. The report noted the total dollar amount of reported medical debt may not significantly change due to the \$500 threshold for reporting medical debt.

Facially False Reporting

In October 2022, the CFPB issued an advisory opinion, stating that failure to accurately detect and remove logically inconsistent data from consumer reports violates the FCRA's reasonable procedures requirement. This advisory opinion continues the CFPB's focus on the accuracy of consumer credit reports, which it labels a "longstanding issue." The CFPB highlighted that in 2021, complaints about incorrect information on consumer reports represented the largest share of credit or consumer reporting complaints submitted to the CFPB.

The CFPB views medical debt collection as less predictive of a consumer's future payments in part because medical debt is usually not a consumer's choice, there is often no upfront disclosure as to cost, and there is limited ability to compare services.

The CFPB provided guidance to CRAs on their legal obligations to "follow reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates." Specifically, the advisory opinion states that CRAs have a legal obligation under the FCRA to screen for and eliminate false and inconsistent information from consumer credit reports.

Examples of "logical inconsistencies" in the advisory opinion include: (1) inconsistent account information of statuses, such as an "Original Loan Amount" that increases over time; (2) illogical reporting of a "Date of First Delinquency," such as a Date of First Delinquency that postdates a charge-off date; (3) illogical reporting of information relating to consumers, such as impossible information or information plainly inconsistent with other reported information; and (4) illegitimate credit transactions for minors. The CFPB alleges that "reasonable procedures to assure maximum possible accuracy" would screen for and eliminate these types of logical inconsistencies that lead to inaccurate, facially false data being disclosed on consumer credit reports.

Inadequate Investigation Practices

In November 2022, the CFPB issued a circular, highlighting inadequate investigatory practices by CRAs and furnishers. The CFPB highlighted two issues related to CRAs' duties. First, the circular clarifies that a CRA improperly limits a consumer's dispute rights when it requires a consumer to submit disputes in a specific format or using a certain form. This CFPB guidance also extends to requiring consumers to submit specific documents, like a police report, when the consumer has already provided sufficient information to investigate the disputed item. The CFPB warned that a CRA's obligation to investigate disputes applies "even if such disputes do not include the entity's preferred format, preferred intake forms, or preferred documentation or forms."

The circular also discussed what information a CRA must forward to a furnisher in a dispute. The CFPB stated a CRA does not necessarily need to



forward to the furnisher every document provided by a consumer with the dispute. However, the CRA must provide “all relevant information” regarding the dispute and suggested that a best practice is to provide copies of the documents sent by the consumer: “While there is not an affirmative requirement to specifically provide original copies of documentation submitted by consumers, it would be difficult for a consumer reporting agency to prove they provided all relevant information if they fail to forward even an electronic image of documents that constitute a primary source of evidence.” The CFPB’s circular warns that inadequate investigatory practices could lead to both state and federal enforcement actions.

In addition, the CFPB’s *Fall 2022 Supervisory Highlights* (Issue 28) revealed that one or more national CRAs failed to properly process consumer complaints forwarded by the CFPB. The CFPB requires CRAs to review such complaints, maintain records related to the complaint, and provide the CFPB with regular updates about the resolution. The CFPB’s *Fall 2022 Supervisory Highlights* details how national CRAs failed to report the results of consumer complaints to the CFPB and failed to address all complaints based on inadequate policies related to disputes sent by credit repair

organizations. As a result, the CFPB reported that the national CRAs revised their policies and procedures.

End Users

On April 4, 2022, the U.S. Department of Justice Civil Division’s Consumer Protection Branch (CPB) released its first-ever annual “recent highlights” report. CPB litigates actions referred by the FTC, seeking civil penalties for violations of various consumer protection statutes, including the FCRA. The report included a case involving the misuse of credit reports against a home security company ordered to pay \$15 million in civil penalties and \$5 million in consumer redress for FCRA violations. The company failed to properly implement and monitor its Identity Theft Prevention Program, which allowed some sales representatives to obtain credit reports without consumer consent. The civil penalty awarded was the highest ever for alleged FCRA violations.

On July 28, 2022, the CFPB announced that it took action against a bank for allegedly accessing its customers’ credit reports and opening checking and savings accounts, credit cards, and lines of credit without the customers’ knowledge or permission.

The bank was ordered to pay restitution to harmed consumers and pay a \$37.5 million penalty. The consent order specifically alleges that the bank violated the FCRA when it “used customers’ credit reports without a permissible purpose, and without its customers’ permission, to facilitate opening unauthorized credit cards and lines of credit.”

Legislative Updates

Federal Legislation

On April 14, 2022, the Servicemembers’ Credit Monitoring Enhancement Act (H.R.7526) was introduced in the House to expand the definition of an active-duty military consumer for purposes of certain credit monitoring requirements. Currently, only active-duty military and National Guard and Reserve in active-duty status are eligible for free credit monitoring services. The bill would make all servicemembers, including traditional National Guardsmen and reservists, eligible for free credit monitoring services.

On July 11, 2022, the Military Consumer Protection Task Force Act of 2022 (H.R.8321) was introduced in the House to establish a task force to protect members of the armed forces, veterans, and military families from financial fraud. According to the bill, the task force would include relevant public and private sector stakeholders, including financial services providers and technology companies. As set forth in the bill, the duties of the task force would include collecting and reviewing data pertaining to medical billing, credit reporting, debt collection, and other serious financial challenges facing members of the armed forces, veterans, and military families.

On May 31, 2022, H.R.7919 was introduced in the House to permit certain credit repair organizations to dispute credit information directly with a furnisher. Specifically, the bill would amend Section 1681s-2(a) (8) to strike the word “consumer” and insert the phrase “consumer and credit repair organization” in its place.

On May 3, 2022, H.R.7661 was introduced in the House to prohibit a CRA from furnishing a consumer

report for a credit transaction not initiated by a consumer if the report is being procured based in whole or in part on the presence of an inquiry made in connection with a residential mortgage loan (as defined under Section 103 of the Truth in Lending Act).

On July 21, 2022, H.R.8478 was introduced in the House to amend the FCRA to require the use of a consumer’s current legal name. The bill would require the use of a consumer’s current legal name on consumer reports after the consumer requests a CRA to do so with the intent of respecting transgender and nonbinary consumers’ decisions to change their names and protect them from facing potentially severe adverse effects from having their former names reflected on their credit reports. The bill would also help ensure that an individual’s credit history is not lost after a name change. The bill was reported out of the House Financial Services Committee by a vote of 28-23.

On September 26, 2022, H.R.8985 was introduced in the House to clarify reporting certain consumer credit information related to lease agreements or by utility or telecommunication firms related to utility and telecommunication services to CRAs.

On July 19, 2022, S.4551 was introduced to the Senate to provide a consumer protection framework necessary to support the growth of accessible, affordable, and accountable financing options for postsecondary education and for other purposes. The bill would amend the FCRA to include income share agreement (ISA) information on consumer reports. Specifically, the bill would permit a description of the contract terms of the ISA and information regarding amounts owed under the ISA to be furnished. However, under the bill, a furnisher may not include any speculation about future amounts that may be owed under the ISA, including the reporting of any payment caps or early termination amounts.

State Legislation

In 2022, a few state legislatures proposed and implemented changes that affect credit reporting.

Rhode Island

On June 29, 2022, Rhode Island Governor Dan McKee(d) signed legislation (S.2432), prohibiting CRAs doing business in the state from using all or part of a consumer's Social Security number as the sole factor when determining whether a credit report matches the identity of a person who is the subject of a credit inquiry from a user of credit reports. If, however, a Social Security number is used as one of several factors, the CRA may disclose the credit report in its files to an inquiring user of credit reports only if the name also matches the identity of the person who is the subject of the inquiry.

Washington, D.C.

On April 22, 2022, the Council of Washington, D.C. enacted the Public Health Emergency Credit Alert Temporary Amendment Act of 2022 (B24-0607), which amended, on a temporary basis, Chapter 38 of Title 28 of the District of Columbia Official Code: (1) to require CRAs to accept a personal statement from a consumer, indicating the consumer experienced financial hardship resulting from a public health emergency; (2) to prohibit users of credit reports from taking into consideration adverse information in a report that was the result of the consumer's action or inaction that occurred during the public health emergency; (3) to require CRAs to notify residents of the right to request a personal statement; and (4) to provide for civil actions for violations.

Vermont

On March 15, 2022, H.B.725 was introduced in Vermont to require a landlord, cable company, cell phone company, or any other entity that accesses consumer credit and has a contract with a fee for early termination to report the results of the entity's consumer transactions to CRAs.

California

On February 18, 2022, A.B.2527 was introduced in California to prohibit a person or entity from using a consumer credit report for a purpose related to the renting of a dwelling unit or requiring an

applicant or tenant to answer a question about the contents of a consumer credit report or the information contained therein for the purpose of renting a dwelling, except if the inquirer is required to do so under state or federal law.

Updates to CDIA Guide

2022 saw numerous changes made by the CDIA to its *Credit Reporting Resource Guide*®, including the below summarizations.

Account Status Code “05” Is Obsolete

Effective April 2022, Account Status Code “05”—which was used to denote an account that had been transferred—is now considered by the CDIA to be obsolete, and it should no longer be reported.

Although the “05” Account Status Code is now considered obsolete, the CDIA has not removed it from the hierarchy rules (i.e., Rules #2 and #3) for determining the proper Date of First Delinquency so that furnishers who have not discontinued use of the 05 Account Status Code will not run a foul of proper date of first delinquency reporting requirements.

The CDIA added general guidelines for data furnishers, indicating that an account should not be reported before communicating with consumer(s) about a debt.

New Frequently Asked Question No. 43

The CDIA added a FAQ reporting scenario for “the available options for reporting an account that has regular payments temporarily postponed.”

The new FAQ describes the reporting guidelines for when a lender (creditor) agrees to temporarily postpone regular payments on an account, such as a payment holiday/skip-a-pay, deferred accounts, and accounts in forbearance. The FAQ also provides suggested guidance for developing business policies and procedures for these types of temporary plans.

Clarification to Debt Buyer/Third-Party Collection Agency Reporting

The CDIA added general guidelines for data

furnishers, indicating that an account should not be reported before communicating with consumer(s) about a debt.

A clarification was also added for medical debt collection accounts (i.e., Creditor Classification Code 02) that went into effect on July 1, 2022. These accounts *should not* be reported until they are at least 365 days past the date of the first delinquency that led to the account being sold or placed in collections.



CRYPTOCURRENCY

Authors: Kalama M. Lui-Kwan, Addison J. Morgan, Rene T. McNulty

Introduction

Although 2022 has generally been a grim year for the burgeoning digital assets market, digital assets and blockchain technology are here to stay. On March 9, 2022, President Joe Biden signed Executive Order 14067 titled, “Ensuring Responsible Development of Digital Assets.” Symbolically, this represents the White House’s recognition of the transformational potential of blockchain technology and its ability to optimize the functionality of financial services. Politically, the executive order encapsulates the White House’s intention to regulate this nascent technology to ensure implementation comports with current laws relating to consumer protection, prevention of illicit finance, and advancing the integrity of the U.S. financial system.

As President Biden’s executive order suggests, currently there is no prudential regulator of digital assets in the United States. The lack of a steadfast digital asset regulatory framework has either led to piecemeal application of existing U.S. financial laws to digital asset-related entities, or it has caused digital asset players with global dominance to seek homes abroad through regulatory arbitrage. The recent implosions of stablecoin TerraUSD and cryptocurrency exchange FTX—each of which resulted in estimated retail investor losses of \$14 billion and \$2 billion, respectively—has illustrated that consumer protection remains a vitally important aspect of any financial system, and a comprehensive statutory regime may be necessary to establish clear ground rules for companies engaging in consumer-facing digital asset activities.

In the absence of regulations, federal financial services regulators like the Office of the Comptroller of Currency (OCC), the Financial Crimes Enforcement Network (FinCEN), and the Office of Foreign Assets Control of the U.S. Treasury (OFAC) generally have relied upon the Bank Secrecy Act (BSA) and the International Emergency Economic Powers Act to deter activity that has become persistent in the digital assets industry:

(1) insufficient AML/CFT compliance; (2) insufficient OFAC-sanctions compliance; (3) obfuscation of cryptocurrency transactions through “mixing” protocols; and (4) transmission of value to individuals associated with OFAC-designated jurisdictions. On the other hand, the Consumer Financial Protection Bureau (CFPB) has been focused on the connection between consumer protection guidelines and the real-time payment use case of digital assets, the Federal Trade Commission (FTC) has been focused on consumer protection involving scams and deceptive consumer representations, and the Federal Deposit Insurance Corporation (FDIC) has been focused on misleading representations concerning FDIC deposit insurance.

At the state level, many regulators have grappled with the increased adoption of interest-bearing digital asset deposit account programs, which have been consistently dinged for failing to incorporate proper disclosures of material information to consumers. Nevertheless, as the industry awaits a digital asset regulatory framework from the federal government, many states have decided to develop their own respective digital asset regulatory frameworks.

U.S. Central Bank Digital Currency

The contemplated U.S. central bank digital currency (CBDC) is receiving more attention than ever before. A CBDC is the digital form of a national currency that uses blockchain technology to maintain an electronic distributed ledger (like Bitcoin and other cryptocurrencies) and exists only in electronic form. In the United States, a CBDC would be the digital form of the dollar. Like existing forms of money, a CBDC would enable the public to make digital payments. The White House and Congress have both shown interest in ensuring that this prospective form of currency is regulated. In addition, the New York Federal Reserve is developing a CBDC with the largest banks in the United States.

According to the CBDC Paper, one of the main risks of a CBDC is that it could fundamentally change the structure of the U.S. financial system because it would alter the roles and responsibilities of the private sector and the central bank. The CBDC Paper noted that a widely available CBDC would serve as a near-perfect substitute for commercial bank money.

The Federal Reserve's CBDC Paper

On January 20, 2022, the Federal Reserve released a paper, "Money and Payments: The U.S. Dollar in the Age of Digital Transformation" (CBDC Paper), which examined the benefits and risks of a potential U.S. CBDC. The CBDC Paper, which was not intended to favor any policy outcome, was the first step in a discussion of whether or how a CBDC could improve the safety and efficiency of the payments system.

The CBDC Paper found that to best "serve the needs" of the United States, a CBDC would need to be privacy-protected, intermediated, widely transferable, and identity-verified. In terms of privacy, according to the CBDC Paper, a CBDC would need to strike an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity. In terms of

being intermediated, the CBDC Paper noted that the Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals, and such accounts would represent a significant expansion of the Federal Reserve's role in the financial system and the economy. Accordingly, under an intermediated model, the private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments. The CBDC Paper stated that potential intermediaries could include commercial banks and regulated nonbank financial service providers and would operate in an open market for CBDC services. With respect to transferability, the CBDC Paper found that for a CBDC to serve as a widely accessible means of payment, it would need to be readily transferable between customers of different intermediaries. As to being identity-verified, the CBDC Paper noted that financial institutions in the United States are subject to robust rules designed to combat money laundering and the financing of terrorism, and therefore, a CBDC would need to be designed to comply with these rules. Accordingly, a CBDC intermediary would need to verify the identity of a person accessing CBDC just as banks and other financial institutions currently verify the identities of their customers.

With respect to its benefits, the CBDC Paper stated that as a liability of the Federal Reserve, "a CBDC would not require mechanisms like deposit insurance to maintain public confidence, nor would a CBDC depend on backing by an underlying asset pool to maintain its value[.]" and "would be the safest digital asset available to the general public, with no associated credit or liquidity risk." The CBDC Paper also listed five main benefits of a CBDC; namely, it would: (1) safely meet future needs and demands for payment services; (2) improve cross-border payments; (3) support the dollar's international role; (4) promote financial inclusion; and (5) extend public access to safe and central bank money.

According to the CBDC Paper, one of the main risks of a CBDC is that it could fundamentally change the structure of the U.S. financial system because it would alter the roles and responsibilities of the private sector and the central bank. The CBDC Paper noted that a widely available CBDC would serve as a near-perfect substitute for commercial bank money. This substitution effect could reduce the aggregate amount of deposits in the banking system, which could in turn increase bank funding expenses, and reduce credit availability or raise credit costs for households and businesses. The CBDC Paper further stated that an interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments, which could subsequently reduce credit availability or raise credit costs.

Executive Order and Related Department of Treasury Report

On March 9, 2022, President Joe Biden signed Executive Order 14067 titled, “Ensuring Responsible Development of Digital Assets.”

The executive order called for certain financial regulatory agencies to study digital assets based on six key objectives: (1) consumer and investor protection; (2) financial stability; (3) illicit finance; (4) U.S. leadership in the global financial system and economic competitiveness; (5) financial inclusion;

and (6) responsible innovation. The executive order noted that digital assets pose heightened risks to consumers if protections are not implemented. Because of these perceived risks, the executive order emphasized that oversight, standards, and other safeguards are essential in financial services so that appropriate measures are taken to ensure consumer protection.

The executive order placed the “the highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC,” and directed certain agencies to consider “the actions required to launch a United States CBDC if doing so is deemed to be in the national interest.” Subsequently, the executive order directed the secretary of the treasury, in consultation with the secretary of state, the Attorney General, the secretary of commerce, the secretary of homeland security, the director of the Office of Management and Budget, the director of National Intelligence, and the heads of other relevant agencies, to submit to President Biden a report on the future of money and payment systems.

On September 16, 2022, the U.S. Department of the Treasury published a report, “The Future of Money and Payments” (Treasury Report), in response to the executive order. The Treasury Report reviewed the U.S. system of money and payments—including instant payments, stablecoins, and a potential U.S. CBDC—and considered the implications of



these developments for key public policy goals, including supporting U.S. global financial leadership, advancing financial inclusion and equity, and minimizing risks. The Treasury Report outlined the following four recommendations to the “U.S. government” to improve the U.S. money and payments system: (1) advance work on a possible U.S. CBDC in case one is determined to be in the national interest; (2) encourage use of instant payment systems to support a more competitive, efficient, and inclusive U.S. payment landscape; (3) establish a federal framework for payments regulation to protect users and the financial system, while supporting responsible innovations in payments; and (4) prioritize efforts to improve cross-border payments.

With respect to the first recommendation, advancing a U.S. CBDC, the Treasury Report found that a U.S. CBDC could contribute to a payment system that is more efficient, provides a foundation for further technological innovation, and facilitates more efficient cross-border transactions. The Treasury Report also found that a U.S. CBDC could promote financial inclusion and equity by enabling access for a broad set of consumers and could be designed to foster economic growth and stability, protect against cyber and operational risks, be consistent with individual rights, and minimize risks of illicit financial transactions. The Treasury Report further noted that a U.S. CBDC could have national security implications and should be designed to help preserve U.S. global financial leadership and support the effectiveness of sanctions.

As to its second recommendation, encouraging the use of instant payment systems, the Treasury Report found that enhancements are possible to make payment systems more competitive, efficient, and inclusive, and such enhancements might also reduce the costs of cross-border transactions. To maximize these benefits, the Treasury Report recommended that the U.S. government continue its outreach efforts around instant payments, with a focus on inclusion of underserved communities, and promote the development and use of innovative technologies that allow consumers to access instant payment systems more readily. The Treasury Report also recommended that U.S. government agencies consider and support the use of instant payment systems.

With respect to its third recommendation, the Treasury Report found that a federal framework for payments regulation could support responsible innovation in payments by establishing appropriate federal oversight of nonbank companies involved in the issuance, custody, or transfer of money or money-like assets. This recommendation recognizes that nonbanks are increasingly providing payment services, and these newer entrants may contribute to enhanced competition, inclusion, and innovation. The Treasury Report noted that current oversight of nonbank payment providers is generally at the state level, which varies significantly, and may not address certain risks in a consistent and comprehensive manner. The Treasury Report stated that a federal framework could provide a common floor for minimum financial resource requirements and other standards that may exist at the state level and would complement existing federal AML/CFT obligations and consumer protection requirements that apply to nonbank payment providers.

The Treasury Report’s final recommendation prioritizes work to develop a faster, cheaper, and more transparent international payment system, while considering potential risks of greater integration of cross-border payment systems. The Treasury Report found that private sector payment innovations have been driven in part by inefficiencies in the current cross-border payment systems, and in response to the inefficiencies, countries are making efforts to improve existing systems and also are leveraging new technologies. The Treasury Report noted that the United States “has a strong national interest in being at the forefront of technological development and supporting global standards for cross-border payment systems that reflect U.S. values, including privacy and human rights; are consistent with AML/CFT considerations; and protect U.S. national security.” The Treasury Report further noted that the United States is active in efforts to improve cross-border payments, including through the G20, FSB, and Committee on Payments and Market Infrastructure.

In sum, the Treasury Report offers a detailed and extensive set of recommendations intended to enhance the U.S. money and payments system.

However, notably absent from the Treasury Report were recommendations or guidance to Congress on legislation that could enhance the U.S. regulatory framework for CBDCs. Instead, the Treasury Report encouraged U.S. regulators to use their existing enforcement and regulatory authorities to address identified risks and ensure compliance with existing law. Nonetheless, as discussed below, Congress is actively developing legislation to clarify the regulatory treatment of digital assets, including CBDCs.

White House Releases Framework for Development of Digital Assets

In addition to the Treasury Report discussed above, there were several other reports submitted to the Biden administration in response to the executive order. These reports reflect the input and expertise of stakeholders across government, industry, academia, and civil society that collectively outline a framework for responsible digital asset development. These reports call on agencies to promote innovation by kick-starting private sector research and development and by helping cutting-edge U.S. firms find footholds in global markets, while also calling for measures to mitigate the downside risks like increased enforcement of existing laws and the creation of commonsense efficiency standards for cryptocurrency mining.

In response to these reports, on September 16, 2022, the Biden administration released “FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets,” which collectively outlined recommendations to develop frameworks and policy that advance six key priorities identified in the executive order: consumer and investor protection; promoting financial stability; countering illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.

With respect to protecting consumers, investors, and businesses, the fact sheet states that the Biden administration plans to: (1) encourage regulators like the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission to

aggressively pursue investigations and enforcement actions against unlawful practices in the digital assets space; (2) encourage the CFPB and FTC to “redouble their efforts” to monitor consumer complaints and enforce against unfair, deceptive, or abusive practices; (3) encourage agencies to issue guidance and rules to address current and emergent risks in the digital asset ecosystem; (4) urge regulatory and law enforcement agencies to collaborate to address acute digital asset risks facing consumers, investors, and businesses; (5) encourage agencies to share data on consumer complaints regarding digital assets; and (6) advise the Financial Literacy Education Commission to lead public-awareness efforts to help consumers understand the risks involved with digital assets, identify common fraudulent practices, and learn how to report misconduct.

To promote safe and affordable financial services for all, the Biden administration plans to: (1) encourage agencies to promote the adoption of instant payment systems, like FedNow, by supporting the development and use of innovative technologies by payment providers to increase access to instant payments and by using instant payment systems for their own transactions where appropriate; (2) consider agency recommendations to create a federal framework to regulate nonbank payment providers; (3) encourage agencies to prioritize efforts to improve the efficiency of cross-border payments by working to align global payments practices, regulations, and supervision protocols, while exploring new multilateral platforms that integrate instant payment systems; and (4) advise the National Science Foundation (NSF) to back research in technical and socio-technical disciplines and behavioral economics to ensure that digital asset ecosystems are designed to be usable, inclusive, equitable, and accessible by all.

To foster financial stability, the Biden administration plans to encourage the Treasury to work with financial institutions to bolster their capacity to identify and mitigate cyber vulnerabilities by sharing information and promoting a wide range of data sets and analytical tools, as well as to work with other agencies to identify, track, and analyze emerging strategic risks that relate to digital asset markets



and collaborate on identifying such risks with U.S. allies, including through international organizations like the Organisation for Economic Co-operation and Development and the Financial Stability Board.

To advance responsible innovation, the Biden administration plans to: (1) advise the Office of Science and Technology Policy (OSTP) and NSF to develop a “Digital Assets Research and Development Agenda” to kick-start fundamental research on topics, such as next-generation cryptography, transaction programmability, cybersecurity and privacy protections, and ways to mitigate the environmental impacts of digital assets, while also supporting research that translates technological breakthroughs into market-ready products; (2) advise the NSF to back social-sciences and education research that develops methods of informing, educating, and training diverse groups of stakeholders on safe and responsible digital asset use; (3) encourage the Treasury and financial regulators to provide innovative U.S. firms developing new financial technologies with regulatory guidance, best-practices sharing, and technical assistance through things like tech sprints and innovation hours; (4) encourage the Department of Energy, the Environmental Protection Agency, and other agencies to consider further tracking digital assets’ environmental impacts, developing performance standards as appropriate, and

providing local authorities with the tools, resources, and expertise to mitigate environmental harms; and (5) advise the Department of Commerce to examine establishing a standing forum to convene federal agencies, industry, academics, and civil society to exchange knowledge and ideas that could inform federal regulation, standards, coordinating activities, technical assistance, and research support.

To reinforce the United States’ global financial leadership and competitiveness, the fact sheet states that the Biden administration plans to: (1) recommend that agencies leverage U.S. positions in international organizations to message U.S. values related to digital assets; (2) advise the State Department, the Department of Justice (DOJ), and other U.S. enforcement agencies to increase collaboration with—and assistance to—partner agencies in foreign countries through global enforcement bodies like the Egmont Group, bilateral information sharing, and capacity building; (3) encourage the State Department, the Treasury, and other agencies to explore further technical assistance to developing countries building out digital asset infrastructure and services; and (4) encourage the Department of Commerce to assist cutting-edge U.S. financial technology and digital asset firms find a foothold in global markets for their products.

With respect to fighting illicit finance, the Biden administration plans to: (1) evaluate whether to call upon Congress to amend the BSA, anti-tip-off statutes, and laws against unlicensed money transmitting to apply explicitly to digital asset service providers—including digital asset exchanges and nonfungible token (NFT) platforms; President Biden will also consider urging Congress to raise the penalties for unlicensed money transmitting to match the penalties for similar crimes under other money-laundering statutes and to amend relevant federal statutes to let the DOJ prosecute digital asset crimes in any jurisdiction where a victim of those crimes is found; (2) continue to monitor the development of the digital assets sector and its associated illicit financing risks to identify any gaps in our legal, regulatory, and supervisory regimes; as part of this effort, the Treasury will complete an illicit finance risk assessment on decentralized finance (DeFi) by the end of February 2023 and an assessment on nonfungible tokens by July 2023; (3) encourage relevant departments and agencies to continue to expose and disrupt illicit actors and address the abuse of digital assets; and (4) encourage the Treasury to enhance dialogue with the private sector to ensure that firms understand existing obligations and illicit financing risks associated with digital assets, share information, and encourage the use of emerging technologies to comply with obligations; this will be supported by a request for comment published to the *Federal Register* for input on several items related to AML/CFT.

Finally, with respect to CBDCs, the fact sheet states that the administration has developed policy objectives for a U.S. CBDC system, which reflect the federal government's priorities for a potential U.S. CBDC. The fact sheet states that "these objectives flesh out the goals outlined for a CBDC in the [executive order]. A U.S. CBDC system, if implemented, should protect consumers, promote economic growth, improve payment systems, provide interoperability with other platforms, advance financial inclusion, protect national security, respect human rights, and align with democratic values." However, the Biden administration

cautioned further research and development on the technology that would support a U.S. CBDC is needed. Accordingly, the Biden administration plans to: (1) encourage the Federal Reserve to continue its ongoing CBDC research, experimentation, and evaluation; (2) support the Federal Reserve's efforts and to advance other work on a potential U.S. CBDC by encouraging the Treasury to lead an interagency working group to consider the potential implications of a U.S. CBDC, leverage cross-government technical expertise, and share information with partners; and (3) advise the leadership of the Federal Reserve, the National Economic Council, the National Security Council, the OSTP, and the Treasury Department to meet regularly to discuss the working group's progress and share updates on CBDC and other payments innovations.

Federal Legislative Developments in CBDCs

This past year, legislators introduced a myriad of crypto-related bills that vary widely in their subject matter and scope—including proposals that would regulate the creation and issuance of a CBDC. For example, on January 12, 2022 (before the release of the CBDC Paper), Congressman Tom Emmer (R-MN) introduced a bill to prevent unilateral control of a CBDC by the Federal Reserve. The bill would prohibit the Federal Reserve from issuing a CBDC directly to individuals, reasoning that the Federal Reserve should not have the power to offer retail bank accounts. Emmer said as "other countries, like China, develop CBDCs that fundamentally omit the benefits and protections of cash, it is more important than ever to ensure the United States' digital currency policy protects financial privacy, maintains the dollar's dominance, and cultivates innovation," and "CBDCs that fail to adhere to these three basic principles could enable an entity like the Federal Reserve to mobilize itself into a retail bank, collect personally identifiable information on users, and track their transactions indefinitely." Emmer stated: "[T]o maintain the dollar's status as the world's reserve currency in a digital age, it is important that the United States lead with a posture that prioritizes innovation and does not aim to compete with the private sector."

This past year, legislators introduced a myriad of crypto-related bills that vary widely in their subject matter and scope – including proposals that would regulate the creation and issuance of a CBDC.

On March 30, 2022, U.S. Senator Ted Cruz (R-TX) introduced legislation to prohibit the Federal Reserve from issuing a CBDC directly to individuals. The bill was cosponsored by Senators Braun (R-IN) and Grassley (R-IA). Specifically, this bill would prohibit the Federal Reserve from developing a direct-to-consumer CBDC, reasoning that it could be used as a financial surveillance tool by the federal government. The bill aims to maintain the dollar's dominance without competing with the private sector. Cruz believes that unlike decentralized digital currencies, such as Bitcoin, CBDCs are issued and backed by a government entity and transact on a centralized, permissioned blockchain, leaving it vulnerable to attack and open for use as a direct surveillance tool.

On June 22, 2022, Congressman Jim Himes (D-CT) released a white paper/proposal, "Winning the Future of Money: A Proposal for a U.S. Central Bank Digital Currency," which advocates for the issuance of a CBDC. In the white paper, Himes argued that the implementation of digital currency by the U.S. government could help preserve the dollar's role as the global reserve currency of choice. Himes further argued that with an increasing interest in CBDCs around the globe and an ever-changing technological marketplace, the United States is falling behind other countries in establishing a federally backed currency of its own. Himes pointed out that the United States is behind many of its allies in developing a central bank digital currency, as well as behind countries like Russia and China, which are among countries that have already piloted their own digital currency programs. Upon introducing the white paper, Himes said that "we

have seen other governments make real progress in establishing a central bank digital currency," and the "longer the United States government waits to embrace this innovation, the further we fall behind both foreign governments and the private sector." Notably, like the CBDC Paper issued by the Federal Reserve, the white paper found that a CBDC should be intermediated (i.e., not issued directly from the Federal Reserve to consumer) like our existing monetary system.

Federal Reserve Launches Pilot CBDC Program

In November 2022, the Federal Reserve, through the Federal Reserve Bank of New York, launched Phase II of its CBDC development, which encompasses a 12-week pilot program with the nation's largest banks. The Federal Reserve has yet to receive authorizing legislation from Congress or an executive order from the Biden administration to issue a CBDC. Thus, the pilot program seems at odds with the Federal Reserve's prior stance on the development of a U.S. CBDC—stating that it would not proceed with the issuance of a CBDC "without clear support from the executive branch and from Congress, ideally in the form of a specific authorizing law," in the CBDC Paper. This CBDC pilot program is intended to experiment with the concept of a regulated liability network and test the technical feasibility, legal viability, and business applicability of distributed ledger technology to settle the liabilities of regulated financial institutions through the transfer of central bank liabilities.

It is important to note that during Phase I of the CBDC development, the prototype for a central bank digital currency was developed. Phase I revealed blockchain-enabled, cross-border payments could be faster, simultaneous, and safer than legacy payments based on a distributed ledger infrastructure—a multi-ledger construct in which each currency was maintained on a separate ledger, operated by its respective simulated central bank.

In addition to the CBDC pilot program, the Federal Reserve, through the Federal Reserve Bank of Boston, launched an initiative, dubbed Project Hamilton, which is currently researching the development of a U.S. CBDC. On December 1, 2022, top Republican on the House Financial

Services Committee Patrick McHenry (R-NC) and Ranking Republican on the House Financial Services Subcommittee on Oversight and Investigations Emmer sent a letter to Federal Reserve Bank of Boston President Susan Collins about Project Hamilton. The letter suggested some firms participating in Project Hamilton may intend to use government resources from the project to design a CBDC with the intent to then sell those products to commercial banks. The letter asked about Project Hamilton’s funding and engagement with the private sector as it seeks to develop a CBDC, and how the Federal Reserve plans to address concerns regarding financial privacy and financial freedom. McHenry and Emmer were joined on the letter by House Financial Services Committee members Ann Wagner (R-MO), Ted Budd (R-NC), Bill Huizenga (R-MI), Andy Barr (R-KY), French Hill (R-AR), Anthony Gonzalez (R-OH), and Warren Davidson (R-OH).

Federal Regulatory Developments

FDIC Developments

Since 1934, the FDIC has insured deposits held in insured banks and savings associations. However, as collaborative ventures between FDIC-insured entities like federally chartered banks and non-FDIC insured entities like cryptocurrency exchanges continue to gain traction, the FDIC has become increasingly concerned with false and misleading

statements pertaining to FDIC deposit insurance. On August 19, 2022, the FDIC issued cease-and-desist notices to five companies that suggested crypto-related products were FDIC-insured. Notably, one company published an article on its website titled, “List of FDIC-Insured Crypto Exchanges,” although, as the FDIC noted in its letter, “FDIC insurance does not cover cryptocurrency.”

Additionally, due to safety and soundness, as well as consumer protection risks associated with cryptocurrencies, the FDIC has created a notification process for FDIC-insured entities that wish to engage in crypto-related activities. On April 7, 2022, the FDIC formalized this notification process by releasing a letter that requires FDIC-supervised institutions, prior to engaging in or if currently engaged in a crypto-related activity, to notify its regional FDIC director. The lack of definitional consistency around cryptocurrencies and crypto-related activities seemingly acted as the catalyst for the FDIC’s letter. And, to combat the potential risks linked to cryptocurrencies, the FDIC disclosed that it must review any crypto-related activity an insured entity proposes to engage in on an “individual basis.”

FTC Enforcement and Developments

Congress created the FTC to protect consumers from fraud and deception in the marketplace. Through its Section 5 powers under the FTC Act,



the FTC has broad authority to prohibit “unfair or deceptive acts or practices affecting commerce.” During 2022, the FTC issued numerous alerts to educate consumers on cryptocurrency scams and how to avoid them.

On June 3, 2022, the FTC released its “Consumer Protection Data Spotlight,” which indicated that consumers reported a total loss of \$329 million in Q1 2022 due to cryptocurrency scams. For comparison, during the entirety of 2021, consumers reported a total loss of \$680 million due to cryptocurrency scams. According to the FTC, cryptocurrencies are attractive to scammers because blockchain does not contain a “centralized authority to flag suspicious transactions and attempt to stop fraud before it happens,” and “most people are still unfamiliar with how crypto works.”

The FTC has determined that most cryptocurrency scams originate through an advertisement, post, or message on social media, but not all cryptocurrency scams are the same:

- **Investment Scams:** These scams entail a fraudster who promises a consumer that the fraudster can obtain quick and lucrative returns for the consumer if the consumer deposits his/her cryptocurrency with the fraudster and allows the fraudster to invest on the consumer’s behalf. Unfortunately, when the consumer “invests” his/her cryptocurrency with the fraudster, the consumer generally deposits his/her cryptocurrency into the fraudster’s digital wallet, and once obtained, the fraudster absconds with the consumer’s cryptocurrency never to be heard from again.
- **Romance Scams:** These scams involve a fraudster who attempts to build a relationship with a consumer under the guise of a fake social media profile that exudes wealth and luxury. Eventually, the fraudster begins to provide cryptocurrency investment tutorials to the consumer, and these tutorials ultimately end with the consumer sending his/her cryptocurrency to the fraudster.
- **Recovery Scams:** Caused by the crypto-related entities that prohibited consumers from withdrawing their cryptocurrency deposits due

to bankruptcy, these scams involve a fraudster who attempts to help a consumer recover cryptocurrency that has already been lost due to fraud.

In addition to cryptocurrency scams, the FTC has also expressed concerns over deceptive consumer representations in the digital asset industry. On May 11, 2022, the FTC issued a civil investigative demand (CID) to Bachi.Tech Corporation, the parent company of cryptocurrency exchange BitMart, in connection with a hack that occurred in December 2021 on BitMart’s platform and resulted in consumer loss of more than \$200 million. According to the FTC, at the time of the hack, BitMart’s website described itself as “the most trusted cryptocurrency platform that is 100% secure” and claimed to have an “advanced risk control system.”

OCC Enforcement and Developments

On April 21, 2022, the OCC issued a cease-and-desist consent order against Anchorage Digital Bank for failing to devise and implement an effective BSA/AML compliance program in violation of the BSA and its implementing regulations. During January 2021, the OCC conditionally approved Anchorage’s application for a national trust charter, making Anchorage the first federally chartered crypto bank in the United States. However, the OCC’s approval of Anchorage’s charter was contingent upon Anchorage’s agreement to enter into an operating agreement, which imposed certain BSA/AML requirements on Anchorage.

In its “Semiannual Risk Perspective Report” issued this year, the OCC disclosed that it “continues to approach crypto-asset products, services, and activities cautiously” considering the multitude of crypto-related entities that have filed for bankruptcy and the network effects of the contagion generated by their collective demise. According to the OCC, current crypto industry risk management practices concerning fraud and custodial services lack maturity, and algorithmic stablecoins, as well as asset-backed stablecoins, are susceptible to run risk. Therefore, the agency remains primarily focused on whether banks are “engaging in these activities in a safe, sound and fair manner.”

CFPB Enforcement

On November 22, 2022, the CFPB issued a decision denying Nexo Financial LLC's petition to modify a CID originally served on the company on December 1, 2021. At that time, Nexo Financial and its affiliates advertised a range of products, including interest-accruing accounts and lines of credit. In its petition, Nexo Financial argued that the CID should be modified to exclude Nexo's earn-interest product, an interest-bearing crypto lending product, because it fell under the SEC's purview and outside of the CFPB's jurisdiction. The CFPB denied the request and ordered a corporate representative to appear for oral testimony on December 19, 2022. According to the CFPB, Nexo Financial did not contend that the SEC has determined that the earn-interest product is a security or that Nexo was required to register the product with the SEC. "Nexo Financial is trying to avoid answering any of the [CFPB's] questions about the [e]arn [i]nterest [p]roduct (on the theory that the product is a security subject to SEC oversight) while at the same time preserving the argument that the product is not a security subject to SEC oversight. This attempt to have it both ways dooms Nexo Financial's petition from the start," stated CFPB Director Rohit Chopra in the decision. The CFPB's investigation into Nexo Financial marks its first investigation to determine whether a crypto firm is abiding by consumer protection laws.

On May 17, 2022, the CFPB announced an enforcement policy aimed at depository products that potentially mislead consumers to believe they are backed by the FDIC, reasoning that "issue has taken on renewed importance with the emergence of financial technologies—such as crypto-assets, including stablecoins—and the risks posed to consumers if they are lured to these or other financial products or services through misrepresentations or false advertising." The guidance emphasizes that: (1) misrepresenting the FDIC logo or name will typically be a material misrepresentation; (2) misrepresentation or misuse of the FDIC name or logo harms customers and puts them at significant risk of unexpected losses; and (3) misuse of the FDIC name or logo harms honest companies. The CFPB's guidance was issued in connection with the FDIC's adoption of a regulation

implementing a statutory provision that prohibits any person or organization from engaging in false advertising or misusing the name or logo of the FDIC and from making knowing misrepresentations about the extent or manner of FDIC deposit insurance. The CFPB's related announcement states that the "CFPB will exercise its authorities to ensure the public is protected from risks and harms that arise when firms deceptively use the FDIC logo or name or make deceptive misrepresentations about deposit insurance, regardless of whether those misrepresentations are made knowingly." Based on this announcement, it appears that the CFPB intends to step up enforcement and oversight for statements regarding FDIC insurance.

It is important to note CFPB Director Rohit Chopra's recent thoughts on cryptocurrency. Based on interviews this past year, it appears that he is primarily concerned with cryptocurrency payments. During a March 11, 2022 CNBC appearance, Director Chopra stated that digital assets are mostly used for "speculative trading purpose, but if [cryptocurrency] ever rides the rails of a big player, maybe like a big tech company, consumer use could dramatically grow and that is where [the CFPB] needs to look closely at consumer protection pieces." Subsequently, the CFPB "has ordered Apple, Google, Facebook" and others to provide the CFPB "with more information about what their plans are" for cryptocurrency, said Chopra. During his July 27, 2022 interview with *Law360*, Director Chopra reiterated his focus on payments, stating that cryptocurrency is "really looked at [] primarily through payments" by the CFPB, and "the primary focus, at least from the CFPB perspective, is around preparing for real-time payments." In his September 22, 2022 interview, Director Chopra stated he sees stablecoins as a rapid growth area that regulators will need to monitor for risks to the rest of the financial system. A "stablecoin, riding the rails of a dominant payments system or a mobile OS, I think that could create ubiquity very quickly," Chopra said, adding that issues around stablecoins, "are very much being thought through, but certainly not just by the CFPB."



FinCEN, Money Services Businesses, and Convertible Virtual Currencies

By way of background, FinCEN regulates money services businesses under the BSA. Money transmitters are a type of money services business subject to FinCEN's authority. Money transmitters are entities that engage in money transmission services or are otherwise "engaged in the transfer of funds." The term "money transmission services" is defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." FinCEN has given broad meaning to two phrases embedded in the "money transmission services" definition: (1) "or other value that substitutes for currency"; and (2) "by any means." When read together, these phrases stand for the proposition that the term "money transmission services" encompasses not only the transmission of "currency"—which the BSA defines as "the coin or paper money of the United States or any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance"—but also the transmission of any currency-type equivalents like a "convertible virtual currency," which FinCEN has defined as "a medium of exchange that operates like a real currency in some environments but does not have all the attributes of real currency and is not considered legal tender in any jurisdiction."

On March 18, 2013, FinCEN issued interpretive guidance, clarifying the circumstances under which FinCEN would apply money services business status to persons engaged in using, exchanging, accepting, or transmitting convertible virtual currencies (2013 VC Guidance). In the 2013 VC Guidance, FinCEN stated that entities that accept and transmit anything of value that substitutes for a currency, including convertible virtual currencies, and are not exempt from money services business status are money transmitters. Similarly, on May 9, 2019, FinCEN issued interpretive guidance, reiterating that "persons accepting and transmitting value that substitutes for currency, such as virtual currency, are money transmitters" and are required to register with FinCEN as a money services business and comply with AML program, recordkeeping, monitoring, and reporting requirements of the BSA, including the filing of suspicious activity reports and currency transaction reports (2019 VC Guidance).

FinCEN v. Larry Dean Harmon d/b/a Helix

On October 19, 2020, FinCEN assessed a civil money penalty in the amount of \$60 million against virtual currency "mixer" Helix and its owner Larry Dean Harmon for failing to register as a money services business, failing to implement an effective AML program, and failing to file suspicious activity reports in violation of the BSA and its implementing regulations.

FinCEN alleged that Harmon failed to register Helix as a money services business from its inception in June 2014 through its wind down in December 2017. Furthermore, from July 2017 through February 2020, FinCEN alleged Harmon began operating another virtual currency “mixer” called Coin Ninja LLC, but Harmon failed to register Coin Ninja as a money services business. Critically, from June 2014 through February 2020, Harmon operated two unregistered money services businesses that neither developed AML programs nor filed any suspicious activity reports despite the frequent engagement both platforms received from darknet marketplaces and other illicit actors. FinCEN concluded that Helix conducted over 1,225,000 transactions for customers and was associated with virtual currency wallet addresses that sent or received more than \$311 million.

On October 19, 2022, the U.S. DOJ, on behalf of FinCEN, filed a lawsuit in the District of Columbia against Harmon. The DOJ’s lawsuit seeks to recover the \$60 million civil penalty FinCEN imposed on Harmon in 2020.

FinCEN v. Bittrex, Inc.

On October 11, 2022, FinCEN assessed a civil money penalty in the amount of \$29,280,829.20 against cryptocurrency exchange Bittrex, Inc. (Bittrex) for failing to implement a sufficient AML program and for failing to file suspicious activity reports over an extended period in violation of the BSA and its implementing regulations. FinCEN’s civil enforcement action against Bittrex was part of a global resolution with OFAC, which alleged that Bittrex committed 116,421 violations of sanctions programs by failing to prevent persons in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its platform to engage in approximately \$263,451,600.13 worth of virtual currency-related transactions. OFAC discovered that from August 2015 through October 2017, Bittrex had not developed an internal sanctions compliance program. More specifically, when Bittrex did devise and implement a sanctions compliance program in October 2017, OFAC alleged that Bittrex’s sanctions compliance program screened only for hits against OFAC’s Specially Designated Nationals (SDN) List

and did not screen customers or transactions for a nexus to a sanctioned jurisdiction.

At its peak, Bittrex had averaged an approximate transaction volume of 24,000 transactions per day. However, Bittrex’s AML program solely consisted of two employees who were responsible for manually reviewing thousands of transactions for suspicious activity. In the consent order, FinCEN described Bittrex’s manual transaction review process as “demonstrably ineffective.” In addition to Bittrex’s insufficient AML program, FinCEN alleged that Bittrex impermissibly operated as a money services business for three years before filing its first suspicious activity report. Notably, in August 2015, Bittrex applied to the New York State Department of Financial Services (NYDFS) to obtain New York’s elusive BitLicense, which is required to engage in “virtual business currency activity” in the state of New York. Nevertheless, on April 10, 2019, the NYDFS denied Bittrex’s application for a BitLicense for the same reason that prompted FinCEN’s enforcement action against the cryptocurrency exchange in 2022, i.e., purportedly obvious deficiencies existed in Bittrex’s BSA/AML/OFAC compliance program.

Looking Ahead

As reflected by the substantial civil penalty imposed on Bittrex, insufficient AML/CFT compliance is poised to remain the predominant basis for enforcement actions filed against crypto-related entities in 2023. For the time being, FinCEN and many other federal and state regulators perceive cryptocurrencies as a technological innovation that is commonly used to anonymously perpetrate a wide variety of cybercrime. Therefore, a financial institution seeking to integrate cryptocurrency transactions into its business model should critically conduct a comprehensive risk assessment of its operations, customers, and geographies to devise a reasonable AML compliance program containing sufficient suspicious activity detection controls, specialized BSA/AML employee training programs, and automatic transaction filtering technology to prevent inadvertent execution of transactions for individuals domiciled in OFAC-sanctioned jurisdictions.

OFAC's Authority, Financial Privacy, and Smart-Contract Sanctions

In 2022, OFAC sanctioned two cryptocurrency “mixers” for processing transactions executed by individuals on OFAC’s SDN List and settled with one cryptocurrency exchange for processing transactions in violation of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. § 560.204.

Cryptocurrency transactions are commonly recorded on a publicly distributed ledger (i.e., blockchain), and the movement of cryptocurrencies from one party to another party remains visible to anyone. To anonymize cryptocurrency transactions, a person may rely upon a cryptocurrency “mixer.” A cryptocurrency “mixer” leverages smart-contract technology, which entails self-executing lines of computer code that automate finality of a transaction when certain predetermined conditions are met. Practically speaking, a user sends the cryptocurrency he/she would like anonymized to a smart contract. Once the mixing process is complete, the user may withdraw the cryptocurrency he/she initially deposited to the smart contract, and upon return, the transactional origins of the user’s cryptocurrency will be difficult to determine. The smart-contract mixer obfuscates the public origin and public destination associated with cryptocurrency transactions to sever the link between a sender and a recipient of cryptocurrency. Smart contracts are an integral component of DeFi, which seeks to disintermediate traditional financial markets through autonomous execution of transactions.

For the time being, FinCEN and many other federal and state regulators perceive cryptocurrencies as a technological innovation that is commonly used to anonymously perpetrate a wide variety of cybercrime.

Blender.io and Tornado Cash

On August 8, 2022, OFAC sanctioned Tornado Cash, a smart-contract cryptocurrency mixer, for allegedly assisting The Lazarus Group, a Democratic People’s Republic of Korea state-sponsored hacking group, in laundering more than \$7 billion worth of cryptocurrency. OFAC sanctioned Tornado Cash under Executive Order 13694. Executive Order 13694 enables OFAC to impose sanctions on “individuals” and “entities” determined to be responsible for or complicit in malicious cyber-enabled activities likely to be a significant threat to the national security of the United States. In effect, OFAC’s designation of Tornado Cash prohibited U.S. persons from engaging in transactions involving the identified Tornado Cash mixing smart-contract addresses and froze movement of preexisting cryptocurrency deposits present in Tornado Cash mixing smart contracts at the time of OFAC’s designation. In addition to adding Tornado Cash to the SDN List, OFAC also added 38 unique cryptographic addresses associated with Tornado Cash, many of which corresponded to mixing smart contracts offered on Tornado Cash’s platform. This designation is unprecedented. It marks the second time OFAC has sanctioned a cryptocurrency “mixer” and the first time OFAC has sanctioned a decentralized cryptocurrency “mixer” whose functionality depends exclusively on smart contracts dissociated from the original developers of the mixer and can be run in perpetuity.

On May 6, 2022, under Executive Order 13694, OFAC sanctioned Blender.io, a centralized cryptocurrency “mixer” that provided Bitcoin mixing services to users. As it did with Tornado Cash, OFAC added various unique cryptographic Bitcoin addresses associated with Blender.io to the SDN List. However, a key operational distinction existed between Blender.io and Tornado Cash. Blender.io offered a service, “natural persons” controlled the Bitcoin addresses associated with Blender.io, and those persons could dictate which users would be allowed to utilize Blender.io’s mixing services. As Blender.io was a blockchain service offered and managed by natural persons, the broader cryptocurrency community did not oppose OFAC’s usage of its sanctioning authority against Blender.io. Conversely, the decentralized nature of Tornado

Cash's operations has generated spirited protests by stakeholders in the digital asset industry.

On September 8, 2022, six individuals filed a lawsuit, challenging OFAC's sanctioning of Tornado Cash. The lawsuit alleged that OFAC's sanction authority under Executive Order No. 13694 is limited to "individuals" and "entities," and Tornado Cash, as an open-source software tool devoid of a formal governing body, does not fall within the definitional scope of either of these terms.

On September 13, 2022, seemingly in response to the lawsuit filed five days earlier, OFAC issued interpretive guidance in the form of responses to frequently asked questions (FAQs). In FAQ 1076, OFAC clarified that U.S. persons are prohibited from engaging in transactions with Tornado Cash, but U.S. persons are not prohibited from copying Tornado Cash's open-source code and making it available online for others to view. In FAQ 1079, OFAC noted that individuals who deposited cryptocurrency to a Tornado Cash mixing contract prior to Tornado Cash's designation on August 8, 2022, could request a license from OFAC to withdraw his/her cryptocurrency provided that the underlying transaction "did not involve other sanctionable conduct." In FAQ 1095, which OFAC issued on November 8, 2022, OFAC stated that the term "person" as defined by Executive Order 13722 and Executive Order 13694 encompasses a "partnership, association, joint venture, corporation, group, subgroup, or other organization." Here, OFAC concluded that Tornado Cash's organizational

structure, which consisted of its founders and the Tornado Cash Decentralized Autonomous Organization (DAO), constituted an organization that could be designated under the International Emergency Economic Powers Act (IEEPA).

OFAC's counteracting guidance suggests that the federal agency is aware of the potentially militating questions sparked by its designation of Tornado Cash. For example, should an individual who deposited cryptocurrency to a Tornado Cash mixing contract, but did not engage in any illicit activity, be precluded from withdrawing his/her cryptocurrency or from otherwise engaging the Tornado Cash platform? Moreover, do the functional aspects of a particular open-source software, which may enable a user to facilitate money laundering, alone render the software subject to OFAC sanctions? In its 2019 VC Guidance, FinCEN distinguished that an "anonymizing *software* provider," (i.e., Tornado Cash) as opposed to an "anonymizing *service* provider" (i.e., Blender.io) is not a money transmitter because "suppliers of tools (communications, hardware, or software) that may be utilized in money transmission ... are engaged in trade *and not* money transmission." Although OFAC is not bound by FinCEN's interpretive guidance, OFAC and FinCEN, as divisions of the U.S. Treasury tasked with ridding the U.S. economy of money laundering and terrorist financing, may look to promulgate similar outlooks on the *decentralized* cryptocurrency "mixer" issue in the future to maintain regulatory continuity.



Payward, Inc. d/b/a Kraken

On November 28, 2022, OFAC settled with cryptocurrency exchange Kraken in the amount of \$362,158.70 for its apparent violations of the Iranian Transactions and Sanctions Program (31 C.F.R. § 560.204), which generally prohibits U.S.-based entities from supplying technology to Iran.

Kraken's internal controls prevented users from opening an account on its platform, while located in a jurisdiction subject to sanctions; however, Kraken's controls did not include "IP address blocking," which would have insulated the exchange from users who *opened* accounts outside of sanctioned jurisdictions and subsequently accessed those accounts (and transacted on Kraken's platform) from a sanctioned jurisdiction. Therefore, OFAC discovered that between October 12, 2015, and June 29, 2019, Kraken processed 826 transactions in the total amount of \$1,680,577.10 on behalf of users who had circumvented Kraken's controls by initially opening an account in a jurisdiction not subject to OFAC sanctions.

OFAC calculated that Kraken's conduct warranted a colossal maximum civil monetary penalty of \$272,228,964.00. But due to Kraken's self-disclosure of the violations, its agreement to spend an additional \$100,000 to invest in sanctions compliance controls and training and other significant remedial actions, OFAC observed that the settlement amount of \$362,158.70 was appropriate.

The civil money penalty OFAC required Kraken to pay pales in comparison to the civil money penalty OFAC imposed on Bittrex (discussed above), although both enforcement actions involved issues concerning inadequate geolocation tools. Still, Bittrex operated without an effective sanctions compliance program for approximately two years and processed almost 120,000 violative transactions, totaling more than \$260 million, and these factors seemed to have greatly contributed to the civil monetary penalty OFAC imposed on it.

Looking Ahead

Whether OFAC may permissibly subject computer code to its sanctioning authority is a question for

the courts. Those who oppose OFAC's designation of Tornado Cash contend that open-source software has neither directors nor officers and that an individual's usage of the software, which theoretically does not have to involve illicit activity, cannot be curtailed by a natural person. Presumably, the lack of an identifiable arbiter of the mixing smart contracts themselves is the precise variable that drove OFAC's designation of Tornado Cash. But it can be surmised that OFAC's designation of Tornado Cash is only the beginning of the U.S. Treasury's effort to integrate digital assets and decentralized blockchain protocols into the current financial regulatory framework to which traditional financial institutions are presently subject. Importantly, FAQ 1021, which OFAC issued on March 11, 2022, prescribes that all U.S. financial institutions are required to comply with OFAC regulations, regardless of whether a transaction is denominated in traditional fiat currency or virtual currency. Given these efforts, compliance procedures—particularly as they relate to the question of whether transactions facilitated on a platform involve an OFAC-designated party or parties domiciled in OFAC-designated jurisdictions—may likely become more important to financial institutions seeking to integrate digital asset transactions into their business models.

State-Level Enforcement

Earn-Interest Products

In 2015, the NYDFS finalized rules relating to the BitLicense regime, which is currently the most comprehensive regulatory and oversight framework imposed on crypto-related entities based in the United States. In New York, before a crypto-related entity engages in any activity involving the state of New York or a New York resident, the entity must obtain a BitLicense from the NYDFS. Although New York infrequently approves applications for BitLicenses, entities that have obtained them are subject to a strict array of requirements relating to compliance, custody, capital, cybersecurity, consumer complaints, and consumer disclosures. In mid-November 2022, while discussing the collapse of cryptocurrency exchange FTX, NYDFS Superintendent Adrienne Harris applauded the

rigor of New York's BitLicense framework. FTX had submitted a BitLicense application, which the NYDFS had not approved. FTX was therefore prohibited from engaging New York residents, who were, as a result, less affected than they might otherwise have been when FTX filed for Chapter 11 bankruptcy protection on November 11, 2022.

Although the state of New York has long been heralded as a respected crypto regulator, other states, like California, have seemingly followed in the steps of the SEC and adopted a more hands-on approach to supervising crypto-related entities, particularly with respect to offerings of interest-bearing crypto deposit accounts.

Over a year ago, on September 1, 2021, the SEC issued a Wells notice to Coinbase, Inc. The Wells notice informed Coinbase that the SEC intended to file a civil enforcement action against Coinbase if the company launched its proposed LEND program, which sought to allow customers to earn interest on customer crypto deposits held on Coinbase's exchange platform. As a result of the Wells notice, Coinbase decided not to move forward with the LEND program.

This past year, the California Department of Financial Protection and Innovation (DFPI) has filed three enforcement actions against crypto-related entities that offered and sold interest-bearing cryptocurrency accounts. An interest-bearing cryptocurrency account enables an investor to lend digital assets to the crypto-related entity that offers the account in exchange for the entity's promise to provide variable monthly interest payments on the consumer's crypto deposits. In each of those actions, the DFPI alleged that the provision of interest-bearing cryptocurrency accounts to consumers constituted the unregistered sale of securities. The crypto-related entities involved in the actions brought by the DFPI were BlockFi, Inc., Celsius Network LLC, and Voyager Digital Holdings, Inc. Notably, before Voyager filed for bankruptcy protection on July 5, 2022, and before Celsius filed on July 13, 2022, they had prohibited consumers from withdrawing their crypto-asset deposits from their respective interest-bearing cryptocurrency accounts. Furthermore, on November 11, 2022, the DFPI announced its decision to suspend BlockFi's

California Financing Law license for 30 days due to BlockFi's decision to "pause client withdrawals."

State regulators have been looking into whether interest-bearing cryptocurrency accounts create counterparty risk as investments and should be subject to the disclosure requirements of state securities laws. For instance, on September 22, 2022, the DFPI announced that it joined Vermont, Oklahoma, South Carolina, Kentucky, New York, Washington, and Maryland in filing cease-and-desist orders against Nexo, Inc., a cryptocurrency lender, for its provision of interest-bearing cryptocurrency accounts to consumers without registering as a securities broker or dealer as required by state law. On September 22, 2022, in a press release addressing the multistate enforcement effort against Nexo, New York Attorney General Letitia James asserted that "[c]ryptocurrency platforms are not exceptional; they must register to operate just like other investment platforms." More notably, on November 29, 2022, the Texas State Securities Board (TSSB) served a notice of hearing on Sam Bankman-Fried, former CEO of bankrupt cryptocurrency exchange FTX, to provide testimony at an administrative hearing scheduled to take place in 2023. Like many of the crypto-related entities discussed above, FTX offered its customers an interest-bearing cryptocurrency deposit product that the TSSB alleged were "investment contracts, evidences of indebtedness, and notes" that are regulated as securities under Texas law.

Relevant State-Level Developments

This year, as the broader digital asset industry awaits regulatory clarity from the federal government, many states have taken matters into their own hands, which has led to divergent approaches to integrating digital assets and blockchain technology into existing state-level legal frameworks.

California: On September 23, 2022, California Governor Gavin Newsom vetoed A.B.2269, better known as the Digital Financial Assets Law. Like the NYDFS' BitLicense standard, the Digital Financial Assets Law would have required digital asset-related entities to first obtain a license from the DFPI prior to engaging in "digital financial

asset business activity” in the state of California. Governor Newsom considered the bill “premature” and cited to Executive Order N-9-22, which he issued on May 4, 2022, to reiterate his desire to establish a digital asset regulatory framework in harmony with the forthcoming federal digital asset regulatory framework.

Connecticut: On July 20, 2022, the Connecticut Department of Banking issued guidance, clarifying that Connecticut money transmission law encompasses the transfer of “monetary value,” which Connecticut law defines as a “medium of exchange, whether or not redeemable in money.” Further, the guidance confirmed that the term “monetary value” includes “virtual currency,” and to the extent that persons take possession or control of virtual currency belonging to another person, or transmit or receive virtual currency for another person, those persons may be required to acquire a money transmission license.

District of Columbia: On August 8, 2022, the District of Columbia Department of Insurance, Securities, and Banking issued a bulletin, notifying industry participants of its position that transactions involving the transmission, storing, or provision of custodial services of Bitcoin and other virtual currencies from consumers via kiosks, mobile applications, and online transactions constitute “money transmission.” Therefore, entities that engage in these practices must obtain a money transmitter license to operate in the District of Columbia.

Florida: On May 12, 2022, Florida enacted CS/HB 273, which broadened Florida’s money transmission law by defining “virtual currency” and clarifying the category of persons required to obtain a money transmitter license. The bill’s definition of “virtual currency” is expansive and includes any “medium of exchange in electronic or digital format that is not currency.” The bill went into effect on January 1, 2023.

Hawaii: On June 17, 2022, Hawaii enacted SB 2695, which creates a blockchain and cryptocurrency task force. The task force must submit a report of its findings and recommendations to the legislature by the time frame established in SB 2695.

Idaho: On March 31, 2022, Idaho enacted the Digital Asset Act. The bill amends Title 28 of the Idaho Code, which governs commercial transactions generally, to include a new chapter dedicated to regulation of digital assets. Idaho’s bill, which became effective on July 1, 2022, is multifaceted:

- It distinguishes digital securities and virtual currencies, the latter of which do not constitute securities under Idaho law;
- It defines “control,” or custody of digital assets, to encompass automated transactions facilitated by “smart contracts” and circumstances where a party has possession of the cryptographic private key associated with a particular digital asset; and
- It incentivizes a secured party to perfect its security interest in digital assets by control instead of through filing a financing statement.

Iowa: On June 13, 2022, Iowa enacted HF 2443, which: (1) amended Iowa’s Uniform Electronic Transactions Act to delete reference to distributed ledger technology; and (2) added a new section to Iowa law, addressing the legal effect of distributed ledger technology and smart contracts. The new section states that a record, signature, or contract shall not be denied legal effect or enforceability solely because it was created, generated, sent, signed, adopted, communicated, received, recorded, or stored by means of distributed ledger technology or a smart contract.

Missouri: On June 16, 2022, Missouri enacted HB 1472, which amended Missouri’s money laundering law to include cryptocurrency, thus making it a criminal offense of money laundering if a person engages in specified financial transactions that involve cryptocurrency.

New Hampshire: On June 28, 2022, New Hampshire enacted HB 1503, which adopted the Uniform Commercial Code Article 12 definition of “controllable electronic records,” which are defined as “a record stored in an electronic medium that can be subject to control under Section 12-105...” The term “controllable electronic records” encompasses virtual currencies, which live electronically on blockchain. Under the amended code, a security interest in a controllable electronic

record may now be perfected by control if a system in which the electronic record is recorded gives the person (1) the ability to enjoy substantially all the benefits from the electronic record and the ability to transfer control of the electronic record to another person; and (2) enables the person to self-identify in any way, including by way of cryptographic key, as having the previously mentioned abilities. As virtual currencies are transferred on blockchain through smart-contract technology, this language suggests that security interests in virtual currencies may be perfected by simply demonstrating that the virtual currency at issue is linked to the person's public wallet address, which can be examined on blockchain.

New York:

- On December 1, 2022, the NYDFS announced a proposed regulation that would enable the agency to impose supervisory costs on licensed virtual currency businesses operating within the state of New York. The proposed regulation is subject to a 10-day preproposal comment period that began on December 1, 2022, which will be followed by a 60-day comment period upon its publication in the State Register.
- On December 15, 2022, the NYDFS issued guidance, reminding all New York banking organizations, as well as all branches and agencies of foreign banking organizations that have received licenses from the NYDFS, that they are expected to seek approval from the NYDFS prior to engaging in new or significantly different virtual currency-related activity. Generally speaking, New York-state chartered banks are exempted from New York's BitLicense requirement, but these organizations must obtain approval from the NYDFS superintendent to engage in virtual currency business activity.

Ohio: On September 1, 2022, the Ohio Department of Commerce Division of Financial Institutions issued Interpretive Guidance 2022-01, clarifying that "a person engaged in the buying or selling of cryptocurrency as a business qualifies as a money transmitter" under the Ohio Money Transmitters Act (OMTA). According to the guidance, an entity's provision of certain crypto-related services to Ohioans will require the entity to obtain a money transmitter license under the OMTA:

- Persons operating cryptocurrency kiosks or cryptocurrency ATMs;
- Persons operating an exchange platform who facilitate the transfer of virtual currency or fiat;
- Persons providing cryptocurrency storage via a hosted wallet; and
- Persons providing payment processing services involving virtual currency.

Virginia: On April 11, 2022, Virginia enacted HB 263, which became effective on July 1, 2022. The new law permits Virginia-chartered banks to offer digital asset custody services to its customers, so long as the bank has "adequate protocols in place to effectively manage risks and comply with applicable laws." Notably, the law provides that "[t]he owner of virtual currency holds cryptographic keys associated with the specific unit of virtual currency in a digital wallet, which allows the rightful owner of the virtual currency to access and utilize it."

Washington: On March 30, 2022, Washington enacted SB 5544, creating the Washington Blockchain Work Group. The state of Washington established the group to examine potential applications for blockchain technology, such as computing, banking and other financial services, the real estate transaction process, health care, supply chain management, higher education, and public recordkeeping.

CYBERSECURITY AND PRIVACY

Authors: Molly DiRago, Ronald I. Raether, Sadia Mirza, Graham T. Dean, Robyn W. Lin, Alexandria Pritchett, Edgar Vargas, Whitney L. Shephard, Natasha E. Halloran

Legislation

Federal Legislation

In 2022, federal data privacy legislation made an unprecedented level of progress. The primary focus of these efforts was the [American Data Privacy and Protection Act](#) (ADPPA), which was introduced on June 21 with bipartisan support. The ADPPA would establish a national standard to protect consumer data privacy, impose obligations on covered entities, and allow for federal, state, and individual enforcement. The bill would also establish a new Bureau of Privacy at the Federal Trade Commission (FTC) as the regulator to enforce the bill. Notably, the ADPPA would preempt existing comprehensive state privacy laws, including the California Consumer Privacy Act (CCPA), [despite](#) objections from the California Privacy Protection Agency (CPPA). Although the ADPPA was not adopted in 2022, it provides valuable insight on the direction the federal government's potential regulations will take in 2023.

Dozens of narrower privacy bills were also introduced during the 2022 legislative session. Many of these laws were limited to single topics, such as protecting health data, limiting the data collected by internet-connected automobiles, and governing data brokers online. Examples include the Stop Commercial Use of Health Data Act, and the Safeguarding Privacy in Your Car Act of 2022.

The success of federal privacy legislation in 2023 will likely be driven in large part by developments at the state level, as the increasingly complex patchwork of requirements further fuels the efforts of those calling for federal preemption.

State Legislation

In 2022, comprehensive privacy legislation was considered in 27 state legislatures. While the majority of these bills failed, Utah and Connecticut successfully passed privacy laws largely based on the Virginia Consumer Data Privacy Act (VCDPA).

In many respects, these results mirror 2021, when about half of state legislatures considered comprehensive privacy laws, and Virginia and Colorado ultimately adopted such laws.

Utah

On March 24, Governor Spencer J. Cox signed the Utah Consumer Privacy Act (UCPA), making Utah the fourth state in the country to adopt a comprehensive privacy law. The UCPA is set to take effect on December 31, 2023, and this law's substantive requirements closely mirror the VCDPA. However, unlike the VCDPA, the UCPA does not provide consumers the right to correction, and consumers do not have the right to appeal in instances where a data subject request is denied. The UCPA includes broad exemptions for businesses and data subject to federal sector-specific privacy regimes, and all enforcement will be carried out by the Utah Attorney General. For more information on the UCPA, click [here](#).

Connecticut

On May 10, the [Connecticut governor](#) signed [An Act Concerning Personal Data Privacy and Online Monitoring](#) into law, making Connecticut the fifth state in the country to enact a comprehensive privacy regime. This legislation closely resembles the laws adopted in Virginia and Colorado, and will take effect on July 1, 2023. The Connecticut law does not include a private right of action and provides a temporary 60-day right to cure that sunsets on December 31, 2024. For more information on Connecticut's Act Concerning Personal Data Privacy and Online Monitoring, click [here](#).

Virginia

Multiple amendments to the [VCDPA](#) were passed during the 2022 legislative session. The first set of amendments established a new exception to the VCDPA's right to delete, applicable when personal data is collected from a source other than the

consumer. Under this new exception, data may be considered deleted if: (1) a minimal record of the deletion request is retained for the exclusive purpose of ensuring the consumer's data is/ remains erased; or (2) the consumer is opted out of all nonexempt data processing activities (e.g., targeted advertising and sales). The second set of amendments eliminates the VCDPA's "Consumer Privacy Fund" and diverts all funds collected under this law to the state treasury's Consumer Advocacy, Litigation, and Enforcement Revolving Trust Fund. These amendments also redefine "nonprofit organizations" to include tax-exempt political organizations.

California

On August 31, California's legislature ended its 2022 session without extending the CCPA employee and business-to-business (B2B) personal information exemptions. In the absence of a special legislative session, these exemptions will expire on January 1, 2023. This means that businesses subject to the CPRA must extend their compliance programs to include the personal information of employees and B2B contacts. For implementation tips, click [here](#).

On September 15, California Governor Gavin Newsom signed Assembly Bill 2273—the [California Age-Appropriate Design Code Act \(ADCA\)](#)—into law. Inspired by the United Kingdom's (U.K.) Age-Appropriate Design Code, the ADCA will impose data privacy requirements on businesses that provide "an online service, product or feature likely to be accessed by a child." Unlike the federal Children's Online Privacy Protection Act (COPPA), which governs the use and sharing of children's data once it has been collected, ADCA goes further by requiring businesses to consider children during the development of a product or service. This includes considering the different needs of a child based on their age. The ADCA will take effect on July 1, 2024. For more information, click [here](#).

Colorado

On October 10, Colorado published [draft regulations](#) for the Colorado Privacy Act (CPA). Notably, the

draft rules exempt biometric information from the definition of "publicly available information," further clarify bona fide loyalty programs, and add greater detail to unified opt-out mechanism requirements. A public hearing is scheduled for February 1, 2023, at which the agency will accept written and oral testimony in support of, or in opposition to, the proposed rule. After the hearing, the public will no longer be able to offer comments on the draft rules unless there are modifications to the language such that the Attorney General's office would be required to start the process over. The office will have 180 days after the February 1 hearing to file adopted rules with the secretary of state for publication in the Colorado Register. The CPA requires the promulgation of rules by July 1, 2023, which is when the CPA goes into effect.

Biometrics

In 2022, biometric privacy legislation was considered in 15 state legislatures. Despite these efforts, no meaningful biometric privacy law was adopted in 2022. While some of this legislation focused on updating existing biometric privacy laws, much of it attempted to establish a comprehensive biometric privacy regime similar to Illinois' Biometric Information Privacy Act (BIPA). Currently, only Illinois, Texas, and Washington have enacted biometric laws, and only BIPA provides individuals with a private right of action. While California's Consumer Privacy Act (CCPA) covers the protection of biometric data, the act only provides a private right of action where the information was involved in an unauthorized exposure as a result of the business's failure to implement and maintain reasonable security procedures and the business's failure to take certain steps after receiving a consumer request.

State and Federal Enforcement

Federal Enforcement

FTC Rulemaking

On August 11, the FTC published an advance notice of proposed rulemaking (ANPR) aimed at commercial surveillance and data security.



The FTC invited comments on whether it should undertake rulemaking on the ways companies collect, aggregate, protect, use, analyze, and retain consumer data. The FTC also sought information on the ways companies transfer, share, sell, or otherwise monetize data using unfair or deceptive methods.

The ANPR highlights the concerns of the FTC over commercial surveillance practices, automated systems that analyze data collected by companies, and the increasing use of dark patterns or marketing “to influence or coerce consumers into sharing personal information.” In its announcement, the FTC noted that its past work in exercising its authority under the FTC Act suggests that the enforcement of the FTC Act on its own may not be sufficient to protect consumers. The questions raised by the FTC cover a wide range of topics, including the potential harms to consumers and children; the relative costs and benefits of any current practice, as well as those for any responsive regulation; algorithmic error, algorithmic discrimination, and the pros and cons of automated decision-making; the effectiveness and administrability of consumer consent to companies’ commercial surveillance and data security practices; and notice, transparency, and disclosure.

The ANPR included a deadline for filing comments by October 21, but extended the deadline to November 21 to provide adequate time to respond to the questions raised by the ANPR, and to help facilitate the creation of a more complete record. Issuing this ANPR is the beginning of the FTC rulemaking process, but its broad scope provides little insight into what formal rule or rules the FTC might formally adopt in the future.

GLBA Safeguards Update

The FTC [extended](#) the deadline for financial institutions regulated by the Gramm-Leach-Bliley Act (GLBA) to comply with certain provisions of its Final Rule, which amended the Standards for Safeguarding Customer Information. The deadline was extended by six months and is now June 9, 2023. The FTC extended the deadline, in part, based on an August 5 letter from the Small Business Administration (SBA), in which the SBA noted the shortage of qualified personnel to implement information security programs and supply chain issues that may lead to delays in obtaining necessary equipment for upgrading security systems.

In 2021, the FTC [announced](#) the updated rule as it applied to covered financial institutions. The Final Rule provides guidance on developing and implementing information security programs, such as access controls, authentication, and encryption.

Broader Definition of “Financial Institution”

Notably, the Final Rule expands the definition of “financial institution” to include entities engaged in activities that the Federal Reserve Board determines to be incidental to financial activities now subject to the FTC’s enforcement authority under the Safeguards Rule. For example, an automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days would qualify as a financial institution for its leasing business. The Final Rule explains, for this example, that leasing personal property on a nonoperating basis with an initial lease term of at least 90 days is a financial activity enumerated in the list of permissible nonbanking activities under 12 CFR 225.28 and referenced in the Bank Holding Company Act.

Additional examples of newly considered “financial institutions” include businesses that regularly wire money to and from consumers; retailers that extend credit by issuing their own credit cards directly to consumers; and check cashing businesses. A business only falls within the expanded definition of “financial institution” if it is “significantly” engaged in activities incidental to financial activities. For example, a retailer that accepts cash, check, or credit as a form of payment; a merchant that allows an individual to “run a tab”; and a grocery store that allows individuals to cash a check would not be considered to “significantly” engage in activities incidental to financial activities and therefore would not fall within the expanded definition.

By defining “financial institution” and enumerating examples, rather than incorporating by reference to the Privacy of Consumer Financial Information Rule (Privacy Rule) promulgated under the GLBA, the Final Rule allows readers to understand the requirements of the Safeguards Rule without having to refer separately to the Privacy Rule.

Requirements for Financial Institutions

Under the Final Rule, covered financial institutions—which now include nonbank lenders, mortgage brokers, consumer reporting agencies, etc.—will be required to develop, implement, and maintain a more comprehensive information security program. The information security program must be written and include, among other things, the following elements:

- **Designation of a Qualified Individual:** In its comprehensive written information security program, a covered financial institution must designate a qualified individual (Qualified Individual) responsible for overseeing and implementing the information security program. The Qualified Individual may be an employee, an affiliate, or a service provider. If the Qualified Individual is a service provider or an affiliate, he/she is subject to additional requirements.
- **Risk Assessments:** A covered financial institution must conduct risk assessments. Risk assessments must be written and include, among other things, criteria for the assessment of identified security risks, confidentiality, and integrity of information systems. A covered financial institution must design and implement safeguards to control the risks identified through such risk assessments.
- **Encryption and Multifactor Authentication:** A covered financial institution must encrypt all customer information held or transmitted both in transit over external networks and at rest. In the event that such encryption is infeasible, the covered financial institution may instead secure the customer information through an effective alternative control reviewed and approved by the Qualified Individual. In addition, a covered financial institution must implement multifactor authentication (or a reasonably equivalent or more secure method of access control approved in writing by the Qualified Individual) for any individual accessing any information system.
- **Periodic Penetration Testing and Vulnerability Assessments:** A covered financial institution must conduct annual penetration testing determined each year based on relevant identified risks (in accordance with the risk assessment). In addition,

at least every six months, a covered financial institution is required to conduct vulnerability assessments, which must include systemic scans or reviews of information systems reasonably designated to identify publicly known security vulnerabilities (based on the risk assessment).

- **Oversight of Service Providers:** A covered financial institution must oversee service providers, including requiring service providers by contract to implement appropriate safeguards for customer information and periodically assessing service providers.
- **Annual Report to the Board of Directors:** At least annually, the Qualified Individual is required to report in writing to a covered financial institution's board of directors or equivalent governing body (or in the absence of an equivalent governing body, a senior officer responsible for the information security program) on the overall status of the information security program and material matters related to such program.

The success of federal privacy legislation in 2023 will likely be driven in large part by developments at the state level, as the increasingly complex patchwork of requirements further fuels the efforts of those calling for federal preemption.

The Final Rule exempts financial institutions that maintain customer information concerning fewer than 5,000 consumers from the above requirements to implement a written risk assessment, conduct annual penetration testing and biannual vulnerability

assessments, and to compel the Qualified Individual to report annually to the board of directors or equivalent governing body.

Executive Order on Implementing EU-U.S. Data Privacy Framework

On October 7, President Biden signed an [executive order](#) on Enhancing Safeguards for United States Signals Intelligence Activities. The order directs the steps the United States will take to implement its commitments under the European Union-U.S. Data Privacy Framework, which was announced by President Biden and European Commission President von der Leyen in March. Specifically, the order adds further safeguards for U.S. signals intelligence activities; mandates handling requirements of personal information collected through signals intelligence activities and extends the responsibilities of legal, oversight, and compliance officials to ensure that appropriate actions are taken to remediate incidents of noncompliance; requires U.S. Intelligence Community (IC) agencies to update their policies and procedures to reflect the new privacy and civil liberties safeguards contained in the order; and creates a multilayer mechanism for qualifying individuals to obtain independent and binding review and redress of claims regarding their personal information.

The order also calls on the Privacy and Civil Liberties Oversight Board to review IC policies and procedures to ensure that they are consistent with the executive order, and to conduct an annual review of the redress process. The board's review will include an assessment of whether or not the IC has fully complied with determinations made by the Civil Liberties Protection Officer in the Office of the Director of National Intelligence and the Data Protection Review Court. President Biden underscored that a primary goal of the order is to provide greater legal certainty for companies using standard contractual clauses and binding



corporate rules to transfer personal data from the EU to the United States.

The order comes after a two-year absence of any legal framework for transatlantic data transfers following the Court of Justice of the European Union (CJEU) [invalidating the EU-U.S. Privacy Shield Framework](#) in July of 2020. The new framework directly addresses the CJEU's findings that the Privacy Shield failed to provide "effective administrative and judicial redress for the EU data subjects whose personal data are being transferred." While a review by member governments and the European Data Protection Board must be completed before the European Commission can issue the final adequacy decision, the European Commission [released a statement](#), remarking on the "significant improvements" between the Privacy Shield and the new executive order, and commenting that the order addresses all points raised by the CJEU. Once the final adequacy decision has been issued, U.S. companies will be able to join the framework by seeking certification from the U.S. Department of Commerce

through a commitment to comply with a detailed set of privacy obligations.

State Enforcement

California Rulemaking

On July 8, the California Privacy Protection Agency (CPPA), which was created by the California Privacy Rights Act (CPRA) to carry out the purposes and provisions of the CCPA, commenced the formal rulemaking process to adopt regulations to implement the CPRA. The proposed regulations update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA; operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand. The Notice of Proposed Rulemaking notes that the proposed regulations provide for compliance with the CCPA "in such a way that would not contravene a business's compliance with other privacy laws," such as the General Data Protection Regulation

(GDPR) in Europe, and U.S. state privacy laws in Colorado, Virginia, Connecticut, and Utah.

On October 17, proposed modifications were released in response to comments received by the public. The proposed language removed a number of requirements, such as the requirement for businesses to disclose in their notices at collection which third parties collect personal information on their websites, and the requirement that the single option to delete all personal information be more prominently present than other choices. The modified language also included newly added or revised definitions, but still did not address risk assessments, cybersecurity audits, or automated decision-making. The CCPA opened a public comment period, which closed on [November 21](#). It is currently considering those comments and will decide whether to adopt or further modify the proposed regulations at a future public meeting, yet to be scheduled.

CCPA Guidance as Cure and Notice Provisions Sunset

The CPRA, which is set to take effect on January 1, 2023, eliminates the 30-day cure period that currently applies to CCPA enforcement, and instead grants both the California Attorney General and the California Privacy Protection Agency (CPPA) discretion on whether to offer a cure period.

With the upcoming expiration of the notice and cure provision in mind, California Attorney General Rob Bonta provided a glimpse of what to expect with his August 24 [announcement](#) of a settlement with Sephora, Inc. for \$1.2 million—making it the first-ever CCPA settlement. The Attorney General alleged that Sephora failed to disclose that it sells data; engaged in the unlawful sale of personal information, including by exchanging data with third parties for analytics information; failed to post a “Do Not Sell My Personal Information” link on its website and homepage; and failed to respond to or process consumer opt-outs in accordance with global privacy controls (GPC). In addition to a \$1.2 million penalty, the settlement includes a two-year monitoring period, additional reporting

requirements, and terms requiring Sephora to review its service provider contracts.

On June 25, 2021, the California Attorney General notified Sephora that it may be in violation of the CCPA and had 30 days to cure its privacy practices before facing legal liability. Specifically, the Attorney General alleged that Sephora failed to disclose that it sells data; engaged in the unlawful sale of personal information, including by exchanging data with third parties for analytics information; failed to post a “Do Not Sell My Personal Information” link on its website and homepage; and failed to respond to or process consumer opt-outs in accordance with global privacy controls (GPC). In addition to a \$1.2 million penalty, the settlement includes a two-year monitoring period, additional reporting requirements, and terms requiring Sephora to review its service provider contracts.

That same day, Bonta also updated the Attorney General’s “[CCPA Enforcement Case Examples](#),” which provides illustrative examples of situations in which companies were sent a notice of alleged noncompliance, and the steps taken by each company. These enforcement cases targeted companies in a variety of industries, including health care services, medical device manufacturers, financial technology, data brokers, clothing retailers, and online advertising and concerned allegations relating to the following:

- A loyalty program that offered financial incentives without a compliant Notice of Financial Incentive;
- Noncompliant opt-out processes, including an opt-out that required consumers to take additional steps by sending them to a third-party trade association’s tool;
- Inadequate privacy policies, including one privacy policy whose hyperlinks did not direct consumers to the relevant section; and
- Failures to properly handle consumer requests.

After receiving notices of alleged noncompliance, the companies cured the noncompliance within 30 days. To review important lessons learned from these announcements, check out Troutman Pepper’s [analysis](#).

While the August 24 announcement of the first CCPA settlement was significant, the CPPA also held a public hearing on the same day regarding the draft CPRA regulations. These public hearings are an important part of the rulemaking process, and these rules will further shape how the CCPA is enforced. To prepare for the CPRA coming into force on January 1, 2023, and for the promulgation of further regulations, businesses should review current privacy practices, policies, and procedures now. Companies should: consider how they interpret the definition of “sale” and review their service provider contracts; pay attention to any financial incentive programs; consider whether their websites are configured to detect or process any GPC signals; review all CCPA/CPRA disclosures and methods to accept data subject requests to ensure the average consumer can understand them and that they are functioning properly, as well as review all notices, including privacy policies and notices of financial incentives; and test or audit consumer request procedures to determine the adequacy of the company’s response.

First Texas Biometrics Lawsuit

In one of the first-ever actions to enforce Texas’s Capture or Use of Biometric Identifier Act (CUBI), Attorney General Ken Paxton sued a leading technology company that owns and operates several leading social media apps on February 14, alleging the company illegally collected users’ biometric data without their consent. The allegations mimic those in another lawsuit that asserted claims under Illinois’ Biometric Information Privacy Act (BIPA), and recently resulted in a \$650 million settlement. CUBI is similar to BIPA in that it: (1) requires businesses to obtain users’ informed consent before collecting their biometric data; (2) mandates destruction of the data in a reasonable time; and (3) prohibits selling, leasing, or otherwise disclosing the data except in limited circumstances. Unlike BIPA, however, CUBI does not have a private right of action component and can only be enforced by the Texas AG.

The Texas suit alleges that the social media company violated the CUBI provision that requires

consent before capturing “a biometric identifier of an individual.” CUBI defines a biometric identifier as a “retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.” The social media company previously stored biometric identifiers contained in photos and videos as part of its Face Recognition system, and the lawsuit asserts that they did so secretly and without the permission of users, intentionally avoiding use of the term “biometric data” and failing to properly inform users of their practices. In 2017, the company introduced a facial recognition opt-out, and announced in November 2021 that it was ending the Face Recognition system altogether and no longer automatically recognizing users who opted in. The Texas AG felt the move came too late, stating in its suit that “by that point ... [the company] had spent more than a decade secretly exploiting Texans and their personal information to perfect its AI apparatus.”

If the company is found in violation of the act, state law imposes a \$25,000 penalty for each unlawful capturing of an identifier, and the additional claims against the company regarding deceptive trade practices carry up to a \$10,000 penalty per violation.

Notable Litigation

CCPA Litigation

As plaintiffs challenge the boundaries of the CCPA’s private right of action, courts continue to clarify the contours of the statute, such as the pleading standards and the scope of the act.

PreTrial Motions

On April 19, a federal district court judge in *Kellman v. Spokeo, Inc.*, No. 3:21-CV-08976, 2022 WL 1157500 (N.D. Cal. Apr. 19, 2022), denied Spokeo’s motion to dismiss, holding that compliance with the CCPA does not necessarily immunize a website operator from liability under California’s Unfair Competition Law (UCL). Spokeo was publicly displaying individuals’ names and information in “teaser” profiles advertising its services, claiming such information was aggregated from various

sources. The plaintiffs claimed that, among other things, Spokeo's "teasers" violated their rights of publicity.

On May 26, a federal district court judge in a case involving a leading insurance company reiterated that under Fed. R. Civ. P. 1, it has the discretion to stay or transfer a case when the facts of a civil action are identical to a civil action in an earlier filed action. As a result, the action was stayed pending resolution of a similar action in the Eastern District of New York. The court held that "[n]otwithstanding the differences between the CCPA and the New York General Business Law and analogous claims asserted in the other four actions, the factual allegations are substantially similar, and allowing this case to continue in this district would be 'duplicative litigation' that threatens 'the possibility of conflicting judgments,' which the first-to-file rule seeks to avoid." This decision serves as a reminder that parties should be aware of the first-to-file rule as more states enact privacy policies.

In a case that exemplifies the tension between obligations under privacy laws to delete unnecessary information and litigation obligations to retain potentially relevant information, on September 29, a federal district court judge in a trademark infringement case held that compliance with the CCPA is not a credible excuse to delete documents, especially when parties are aware of anticipated litigation. The court found that the defendants' intentional destruction of data and failure to preserve data constituted a violation of Fed. R. Civ. P. 37(e) and warranted a mandatory adverse-inference jury instruction. Irrespective of the CCPA, the court found that the defendants "knowingly spoliated the Slack data with the intent to deprive [the plaintiff] from discovering its content."

The district court in *In re Arthur J. Gallagher Data Breach Litig.*, No. 1:22-CV-137, 2022 WL 4535092, at *10–11 (N.D. Ill. Sept. 28, 2022), denied defendant's motion to dismiss for failure to allege a plausible CCPA claim, holding that plaintiffs' allegations that defendant's lack of security measures caused a data breach were sufficient to state a claim for violation of the CCPA. While a CCPA claim must demonstrate specific injury or

harm to have standing, it does not need to allege with specificity a defendant's particular action or omission that contributed to the breach of the duty to maintain "reasonable" security measures.

Rulings on CCPA Standing

Standing remains an important aspect of CCPA litigation, as courts continue to dismiss plaintiffs' CCPA claims for lack of subject matter jurisdiction.

On April 29, a federal district court judge in *I.C. v. Zynga, Inc.*, No. 20-CV-01539, 2022 WL 2252636 (N.D. Cal. Apr. 29, 2022), found that the plaintiffs' alleged privacy injuries were not sufficiently concrete to provide a basis for Article III standing. In *Zynga*, a group of individual gamers sued a game developer following a data breach that resulted in the theft of email addresses, phone numbers, online usernames, passwords, and one user's date of birth. The court noted that it was "hard pressed to conclude that basic contact information, including one's email address, phone number, or Facebook or Zynga username, is private information. All of this information is designed to be exchanged to facilitate communication and is thus available through ordinary inquiry and observation." The court also noted that a plaintiff's date of birth was a matter of public record, and that it was not clear how discovery of the passwords "would be highly offensive to a reasonable person." *Id.*

In contrast, in *Wynne v. Audi of Am.*, No. 21-CV-08518, 2022 WL 2916341, at *4 (N.D. Cal. July 25, 2022), the plaintiff survived the defendant's 12(b)(1) motion to dismiss because the personally identifiable information (PII) at issue included nonpublic, highly sensitive information such as the plaintiff's driver's license number, Social Security number, and account and loan numbers. The court reiterated that under Article III, only those plaintiffs who have been concretely harmed by a defendant's statutory violation may bring action in federal court. The *Wynne* court further noted that long-standing Ninth Circuit precedent recognizes that historical privacy rights "encompass[] the individual's control of information concerning his or her person ... the violation of which gives rise to a concrete injury sufficient to confer standing."

BIPA Litigation

The [Illinois Biometric Information Privacy Act \(BIPA\)](#) continues to be one of the most litigated privacy statutes in the nation. In 2022, there were many notable settlements, such as Snap, Inc.'s class action settlement agreement to pay \$35 million, and judicial approval of a \$92 million class action settlement against TikTok and Clearview AI.

The Illinois Biometric Information Privacy Act (BIPA) continues to be one of the most litigated privacy statutes in the nation. In 2022, there were many notable settlements, such as Snap, Inc.'s class action settlement agreement to pay \$35 million, and judicial approval of a \$92 million class action settlement against TikTok and Clearview AI.

Two Important BIPA Cases to Watch: *Tims* and *Cothron*

Two consequential cases await decisions by the state's Supreme Court: *Tims* and *Cothron*. On May 17, the Illinois Supreme Court heard oral arguments on when claims accrue under Sections 15(b) and 15(d) of BIPA in *Cothron v. White Castle*. Responding to a question certified by the Seventh Circuit, the Illinois Supreme Court will decide whether BIPA claims accrue each time a private entity scans a personal biometric identifier or transmits such a scan to a third party, or whether such claims accrue only upon the first scan or transmission to a third party. The answer to this question is crucial not only for these litigants (if accrual only occurs

on the first scan or transmission, plaintiff's claims are completely time-barred), but for future BIPA litigants as well. BIPA provides for steep statutory penalties "for each violation." Therefore, a ruling that only the first scan or transmission is a "violation" would limit claims and, more importantly, damages recoveries for BIPA plaintiffs going forward. A ruling that each scan or transmission is a "violation" would likely mean exponentially more exposure for future defendants, as damages awards would be multiplied by each scan or transmission.

On September 21, the Illinois Supreme Court heard arguments in *Tims et al. v. Black Horse Carriers, Inc.*, urging the court to set uniform limitation periods for bringing claims under BIPA. BIPA itself does not include a limitation period, so the question was whether Illinois' "catchall" five-year limitation period applied, or whether the court would borrow from another statute, applying a one-year limitation period. The appellate court had ruled that claims brought under BIPA's Sections 15(c) and (d) were governed by a one-year limitation period, whereas claims brought under Sections 15(a), (b), and (e) enjoyed a five-year limitation period. For more information on the two pending cases and their potential impact on future BIPA litigation, click [here](#).

Courts in the Northern District of Illinois are split about whether to stay cases due to two pending cases before the Illinois Supreme Court. Compare, e.g., *Gibbs v. Abt Elecs., Inc.*, No. 21 C 6277, 2022 WL 1641952, at *7 (N.D. Ill. May 24, 2022) (staying the case pending *Tims* and *Cothron* because the Illinois Supreme Court's decisions "in these cases will have a considerable impact on a very rapidly evolving area of law, as well as on how this case proceeds") with *Woods v. FleetPride, Inc.*, No. 1:21-CV-01093, 2022 WL 900163, at *7 (N.D. Ill. Mar. 27, 2022) (declining to stay because "the potential for the scope of this particular case to change does not justify completely halting the case and delaying discovery"); see also, *Sambolin v. Ethos Veterinary Health, LLC*, No. 22-CV-3276, 2022 WL 5240581, at *1–2 (N.D. Ill. Oct. 6, 2022) ("While there is not yet binding authority on the issue of single- or multiple-accrual, the Court nonetheless can move forward with discovery on Plaintiff's individual claim and the propriety of class certification.").

New Targets

Plaintiffs wielding their private right of action under Illinois' BIPA grew more creative in 2022. In addition to the typical employee time-clock litigation, plaintiffs focused on three new targets: companies using or offering (i) dash-cam "telematics"; (ii) voice-recognition technology; and (iii) "virtual try-on" technology. [Telematics](#) involves use of an in-vehicle camera device that employs artificial intelligence, machine-learning, and "computer vision" to collect and analyze, among other things, driver behavior. Voice recognition is commonly used to field and expedite calls from consumers by creating a "voiceprint" so that retailers can recognize customers more quickly in the future. Around 20 voiceprint cases were filed under BIPA in 2022. Virtual try-on technology is used by beauty and fashion industry companies, allowing users to see what they would look like with certain makeup or accessories. While BIPA claims involving such technology is not new (just last year Sephora [settled](#) a 2018 case involving its virtual makeup kiosks), they increased exponentially in 2022.

BIPA Cases Clarified BIPA Scope in 2022

BIPA does not infringe on First Amendment rights. On February 14, a federal judge rejected Clearview AI's arguments that BIPA violates the First Amendment. In *In re: Clearview AI, Inc. Consumer Privacy Litigation*, Clearview AI faces a multidistrict litigation class action over allegations it covertly scraped over 3 billion photographs of facial images from the internet. The court held that the additional conduct of scraping photographs from the internet "presents a grave and immediate danger to privacy, individual autonomy, and liberty." A more detailed analysis can be found [here](#).

Applicability of arbitration clause must be arbitrated. On March 24, the Seventh Circuit [affirmed](#) an Illinois district court's dismissal of a BIPA case made against Snap, Inc. due to an arbitration provision in the company's terms of service. The district court found that the plaintiff was bound by the arbitration provision despite the plaintiff's defense to the enforceability of Snapchat's terms of service—that she was only 11 years old when she signed up for Snapchat. The Seventh Circuit

held the viability of the defense was a question for the arbitrator.

BIPA requires some measure of knowing. On March 31, a federal judge granted in part and denied in part a social media company's motion for summary judgment relating to BIPA's notice and consent provisions. Specifically, the court found that the company did not have to provide notice to, and obtain consent from, "non-users who were for all practical purposes total strangers to [the company], and with whom [the company] had no relationship whatsoever." Essentially, BIPA does not require an entity to proactively identify individuals whose biometric data may possibly be in its possession, as there must be "some measure of knowing contact with and awareness of the people subject to biometric data collection." However, the court also found that the company could still be held liable for violating another BIPA provision, Section 15(a), which requires companies that take people's biometric data to have written policies explaining how the data will be used and for how long it will be retained.

Virtual try-on applications attracting BIPA litigants' attention. On April 8, plaintiff Paula Theriot [filed](#) a class action lawsuit against Louis Vuitton for violating Illinois' BIPA with its virtual "try-on" application on its website. The complaint alleges that Louis Vuitton encourages consumers to virtually try on its sunglasses and collects complete facial scans and images of their faces—sensitive biometric identifiers—without obtaining appropriate consent or being informed of the biometric data collection. The plaintiff alleges she never signed a written release, authorizing the biometric data collection and was never informed about the purpose for collecting her biometric data. Further, the website's terms and conditions did not indicate that any biometric information would be collected. On December 5, the federal judge dismissed part of the suit after finding that the duty to develop a plan for destroying biometric data is owed to the public generally, not to particular individuals.

Extracting biometric identifiers from a photograph violates BIPA. On April 25, an Illinois judge [held](#) that BIPA governs photograph-derived



facial information and denied a motion to dismiss by defendant software maker Onfido, Inc. The class action alleges that Onfido violates BIPA by scanning uploaded photographs and extracting biometric identifiers without consent. Onfido argued that because it was scanning a photograph and not a person's face, BIPA did not apply. The court disagreed, concluding that "the information Onfido allegedly obtains plausibly constitutes a scan of face geometry," which qualifies as a biometric identifier under BIPA.

Voice-recognition technology targeted by BIPA litigants. On May 31, a Northern District of Illinois judge [denied](#) Walmart's motion to dismiss a class action, alleging Walmart violated BIPA by requiring warehouse workers to speak into a headset with software that captured and used their voiceprints without their consent. The court denied the motion to dismiss because the question of whether a retailer's headset software can identify individuals is a factual question that is better addressed after discovery. Walmart argued that the plaintiff failed to allege that the voice recording system collected biometric data because the system could not identify specific employees by their voice.

BIPA does not apply extrajudicially unless conduct occurred "primarily and substantially"

in Illinois. On October 17, a Western District of Washington judge issued an [order](#) and [judgment](#), ending two related putative class actions alleging tech companies violated BIPA by using datasets containing geometric scans of their faces without their permission. The court granted summary judgment in favor of the tech companies, holding that BIPA does not apply extraterritorially to conduct outside of Illinois, and the plaintiffs had not met their burden to establish the relevant conduct occurred "primarily and substantially" in Illinois. For a more detailed analysis, read [here](#).

Financial institutions covered by GLBA are exempt from BIPA. On November 4, a U.S. District Court judge for the Northern District of Illinois granted DePaul University's motion to dismiss, which argued that DePaul University qualified as a "financial institution," and thus was exempt from BIPA in a lawsuit over its remote test-proctoring software. BIPA's express terms specify that it does not apply to financial institutions that are subject to Title V of the Gramm-Leach-Bliley Act (GLBA).

Workers' Compensation Act does not preempt BIPA injury. On February 3, the Illinois Supreme Court held that the Workers' Compensation Act did not preempt BIPA injury. The court held that plaintiff McDonald's injury involved the loss of her

ability to maintain her privacy, which was neither a psychological nor physical injury and therefore not compensable under the Workers' Compensation Act. The Workers Compensation Act awards damages according to a predetermined fee schedule, which eliminates variability in the value of each judgment. In comparison, BIPA awards the greater of actual or liquidated damages of \$1,000 (for negligent violations) or \$5,000 (for intentional or reckless violations). For a more fulsome description, read Troutman Pepper's analysis [here](#).

BIPA's health care exemption does not apply to information collected from health care employees.

On September 30, an Illinois appellate court [held](#) in *Mosby et al. v. Ingalls Memorial Hospital et al.*, that fingerprint scans collected by a health care employer from its employees do not fall within the BIPA health care exclusion. The exclusion provides, "biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)." Lead plaintiff Mosby had argued that she was required to scan her fingerprint to gain access to a medication dispensing system in her capacity as an employee, not a patient. The court held that the health care exemption only applies to information protected "under HIPAA," which the court stated is limited to information from patients, not employees.

Trial

The first-ever BIPA trial was held this year, with unfortunate, but unsurprising takeaways for companies defending BIPA claims. On October 12, the federal jury in *Rogers v. BNSF Railway Co.*, No. 1:19-cv-03083 (N.D. Ill.), found that defendant BNSF recklessly or intentionally violated BIPA, resulting in a \$228 million judgment entered against it. The jury deliberated for roughly an hour and found that BNSF unlawfully scanned the plaintiff's and over 44,000 other truck drivers' fingerprints for identity verification purposes without written informed permission or notice while the individuals visited BNSF's rail yards. BIPA permits a prevailing party to recover the greater of \$5,000 in liquidated damages or actual damages for each willful or

reckless violation and the greater of \$1,000 in liquidated damages or actual damages for each negligent violation. Thus, the \$228 million judgment was the sum of the jury's finding of 45,600 reckless or intentional violations.

BNSF had argued that its third-party vendor processed drivers' fingerprints at the gates of the Illinois rail yards, was the only party to collect drivers' fingerprints, and therefore, the third-party vendor violated BIPA instead of BNSF. However, the district court rejected BNSF's argument and found in its motion in limine opinion that BIPA does not exclude vicarious liability for third-party vendors' acts and that Section 15(b) is broad enough to include companies, such as BNSF, that hire third parties to collect data on their behalf. The BNSF decision thus significantly broadens the scope of BIPA.

The Florida Telemarketing Law (the Mini TCPA) Litigation

Effective July 1, 2021, Florida enacted an amendment to its telemarketing laws, the Florida Telephone Solicitation Act (FTSA) or "Mini-TCPA," which mirrors the federal Telephone Consumer Protection Act (TCPA) and has spawned several class actions against companies making calls and sending texts to phone numbers with Florida area codes.

In *Davis v. Coast Dental*, 2022 WL 4217141 (M.D. Fl. Sept. 13, 2022), a federal district court held that receipt of an unsolicited marketing call, standing alone, is not enough to state an FTSA claim. The plaintiff merely alleged: "To transmit the above telephonic sales calls, Defendant utilized a computer software system that automatically selected and dialed Plaintiff's and the Class members' telephone numbers." The court found that plaintiff's allegation was insufficient to state a claim as a matter of law and failed to allege facts making it plausible that the defendant used an automated dialing system as described by the state statute. *Davis* demonstrates that conclusory allegations are insufficient to state an FTSA claim and are unlikely to survive a 12(b)(6) motion to dismiss.

Data Breach Litigation

Several notable decisions related to data breach litigation were reached in 2022. Overall, recent data breach cases show courts and government agencies are increasingly holding companies accountable for data breaches and other privacy-related issues that may affect consumers.

No standing in Bonobos litigation. On January 19, the Southern District of New York dismissed a class action lawsuit against Bonobos for failing to meet standing requirements. The class action alleged that partial credit card numbers, encrypted passwords, telephone numbers, email addresses, and other personal data were compromised in a data breach and posted to an online forum used by cybercriminals. The court found that the plaintiff did not make “plausible allegations of misuse” or show a “substantial risk of future identity theft or fraud.” The court explained that although plaintiff’s partial credit card number had been compromised, he had the ability to cancel the card, which would eliminate any future risk of harm. As to the compromised passwords, they were encrypted, Bonobos reset the passwords, and there were no allegations that the compromised passwords were used on other websites/accounts. Accordingly, the likelihood that harm would result from the exposed data was too remote to support standing.

Partial class certification against international hotel chain. The U.S. District Court for the District of Maryland issued a class certification decision in a multidistrict consumer data breach case against an international hotel company, becoming one of the few district courts to certify a limited Rule 23(b)(3) class in a consumer data breach case. Notably, the court substantially narrowed the classes to eliminate individuals whose claims were dissimilar to the named plaintiffs, and denied certification of a proposed class of plaintiffs claiming breach of state data breach notification laws and classes requesting injunctive relief. The court held that the limited proposed 23(b)(3) classes were ascertainable, however, because the single database that was exposed in the data breach contained the names and contact information for virtually all of the class members. The court concluded that any gaps could be filled through an objective, “mechanical” review of available additional records.

Major settlement wins in data breach cases. In October, U.S. District Judge Amy Berman Jackson granted final approval for the \$63 million settlement in a class action brought by the victims of the 2015 Office of Personnel Management (OPM) data breach. The settlement provided awards between \$700 and \$10,000 to eligible persons and resolved the long-running legal claims that filtered through the U.S. courts in the wake of the June 2015 incident. Over 25.7 million current and former federal employees were affected by the data breach. While it was unclear who orchestrated the attack, experts agree the cyberattack was carried out on behalf of foreign governments. Under the settlement, OPM will pay \$60 million into the settlement, and a defense contractor that operated the electronic information systems, will contribute \$3 million.

The plaintiffs in 13 consolidated actions titled *In re Accellion, Inc. Data Breach Litigation*, Case No. 21-cv-01155-EJD, await final approval of an \$8.1 million settlement in the Northern District of California. The consolidated action stems from a late 2020 data breach where hackers stole names, dates of birth, Social Security numbers, driver license numbers, and bank account information from hundreds of law firms, universities, companies, and government agencies by compromising Accellion’s file-sharing application, “File Transfer Appliance.” If approved as is, class members would receive two of three credit monitoring and insuring services, reimbursement of up to \$10,000, or a cash fund payment between \$15 and \$50. The settlement also would provide injunctive relief to be implemented four years from the effective date of the settlement. This would require Accellion to retire its File Transfer Appliance, provide annual cybersecurity training to all employees, employ personnel with formal cybersecurity responsibilities, and take other measures. The parties seemed poised to secure final approval, but on September 8, the court terminated the motions for settlement approval and instead began focusing on appointing lead counsel and a plaintiffs’ steering committee.

Third Circuit reverses standing decision in data breach cases, finding “sufficient risk” of harm.

In September, the Third Circuit held that a former ExecuPharm, Inc. employee had Article III standing in her negligence class action. Plaintiff alleged that

the company's negligence led to a data breach, which leaked her private information onto the dark web. The lower court held she had no standing because she had not suffered identity theft or fraud as a result of the leak. The Third Circuit reversed, however, holding that under Supreme Court case law, "sufficient risk" of future harm could confer Article III standing. The Third Circuit found that this standard was met because: (i) a well-known hacker group had intentionally gained access and misused her data by placing it on the dark web; and (ii) the "data was also the type of data that could be used to perpetrate identity theft or fraud." This combination of factors raised a sufficient risk of harm to confer standing.

Notable Video Privacy Protection Act Litigation

A sizable surge in Video Privacy Protection Act (VPPA) [lawsuits](#) were filed in 2022 against companies that offer videos on their websites using common adtech data tools. The VPPA was enacted in 1988 in direct response to the disclosure of U.S. Supreme Court nominee Robert Bork's videotape rental history during his confirmation hearings. The VPPA, which prohibits a "video tape service provider" from "knowingly" disclosing "personally identifiable information concerning any consumer of such provider," was written when the internet was still in its infancy—and certainly before the act's drafters knew anything about advertising technology or cookies.

Accordingly, few have thought about the VPPA since streaming services have put videotape rental stores out of business. That has all changed. Courts have begun grappling with the VPPA's application to more modern technologies, such as streaming services. Among other things, courts have considered the definition of personally identifiable information, and the definition of consumer, and these varying definitions have led to circuit splits. Three major VPPA lawsuits in 2022 include: *Buechler et al. v. Gannett Company, Inc.*; *Salazar v. Paramount Global*; and *Swartz v. ESPN, Inc.*

In *Buechler et al. v. Gannett Company, Inc.*, two Gannett newsletter subscribers sued the company in Delaware federal court, alleging that the

newspaper giant "knowingly and systematically" disclosed their personal viewing information to a social media app without obtaining their consent, violating the VPPA. The plaintiffs' complaint alleged that they subscribed to newsletters from Gannett and *The Tennessean*, and then watched videos on their website from a device that was simultaneously signed into the social media app. The plaintiffs alleged that tracking methods embedded in the Gannett sites automatically shared their viewing history and personally identifiable information with the app.

Similarly, in *Salazar v. Paramount Global*, a proposed class filed suit in Tennessee federal court alleging that Paramount Global violated the VPPA by tracking user data and sharing it with a social media company without consent. The plaintiffs allege that the personal viewing information Paramount discloses to the company allows the social media site to "build from scratch or cross-reference and add to the data it already has in their own detailed profiles for its own users, adding to its trove of personally identifiable data."

Several notable decisions related to data breach litigation were reached in 2022. Overall, recent data breach cases show courts and government agencies are increasingly holding companies accountable for data breaches and other privacy-related issues that may affect consumers.

Lastly, in *Swartz v. ESPN Inc.*, the plaintiff alleged that the NBA intentionally disclosed the personal viewing information of its subscribers. Plaintiff



alleged that when customers set up an account on NBA.com, the league was able to gather the subscribers' city, ZIP code, and physical location through their IP address, as well as information provided by the user, including name, email address, phone number, credit card information, username, password, and information about previous videos watched by a particular consumer. This was disclosed upon sign-up, but according to the lawsuit, the NBA did not state that it would share personal viewing information with third parties.

Wiretapping Cases and CA Invasion of Privacy Cases

We saw an influx in privacy litigation in 2022 in which plaintiffs attempted to bring claims under outdated and discrete state wiretapping and invasion of privacy laws.

In August, the Third Circuit overturned a lower court's ruling in *Popa v. Harriet Carter Gifts, Inc.*, that Harriet Carter, an online retailer, and third-party marketing company NaviStone, Inc. were exempt from liability under Pennsylvania's anti-wiretapping law. Case No. 21-2203, 2022 WL 3366425 (3rd Cir. Aug. 16, 2022). The lawsuit was one of many recent putative class actions attempting to apply decades-old wiretapping laws against websites and their service providers. The

named plaintiff allegedly shopped on Harriet Carter Gifts' website, on which NaviStone's marketing software was installed. Plaintiff argued that defendants violated Pennsylvania's Wiretapping and Electronic Surveillance Control Act (WESCA) by sending her interactions with Harriet Carter's website to NaviStone. The district court granted summary judgment in favor of the defendants, holding that there was no interception as a matter of law because NaviStone was a direct recipient of plaintiff's communications. However, the Third Circuit disagreed, holding that NaviStone's position as a direct recipient of Popa's communications did not allow it to escape liability under WESCA.

Additionally, in late 2022, several cases were filed against major companies for violation of the California Invasion of Privacy Act (CIPA), Section 637.3. For example, in September, five financial institutions were sued for allegedly using voice-recognition software at call centers in violation of Section 637.3 of CIPA. Section 637.3 states: "No person or entity in this state shall use any system which examines or records in any manner voice prints or other voice stress patterns of another person to determine the truth or falsity of statements made by such other person without his or her express written consent given in advance of the examination or recordation." According to the complaints, the banks implemented software at their call centers that stores a caller's

voiceprint—i.e., the unique pattern of a person’s voice—and uses the data to verify the person’s identity during subsequent calls. The lawsuits argue that each system’s analysis of callers’ voices to authenticate or refute their identities constitutes a use of voiceprints “to determine the truth or falsity of an individual’s statements,” as governed by the California Invasion of Privacy Act.

Lastly, in December, putative class actions were filed against Ulta and Bass Pro Shops in the Southern District of California for allegedly violating the federal Wiretap Act and Section 631 of CIPA by using “session replay” software on their websites to spy on users. The complaints allege the beauty store chain and outdoor gear retailer violated the federal Wiretap Act and CIPA when their websites tracked users’ mouse movements, keystrokes, search terms, and more. Plaintiffs further allege that site visitors were not alerted via a pop-up disclosure or consent form that their activity on the website was being tracked. The complaints allege the companies embedded into their website code third-party scripts called “session replay” to intercept “every incoming data communication ... the moment [a] visitor accessed” their sites. From there, Ulta and Bass Pro Shops allegedly stored users’ sessions to analyze and use for business purposes.

Information Security

Legislation

On June 21, President Biden signed the State and Local Government Cybersecurity Act of 2021 (S.2520), which updated the Homeland Security Act and directed the Department of Homeland Security to improve information sharing and coordination with state, local, and tribal governments. This legislation encouraged federal cybersecurity experts to share information on cybersecurity threats, vulnerabilities, and breaches, as well as resources to prevent and recover from cyberattacks. The law also built on previous efforts by the Multi-State Information Sharing and Analysis Center (MS-ISAC) to prevent, protect, and respond to future cybersecurity incidents. For more information, click [here](#).

On July 21, U.S. Senators Kyrsten Sinema (D-AZ) and Cynthia Lummis (R-WY) [introduced](#) the Improving Digital Identity Act of 2022. The legislation would create a taskforce to improve cybersecurity to allow access to “critical services” online. It also would require federal agencies to strengthen the “security, accessibility, and privacy” of their networks.

Regulation/Industry Guidance

On July 21, the National Institute of Standards and Technology (NIST) updated its cybersecurity guidance for the health care industry. NIST revised its 2008 guidance primarily because it wanted to integrate it with other guidance that has not yet existed. This new guidance has helpfully mapped out the elements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, increasing the emphasis “on the guidance’s risk management component, including integrating enterprise risk management concepts.” NIST accepted comments until October 5, 2022. To learn more about this new guidance, click [here](#).

On June 13, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released guidance on how health care providers and health plans can use remote communication technologies to provide audio-only telehealth services that comply with the Health Information Portability and Accountability Act (HIPAA) privacy, security, and breach notification rules. OCR Director Lisa J. Pino stated that audio-only telehealth can assist “in reaching patients in rural communities, individuals with disabilities, and others seeking the convenience of remote options.” To read more, click [here](#).

On July 26, the National Credit Union Administration announced a proposed rule to require federally insured credit unions experiencing a reportable cyber incident to report the incident to the agency as soon as possible, and no later than 72 hours after the credit union reasonably believes it experienced a reportable cyber incident. This proposed rule would not require a detailed incident assessment, but just an early alert to the agency. Comments on the proposed rule were due on or

before September 26. The National Credit Union Administration is currently reviewing comments and is expected to provide an update sometime in 2023.

Originally slated for last February, on June 1, the FTC refiled an Advance Notice of Proposed Rulemaking (ANPRM) with the Office of Management and Budget for a potential rule on artificial intelligence and privacy abuses under Section 18 of the FTC Act. Stakeholder consultation began June 1 and ended August 1. The FTC hopes to curb lax security practices and combat unlawful discrimination in algorithm decision-making. Click [here](#) to view the ANPRM.

On January 20, President Biden signed a memorandum aimed at improving the cybersecurity of the National Security, Department of Defense, and Intelligence Community Systems (together, the National Security Systems (NSS)). An NSS is an information system used or operated by an agency or on its behalf, the function, operation, or use of which involves: (i) intelligence activities; (ii) cryptologic activities related to national security; (iii) command and control of military forces; or (iv) equipment that is an integral part of a weapon or weapons system. This designation also applies to information systems that are critical to the direct fulfillment of military or intelligence missions or ones that are to be kept classified in the interest of national defense or foreign policy. In essence, the memorandum directs agencies (departments that own or operate an NSS) to: (1) identify systems that are or are likely to constitute an NSS; (2) implement protocols to protect that information against cyberthreats; and (3) develop a plan to respond to a suspected or actual cyberthreat. To learn more, click [here](#).

On January 13, Him Das, the acting head of the Financial Crimes Enforcement Network (FinCEN), highlighted ransomware as a chief national security risk. At the Financial Crimes Enforcement Conference, Das suggested that the current anti-money laundering regulations are insufficient to protect against tech-driven threats, from cyberattacks to digital asset schemes. FinCEN is currently enacting new regulations under the

Anti-Money Laundering Act of 2020 (AML Act), which will seek to address threats, such as corruption and anti-terrorism, while also taking a proactive approach against crimes tied to ransomware, digital assets, and strategic corruption. To this end, the agency recently issued two Notices of Proposed Rulemaking, the [first](#) on December 7, 2021, and the [second](#) on January 24, 2022. To learn more, click [here](#).

The FTC [proposed a consent order against CafePress](#) over allegations the company failed to implement reasonable security measures to protect sensitive information stored on its network, including Social Security numbers, inadequately encrypted passwords, and answers to password reset questions. According to the FTC's complaint, a hacker exploited the company's security failures in February 2019 to access millions of email addresses and passwords with weak encryption, more than 180,000 unencrypted Social Security numbers, and tens of thousands of partial payment card numbers and expiration dates. Some of this information was found on the dark web. The allegations also stated the company failed to properly investigate the breach for several months despite multiple warnings from individuals and a foreign government. The proposed settlement will require Residual Pumpkin Entity, LLC—the former owner of CafePress—to pay \$500,000 in redress to victims of the data breach.

On May 9, the National Association of Attorneys General (NAAG) announced the creation of the [Center on Cyber and Technology](#) (CyTech). CyTech seeks to enhance the technical competency of state AGs and staff by: (1) developing programming and dedicating resources to support the understanding of emerging and evolving technologies; (2) conducting cybercrime investigations and prosecutions; and (3) ensuring secure and resilient public and private sector networks and infrastructure. CyTech will also provide tools and support for state AGs' technology-related enforcement actions. Companies, in-house counsel, and their IT executives should take additional steps to pay attention to CyTech's list of topics to anticipate potential areas of scrutiny and enhance their policies, procedures, and training in those [areas](#).

An amendment to the National Defense Authorization Act passed by the House in July would create a “systemically important entity” designation, applying new regulations and offering priority aid to certain critical infrastructure companies. But the American Bankers Association and Bank Policy Institute say the amendment as applied to financial institutions would duplicate existing regulations under the Dodd-Frank Act, while also requiring the turnover of a substantial amount of cybersecurity-related data that could prove dangerous in the wrong hands. The amendment, introduced by U.S. Rep. Jim Langevin (D-RI), chairman of the House Armed Services Committee’s Subcommittee on Cyber, Innovative Technologies, and Information Systems, focuses on those private sector entities whose core functions are of national consequence to the United States, a definition which would encompass some of the largest companies in the nation’s banking industry. As of mid-December 2022, the amendment was in the Senate for consideration. To learn more, click [here](#).

On August 11, the Consumer Financial Protection Bureau (CFPB) [published](#) a circular, answering the question “Can entities violate the prohibition on unfair acts or practices in the Consumer Financial Protection Act (CFPA) when they have insufficient data protection or information security?” with a resounding “yes.” Specifically, the CFPB pointed to three practices—inadequate authorization, poor password management, and lax software update policies—as examples of data security practices that would likely cause substantial unavoidable injury to consumers without a countervailing benefit and that could trigger liability for financial institutions and/or their service providers. Failure to comply with these requirements may violate the CFPA’s prohibition on unfair acts or practices. To learn more, click [here](#).

On July 29, New York State’s Department of Financial Services (NYDFS) released [draft amendments to its Part 500 Cybersecurity Regulation](#) for financial services companies that, among other things: (1) contain significant changes regarding ransomware; (2) propose a new class comprising larger entities, which will be subject to increased obligations for their cybersecurity programs; (3) require enhancements to governance

policies and procedures; (4) announce new restrictions on privileged accounts; and (5) clarify its enforcement authority. To learn more, click [here](#).

Notable Security Settlements

In July, T-Mobile announced the terms to its settlement for a consolidated class action lawsuit following a data breach that occurred earlier in 2021. To read the SEC’s filing, click [here](#).

In January, Morgan Stanley [agreed to pay \\$60 million](#) to settle claims relating to a class action lawsuit relating to data security incidents that occurred in 2016 and 2019. The lawsuit alleged that the company failed to properly dispose of certain IT assets and that it resulted in third parties having access to individuals’ personal information, which included sensitive financial information. The company also agreed to hire a third party to assist it in locating the IT devices that have been sold to others in hopes of mitigating potential future risk.

In October, the U.S. Securities and Exchange Commission (SEC) recommended an enforcement action due to violations of U.S. securities laws specifically “with respect to [SolarWinds] cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures.” Soon after, SolarWinds announced it had agreed to pay \$26 million to settle a lawsuit filed by shareholders. The potential enforcement action and lawsuit stem from a 2019 data breach that also affected hundreds of companies and government systems.

The DOJ agreed to its first-ever False Claims Act (FCA) settlement under its newly instituted Civil Cyber Fraud Initiative. Among other things, the initiative employs the False Claims Act as an avenue to pursue cybersecurity-related fraud by government contractors and grant recipients. The \$930,000 settlement with Comprehensive Health Services (CHS) is a watershed moment in the department’s approach to cybersecurity, highlighting its renewed focus and commitment to holding vendors doing business with the federal government accountable for meeting federal cybersecurity requirements. For further analysis and discussion, click [here](#).



Specifically, the CFPB pointed to three practices—inadequate authorization, poor password management, and lax software update policies—as examples of data security practices that would likely cause substantial unavoidable injury to consumers without a countervailing benefit and that could trigger liability for financial institutions and/or their service providers. Failure to comply with these requirements may violate the CFPB’s prohibition on unfair acts or practices.

Criminal

On October 5, Joe Sullivan, the former chief security officer for Uber, was [convicted](#) of obstructing justice by failing to disclose a breach to the FTC. The charges stem from a data breach in 2016, and a nondisclosure agreement Sullivan signed with the hackers, despite consulting with the CEO at the time and legal personnel at Uber. Prosecutors argued this was evidence he participated in a cover-up. This conviction highlights the doubts many chief information security officers have about corporate support, emphasizing the need for improved governance and collaboration with general counsels.

International Developments

After the Warsaw University of Technology suffered a data breach in May 2020, the Polish data protection authority (DPA) investigated and held that the university did not implement the appropriate technical and organizational measures to ensure the security of the personal data processed. The fine totaled PLN 45,000 (approximately EUR 9,900 and \$11,200 USD).

The [Integritetsskyddsmyndigheten](#), the Swedish DPA, warned of a significant increase in health care sector cybersecurity attacks in 2021. In total, 5,767

cyber incidents were reported, or approximately 110 incidents a week, to the Swedish DPA. Almost six out of every 10 reported cyber incidents resulted from human error, such as incorrectly sending emails. The Swedish DPA stated that the human error factor behind many of the cyber incidents highlights the need for organizational and technical measures, as well as employee training.

On September 15, the European Commission [presented](#) EU-wide legislation mandating cybersecurity requirements for software and hardware products called the Cyber Resilience Act (CRA), which includes fines for noncompliance reaching up to 2.5% of a business's annual revenue. The act applies to any digital product connected directly or indirectly to another device or network, including wireless and wired devices and software, covers the product's life cycle, and requires manufacturers to provide security support and software updates to address identified vulnerabilities. Exceptions exist for certain products whose cybersecurity requirements are already established by existing EU rules, including medical devices, vehicles, aviation, and software as a service. The act aims to ensure that businesses will only need to comply with a single set of cybersecurity rules across the EU and must undergo analysis by the European Parliament and Council before its adoption.

International Updates

Europe – Digital Markets Act

On July 5, the European Parliament voted in favor of the new [Digital Services Act](#) (DSA) and [Digital Markets Act](#) (DMA). The two bills addressed the societal and economic effects of the tech industry by setting clear standards for operation and provision of services in the EU. The DSA established obligations for digital service providers, such as social media or marketplaces, to tackle the

spread of illegal content, online disinformation, and other societal risks. In other words, what is illegal offline, should be illegal online. These obligations intend to be proportionate to the size and risks that such platforms pose to society. Accordingly, large platforms with 45 million or more monthly users will have to comply with stricter obligations as they present the highest risk. The DMA established new rules for “gatekeepers” to comply with their daily operations. Gatekeepers are large online platforms, that have strong economic positions and an entrenched and durable position in the market. The goal of the DMA is to prevent gatekeepers from using unfair practices toward business users and customers that depend on them.

China – Personal Information Protection Law

Last year, China passed the Personal Information Protection Law (PIPL). Under PIPL, companies engaging in [cross-border transfers](#) of information must comply with a security assessment. On July 7, China's top regulator, the Cyberspace Administration of China (CAC), released the final version of the Measures for Security Assessment of Data Exports (Security Assessment Measures or Measures). Under China's Personal Information Protection Law (PIPL), Article 40, when personal information handlers (the PIPL equivalent of a controller under the GDPR) and critical information infrastructure operators (CIIO) need to export personal information abroad, both handlers and CIIOs must first pass a security assessment organized by the State Cybersecurity and Informatization Department.

Canada – Federal Comprehensive Privacy Act

On June 16, the Canadian Minister of Innovation, Science, and Industry introduced the [Digital Charter Implementation Act, 2022](#), which features three pieces of legislation: the Consumer Privacy Protection Act (CPPA), the Personal Information

and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act. The CPPA would replace the current privacy framework—the Personal Information Protection and Electronic Documents Act (PIPEDA)—and would provide consumers greater control over their personal information.

The second component would establish a tribunal to oversee CPPA violations, and the third legislation would require companies that build high-impact artificial intelligence systems to identify, assess, and mitigate the risk of harms and bias.



DEBT COLLECTION

Authors: James K. Trefil, Stefanie H. Jackman, Jonathan P. Floyd, Joshua D. Howell, Stephen D. Lozier

Although 2022 brought multiple significant developments in the debt collection industry, the question of federal standing—whether a consumer has the legal right to bring a claim in federal court—was perhaps one of the most prominent. As debt collection defendants found themselves increasingly unable to remove consumer cases claiming only statutory damages to federal court, it became clear that the U.S. Supreme Court’s Article III standing jurisprudence was working to reshape the debt collection litigation landscape.

Federal Jurisdiction Becomes Less Certain in Consumer Law Cases

Indeed, throughout 2022, federal courts continued to grapple with the implications of the Supreme Court’s decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021). Recall that in *Ramirez*, the Court held that certain class plaintiffs asserting claims under the Fair Credit Reporting Act (FCRA) could not demonstrate Article III standing without showing that TransUnion had disseminated the derogatory consumer information at issue to third parties. Absent publication of the derogatory information and resulting real-world injury, the Court determined the plaintiffs did not suffer a concrete harm sufficient to confer federal standing.

Though *Ramirez* dealt with the FCRA, its holding applies to any federal statute conferring a private cause of action for violation of its provisions, most notably including the Fair Debt Collection Practices Act (FDCPA). As a result, throughout 2022, federal district courts repeatedly held that the type of unadorned, “informational” injuries so often alleged in FDCPA claims were no longer sufficient to confer Article III standing. The impact here is felt first in the removal context, with scores of FDCPA cases being remanded on motion or *sua sponte* to state courts—often over the objection of not only plaintiffs but defendants, who, paradoxically, find themselves arguing that a plaintiff *has alleged* concrete injury in order to remain in federal court.

We expect this trend to continue into 2023, with the looming implication being that a large amount of post-*Ramirez* FDCPA case law will be developed in state, not federal, courts. This large-scale shift of FDCPA litigation to state courts will require defendants and counsel to recalibrate litigation strategies that previously assumed the availability of a federal forum (and procedural rules) to decide issues arising under the FDCPA. State constitutional standing doctrine and procedural rules also will take on newfound importance when developing FDCPA litigation strategies.

Aside from its impact on forum, *Ramirez* also compelled courts and litigants over the past year to reconsider (and, of course, litigate) what constitutes a concrete injury for purposes of an FDCPA claim. In the credit reporting context, for example, *Ramirez* calls into question whether a debt collector’s mere reporting of a disputed debt to credit bureaus is the kind of privacy-implicating publication necessary to demonstrate concrete injury under the FDCPA’s third-party disclosure provisions.

Further complicating matters in 2022 was Article III’s inevitable dovetailing with the Eleventh Circuit’s recent decision in *Hunstein*, where an *en banc* panel held a debt collector’s communication of debt-related information to a mailing vendor is not actionable under the FDCPA due to the lack of a concrete harm for purposes of Article III standing. Query whether a mailing vendor of the type at issue in *Hunstein* is similar to, or different from, a credit reporting agency in any meaningful way for purposes of this analysis? Further, the extent to which an aggrieved party’s alleged “emotional” injuries constitute concrete harm is another issue *Ramirez* pushed further to the forefront. Throughout 2022, courts frequently gave increased scrutiny to the plausibility of alleged emotional harm for purposes of establishing Article III standing, and we expect this trend to continue, if not intensify, in 2023.



These and myriad other issues will crop up in 2023 as courts continue to wrestle with *Ramirez* and its implications, both foreseen and unforeseen.

Hunstein v. Preferred Collection and Management Services, Inc. Is Reversed by an En Banc Panel of the Eleventh Circuit

In a decision released September 8, an *en banc* panel of the Eleventh Circuit Court of Appeals reversed its own decision that a debt collector's outsourcing of its letter process to a third-party mail vendor stated a claim for violation of the FDCPA's prohibition against unauthorized debt disclosure. Instead, the *en banc* panel ruled that the plaintiff lacked standing to bring the underlying claim. Per the court: "Under the most generous reading of his complaint, one company sent his information to another, where it was 'populated' into a private letter that was sent to his home. That is simply not enough."

On April 21, 2021, a panel of the Eleventh Circuit had issued the original *Hunstein v. Preferred Collection and Management Services, Inc.* opinion, holding that: (1) a consumer had standing to bring a claim under the FDCPA because he alleged an invasion of privacy based on the spread of his debt-related information; and (2) the plaintiff had sufficiently alleged a claim that a debt collector's outsourcing of its letter process to a third-party mail vendor violated the FDCPA's prohibition against unauthorized debt disclosure as set forth in FDCPA Section 1692c(b).

On October 28, 2021, the Eleventh Circuit panel vacated its original opinion and issued a substitute opinion wherein the panel majority reaffirmed its original opinion and held that Hunstein had standing to sue. See *Hunstein vs. Preferred Collection & Management Services, Inc.*, 17 F. 4th 1016 (11th Cir. 2021). The impetus for the substituted opinion was the Supreme Court's

intervening decision in *Ramirez*, which had suggested in passing that standing might be an issue in the *Hunstein* context.

On November 17, 2021, the Eleventh Circuit vacated the substitute opinion and agreed *sua sponte* to reconsider *en banc* whether a debt collector's transmission of private debtor information to its mail vendor violated the FDCPA. See 2021 WL 5353154 (11th Cir. Nov. 17, 2021). However, in so doing, the Eleventh Circuit asked the parties to focus their arguments on Article III standing. Oral arguments were held on February 22, 2022.

Relying heavily on *Ramirez*, 141 S. Ct. 2190 (2021), which held that a concrete injury under the FCRA requires more than the existence of a risk of harm that never materializes, the *en banc* panel held that Hunstein's proffered harm of publicity was insufficient to confer Article III standing. "We first identify the precise harm at issue. Hunstein alleged that, rather than preparing a mailing on its own, Preferred Collection sent information about his debt to a mail vendor, which then populated the data in a form letter. That act, according to Hunstein, violated the statutory prohibition on communicating, 'in connection with the collection of any debt, with any person other than the consumer.'" Hunstein analogized this harm to the tort of public disclosure. However, the court held the disclosure alleged lacked the fundamental requirement of publicity.

According to the *en banc* panel, publicity requires more than just any communication to a third party. Instead, the private information must be made public in some manner. The court noted that Hunstein did not allege that a single employee ever read or understood the information about his debt.

"[N]owhere does Hunstein suggest that Preferred Collection's communication reached, or was sure to reach, the public. Quite the opposite – the

complaint describes a disclosure that reached a single intermediary, which then passed the information back to Hunstein without sharing it more broadly."

Ultimately, the court held that because Hunstein alleged only a legal infraction and not a concrete harm, the court lacked jurisdiction to consider his claim. "As *Hunstein* explained, courts have no 'freewheeling power to hold defendants accountable for legal infractions.'" Although dismissed on Article III standing grounds, the court's express rejection of the idea that preparation of a letter, without more, constitutes a public disclosure should prove useful in continuing litigation, including in state courts that sometimes have more lax standing requirements. In the wake of the *en banc* decision, countless copycat cases based on the *Hunstein* theory remain active and will no doubt continue to be litigated, in both state and federal courts.

"[N]owhere does Hunstein suggest that Preferred Collection's communication reached, or was sure to reach, the public. Quite the opposite – the complaint describes a disclosure that reached a single intermediary, which then passed the information back to Hunstein without sharing it more broadly."

The CFPB's Constitutionality Is Challenged Again

Two years ago, the Supreme Court curtailed the independence of the CFPB in *Seila Law v. CFPB*, finding the director's insulation from presidential control violated the Constitution. 591 U.S. (2020). The Court struck the unconstitutional language from the Dodd-Frank Act, thereby vesting the President with authority to dismiss a CFPB director at will. *Seila Law* did not involve any question relating to the CFPB's funding mechanism under Dodd-Frank.

On October 19, 2022, a three-judge panel of the Fifth Circuit Court of Appeals took this a step further, holding the CFPB's funding mechanism itself to be unconstitutional. Specifically, the court in *Community Financial Services Association of America, Ltd. v. Consumer Financial Protection Bureau* held the CFPB's funding violates the Constitution because the CFPB does not receive its funding from annual congressional appropriations like most executive agencies. Instead, the CFPB is funded directly from the Federal Reserve based on a request by the CFPB's director.

In the underlying case, the plaintiffs, Community Financial Services Association of America and Consumer Service Alliance of Texas, challenged the validity of the payment provision contained in the CFPB's 2017 Payday Lending Rule (Rule). The payment provision prohibits lenders from initiating additional payment transfers from consumers' accounts after two consecutive attempts have failed for insufficient funds unless the consumer authorizes additional payment transfers. The district court initially granted summary judgment in favor of the CFPB. The plaintiffs appealed on multiple grounds including: (1) the Rule's promulgation violated the APA; (2) the Rule was promulgated by a director unconstitutionally insulated from presidential removal; (3) the CFPB's rulemaking violates the non-delegation doctrine; and (4) the CFPB's funding mechanism violates the Constitution's appropriations clause. The Fifth Circuit affirmed the district court's entry of summary judgment in favor of the CFPB on each of the first three issues. But importantly, the Fifth Circuit panel held that "Congress's cession of its power of the purse to the Bureau violates the Appropriations Clause and the Constitution's underlying structural

separation of powers" and reversed on that issue, invalidating the Payday Lending Rule. The court rooted its decision in the foundational precepts of the Federalist Papers and the Federal Convention of 1787, at one point quoting George Mason in support of its decision: "The purse & the sword ought never to get into the same hands."

In its opinion, the Fifth Circuit focused on what it characterized as the CFPB's double insulation from Congress's appropriation power. In the court's view, not only does the CFPB receive its funding via request by the director to the Federal Reserve, but also the Federal Reserve itself falls outside the appropriations process by receiving its funding by way of bank assessments. Moreover, funds derived from the Federal Reserve System are not subject to review by the House or Senate Committee on Appropriations. As the Fifth Circuit found: "[T]he Bureau's funding is double-insulated on the front end from Congress's appropriations power. And Congress relinquished its jurisdiction to review agency funding on the back end." The court determined this relinquishment to be even more problematic given the CFPB's expansive authority. "An expansive executive agency insulated (no, double-insulated) from Congress's purse strings, expressly exempt from budgetary review, and headed by a single Director removable at the President's pleasure is *the epitome* of the unification of the purse and the sword in the executive"

Ultimately, the Fifth Circuit held that while Congress properly authorized the CFPB to promulgate the Rule, the CFPB lacked the wherewithal to exercise that power via constitutionally appropriated funds. The plaintiffs were thus harmed by the CFPB's improper use of unappropriated funds to engage in the rulemaking at issue and were entitled to a "rewinding" of the CFPB's action.

If it stands, at least within the Fifth Circuit, this opinion would invalidate all CFPB actions from its inception in 2011, as well as the CFPB's current activities, as unconstitutional. This is because, like the 2017 Payday Lending Rule, none of the CFPB's actions, from rulemaking to enforcement, could have occurred absent the unconstitutional funding. The opinion also renders the CFPB's action from inception vulnerable to challenge nationwide.

Already, the same appropriations argument is being made in a number of other cases involving the CFPB, including several enforcement cases pending in courts in the Fifth Circuit and elsewhere, as well as in the U.S. Chamber of Commerce case challenging the CFPB's authority to prohibit discrimination under its UDAAP authority, which is also pending in a district court in the Fifth Circuit.

On November 15, 2022, the CFPB filed a petition for certiorari with the U.S. Supreme Court in which it sought expedited review of the Fifth Circuit's decision. Thereafter, the Court granted CFSA's request to have through January 13, 2023, to file its brief in opposition to the CFPB's certiorari petition. The Court is expected to consider the CFPB's petition and any opposition or cross-petition filed by CFSA at the Court's February 17, 2023 conference. This will be an important case to watch in 2023, as the decision stands to have a significant and potentially wide-ranging effect on not just the CFPB, but possibly other agencies that are funded outside of the congressional appropriations process, such as the FDIC, the OCC, and even the Federal Reserve itself.

Medical Debt Collection Falls Under Greater Scrutiny

On March 1, 2022, the CFPB released a report highlighting the complicated and burdensome nature of the medical billing system in the United States. This is one of the CFPB's largest areas of concern, and its report makes clear the CFPB's view that the U.S. health care system is supported by a billing, payments, collections, and credit reporting infrastructure where mistakes are common, and where patients often have difficulty getting these errors corrected or resolved.

Thereafter, in April, the Biden administration announced several reforms to address the nearly \$200 billion worth of medical debt in the United States. These actions included holding medical providers and debt collectors accountable for harmful practices, reducing the role medical debt plays in accessing credit, helping veterans get their debt forgiven, and informing all Americans of their rights as consumers in the health care market. A federal consumer protection law, the

"No Surprises Act," also came into force in 2022. The Act provides billing and collection rights to medical patients, both insured and uninsured. In a related bulletin, the CFPB issued a warning that attempting to collect a medical debt barred by the No Surprises Act also may violate the FDCPA. Further, continuing what we observed throughout 2021, a number of states passed, or continued to work to pass, laws in 2022 that heavily regulate medical billing, collection, and credit reporting practices.

In combination with all of these federal and state developments, the three largest credit bureaus announced that they were removing certain categories of medical debts from consumer credit reports beginning July 1, 2022. Specifically, tradelines involving paid medical collection debts and reported medical debts of less than \$500 will be removed. Going forward, medical debts of less than \$500 are not to be reported and the credit bureaus are increasing the time before an unpaid medical collection debt will appear on a consumer's tradeline from six to 12 months.

Debt collectors working on behalf of medical service providers should review their collection procedures as well as the billing, collection, and credit reporting policies of their clients to protect themselves proactively from the aggressive regulatory oversight, enforcement, and civil litigation that already has begun. Coordination with, and education of, their health care provider clients will be critical to reducing potential risk and ensuring continued collectability of medical debt.

The CFPB Targets Convenience Fees

On June 29, 2022, the CFPB issued an advisory opinion declaring that the FDCPA prohibits debt collectors from collecting "pay-to-pay" or convenience fees unless applicable law or the agreement creating the debt expressly authorized that fee. According to the CFPB, debt collectors also risk violating the FDCPA when using a third-party payment processor that charges such fees if the processor remits any amount in connection with that fee to the collector.

The CFPB's opinion and accompanying press release follow a number of recent pronouncements by the agency focusing on what it considers to be "junk fees" and targets any fees incurred by consumers to make payments to a debt collector through a particular channel, such as by phone or online. The opinion serves as a signal to debt collectors and original creditors that the CFPB, along with state regulators, is likely to subject convenience fees to more exacting scrutiny, whether under the FDCPA, the CFPB's authority to prohibit unfair, deceptive, or abusive acts or practices (UDAAP), or state law analogues.

Finally, in its opinion, the CFPB rejected the position adopted by some courts that state contract law permits debt collectors to collect fees that are the subject of a separate agreement. Per the CFPB's analysis, the FDCPA "only permits collecting amounts authorized by contract when the amount is expressly authorized by the contract 'creating the debt.'"

Regulation F Is Slowly Being Interpreted by the Courts

The CFPB's new Regulation F interpreting the FDCPA took effect November 30, 2021. The rule is the first major update to the FDCPA since its enactment in 1977, and gives much-needed clarification on the bounds of federally regulated activities of "debt collectors," as that term is defined in the FDCPA, particularly for communications by voicemail, email, and texts.

Although FDCPA lawsuits were down in 2022, consumer claims targeting Regulation F were largely focused on the following topics:

- **Electronic Communication Opt-Out Notices:** 12 C.F.R. § 1006.6(e) requires debt collectors to provide a "clear and conspicuous" notice in any electronic communication to the consumer describing a "reasonable and simple" method by which the consumer can opt out of such electronic communications.
- **Limited Content Messages:** 12 C.F.R. § 1006.2(j) creates a definition for a type of voicemail that debt collectors could leave for consumers. A "limited content message" that fully complies with Regulation F's requirements is deemed not to be a "communication" and effectively provides debt collectors with a safe harbor from the requirements of 15 U.S.C. §§ 1692c(b), 1692d(6), and 1692e(11).
- **Frequent Calling:** 12 C.F.R. § 1006.14(b)(2) creates a presumption of a violation where more than seven unanswered calls are made per week or where a second conversation is held within seven days—certain exceptions apply and the presumption is rebuttable. These limitations generally apply per account in collection, meaning that if a collector is collecting on three different debts, the allowed calls and conversations triple.



- **Preconditions to Credit Reporting:** 12 C.F.R. § 1006.30(a) now requires collectors to take certain steps to attempt to contact the consumer before furnishing information to CRAs. Before Regulation F, it was possible to report adverse information about the debt with consumer reporting agencies (CRAs) without informing the consumer about the alleged debt.
- **Validation Notices:** 12 C.F.R. § 1006.34 now has new extensive requirements for the content of validation notices and provides a model form for the same. Several new information requirements relate to newly defined terms like the “itemization date.” For example, the validation notice must

disclose the itemization date, the amount owed on the itemization date, the name of the creditor on that date (for consumer financial product or services debts), an itemization of interest, fees, payments, and credits since the itemization date, and the current amount of the debt.

Most cases alleging Regulation F-based claims remain in their early stages, and no court has issued a significant decision interpreting Regulation F. However, it is widely expected that 2023 will see a number of such decisions from both district and circuit courts of appeal as these cases work their way through courts and begin to percolate out in published opinions.



FAIR LENDING

Authors: Lori J. Sommerfield, Chris Willis, Christine R. Emello, Sarah E. Pruett

During 2022, the federal financial institution regulatory agencies, led by the CFPB (Bureau) and the U.S. Department of Justice (DOJ), continued to take an aggressive approach to enforcing the federal fair lending laws (the Equal Credit Opportunity Act (ECOA) and Fair Housing Act (FHA)) against lenders and consumer finance companies. Under the Biden administration, an unprecedented “whole of government” approach is being taken to address redlining practices, root out appraisal bias in residential home lending, and to encourage use of special purpose credit programs to expand access to credit to protected class groups. Federal regulators and Congress have also begun focusing on fair lending risks related to algorithmic bias and digital redlining in marketing and advertising practices, as well as machine-learning and artificial intelligence credit decisioning models.

The CFPB announced in March 2022 that it will begin targeting discrimination as an unfair practice under its unfair, deceptive, and abusive acts or practices (UDAAP) authority, thus vastly expanding the reach of its anti-discrimination enforcement beyond the limits of the ECOA. This policy action, undertaken by the Bureau without notice and comment rulemaking, represents a massive expansion of UDAAP applicability, and the new standard will apply to all consumer financial products and services. The FTC adopted this same view under Section 5 of the FTC Act in an auto dealer case brought in October 2022, asserting that discrimination is “unfair,” just as the CFPB had done earlier in the year. The CFPB also announced that it will issue a final rule implementing Section 1071 of the Dodd-Frank Act by March 31, 2023, to require data collection and reporting for small business loan data collection (including demographic data of principal business owners) in a manner similar to the Home Mortgage Disclosure Act to detect

discrimination in small business lending. This rulemaking will present significant fair lending risks and operational challenges for the financial services industry.

A notable development at the state level over the past year was the New York Department of Financial Services’ settlements with three indirect auto lenders, in which the agency alleged pricing disparities that adversely impacted racial/ethnic protected class groups. To our knowledge, this is the first time a state regulator has pursued fair lending dealer mark-up charges against an assignee of retail installment sales contracts.

Combating Redlining Initiative

In October 2021, the DOJ announced a comprehensive and unprecedented “Combating Redlining Initiative” in which it sought to partner with U.S. attorneys, state attorneys general, and financial regulatory agencies by taking a “whole of government” approach to enforcing the federal fair lending laws. The initiative also seeks to expand the DOJ’s analyses of potential redlining practices to both depository and non-depository institutions. This initiative represents an aggressive and coordinated enforcement effort to address and eradicate redlining that is prohibited by the FHA and the ECOA. Since the launch of this initiative, the DOJ has announced three redlining settlements with a combined \$38 million in relief, and with many more investigations underway. Two of those settlements occurred during 2022 with record settlements. One is discussed below.

During 2022, the DOJ entered into a \$13 million settlement with Lakeland Bank to resolve allegations that it engaged in redlining by avoiding providing loans to prospective applicants and engaging in conduct that would discourage

applications from prospective applicants in Majority-Black and -Hispanic census tracts in the Newark, New Jersey metropolitan area. The consent order provides that Lakeland will invest \$12 million in a loan subsidy fund for residents of Black and Hispanic neighborhoods in the Newark area; spend \$750,000 for advertising, outreach, and consumer education; and invest \$400,000 for development of community partnerships to provide services that increase access to residential mortgage credit. In addition, Lakeland must open two new branches in neighborhoods of color and employ four mortgage loan officers and a community development officer to serve neighborhoods of color in the Newark area. This settlement represents the third-largest redlining settlement in DOJ's history.

Under the Biden administration, an unprecedented “whole of government” approach is being taken to address redlining practices, root out appraisal bias in residential home lending, and to encourage use of special purpose credit programs to expand access to credit to protected class groups.

Section 1071: Small Business Lending Data Collection and Reporting Notice of Proposed Rulemaking

The CFPB announced that its final rule under Section 1071 of the Dodd-Frank Act will be issued by March 31, 2023. The rule requires small business lenders to collect and report certain loan data to the Bureau. The proposed rule was

issued in September 2021, and the CFPB received approximately 2,100 comments on the proposal in January 2022. The proposed rule contains similar requirements to the Home Mortgage Disclosure Act related to data collection and reporting, but is aimed at small business lending.

After the end of the comment period, several Republican U.S. representatives sent a letter to CFPB Director Rohit Chopra, highlighting several “issues of particular concern.” Those included seeking:

- An expansion of the *de minimis* exemption from compliance, which is proposed to be only 25 covered credit transactions;
- A longer implementation period than the proposed 18-month period;
- Elimination of a requirement for a financial institution to “collect at least one principal owner’s race and ethnicity (but not sex) via visual observation or surname” where the applicant chooses not to submit information on race, gender, or ethnicity; and
- Clarity on what collected data will be made public before the data is collected.

Until the CFPB issues its final rule, it is unclear whether there will be any changes to the proposed rule. If the CFPB adopts the implementation period for the rule as proposed, compliance with the final rule will not be required until 18 months after the final rule is issued, although covered small business lenders will be permitted to collect data from applicants beginning approximately 12 months before compliance is required.

Special Purpose Credit Programs

Special purpose credit programs (SPCPs) are lending programs designed to facilitate access to credit to an economically disadvantaged group of people. The ECOA and Regulation B allow creditors to design SPCPs that explicitly consider protected characteristics, such as race, national origin, or sex, as long as certain criteria are met.

In December 2020, the CFPB issued an advisory opinion on SPCPs to address regulatory uncertainty concerning how creditors could develop SPCPs in a manner consistent with Regulation B. The advisory opinion states that for-profit organizations must establish and administer an SPCP “pursuant to a written plan that identifies the class of persons the program is designed to benefit and sets forth the procedures and standards for extending credit pursuant to the program.” The written plan must contain the class of persons the program is designed to benefit, the procedures and standards for extending credit, the time period of the program or when it will be reevaluated for continuation, and a description of the analysis the creditor conducted to determine the need for the program. In addition, the program must be extended to a class of people who would probably not receive such credit or would receive it on less favorable terms.

The Fair Housing Act does not contain any provision that allows SPCPs, and doubts about whether such programs are permissible for mortgage loans (which are covered by the FHA) caused both industry and consumer groups to request guidance on this issue. In December 2021, the U.S. Department of Housing and Urban Development (HUD) released guidance

clarifying its view that SPCPs do not violate the FHA so long as they comply with the ECOA and Regulation B. In February 2022, a number of agencies, including the CFPB, DOJ, Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), HUD, and the Federal Housing Finance Agency (FHFA), issued an Interagency Statement on SPCPs reminding creditors of their ability to create SPCPs under the ECOA and encouraging use of SPCPs in a manner consistent with the ECOA and Regulation B, as well as safe and sound lending principles. The regulators’ guidance and support for SPCPs have encouraged many creditors to develop and implement SPCPs in 2022. We believe that with the advent of the Section 1071 final rule, SPCPs will become more popular in the small business lending context.

Appraisal Bias

In recent years, bias within the appraisal and property evaluation process has garnered the attention of President Biden and prompted discussions among federal government agencies with a stake in residential mortgage lending matters.



On March 23, 2022, the Property Appraisal and Valuation Equity Interagency (PAVE) Task Force issued its Action Plan to Advance Property Appraisal and Valuation Equity to President Biden.

PAVE was created in response to President Biden's June 1, 2021 directive to HUD Secretary Marcia Fudge to lead a "first-of-its-kind interagency initiative to address inequity in home appraisals." The task force was instructed to evaluate the causes, extent, and consequences of appraisal bias and to establish a transformative set of recommendations to root out racial and ethnic bias in home valuations. The scope of the task force's work includes: (1) ensuring that government oversight and industry practice further valuation equity; (2) combating valuation bias through educating the consumer and training the practitioner; (3) ensuring equity in valuation by making available high-quality data; and (4) creating a comprehensive approach to combating valuation bias through enforcement and other efforts.

PAVE's action plan primarily focuses on reducing racial bias in home appraisals. PAVE stated that it will exercise broad oversight and compliance authority to strengthen "guardrails against unlawful discrimination in all stages of residential valuation."

Several federal agencies made public statements in response to PAVE's action plan:

- CFPB Director Rohit Chopra stated that the Bureau will take an active leadership role and will work "to implement a dormant authority in federal law to ensure that algorithmic valuations are fair and accurate." Director Chopra was referring to the CFPB's authority to issue an Automated Valuation Model (AVM) rule, and the Bureau released the report from its small business review of the AVM rule outline on May 13, 2022.
- OCC Acting Comptroller Michael Hsu stated the OCC will enhance its supervisory methods for identifying discrimination in property valuations and will take steps to ensure consumers are aware of their rights regarding appraisals.
- FDIC Acting Chairman Martin Gruenberg stated that the FDIC is committed to taking concrete

actions, including collaborating with PAVE members to exercise authority "to support a more equitable state appraisal certification and licensing system."

On February 23, 2022, the CFPB issued an outline of proposals and alternatives under consideration related to the AVM rulemaking to prevent algorithmic bias in home valuations. Section 1125 of the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA) sets out certain quality control standards for AVMs and authorizes the CFPB, among other federal regulators, to promulgate regulations to implement those quality control standards. Specifically, Section 1125 requires that AVMs meet quality control standards designed to:

- Ensure a high level of confidence in the estimates produced by automated valuation models;
- Protect against the manipulation of data;
- Seek to avoid conflicts of interest;
- Require random sample testing and reviews; and
- Account for any other such factor that the agencies determine to be appropriate.

The outline covers the scope of potential eventual rule requirements related to AVMs. The CFPB appears set on requiring regulated institutions to maintain policies and procedures related to the first four standards listed above to ensure AVMs used for covered transactions adhere to the specific quality control standards. The CFPB is considering specifying "nondiscrimination quality control criteria" as an additional standard under the fifth standard listed above.

Noting that the use of algorithmic systems, such as AVMs, is subject to the ECOA and the FHA, the CFPB states that it is considering the potential positive and negative consumer and fair lending implications of the use of AVMs. In its discussion of fair lending concerns, the CFPB reiterates several points that have become the hallmark of Director Chopra's views on algorithmic systems. The outline provides the following:

- The “black box” nature of many algorithms, including those used in AVMs, introduces additional fair lending concern. The complex interactions that machine-learning algorithms engage in to form a decision can be so opaque that they are not easily audited or understood. This makes it challenging to prevent, identify, and correct discrimination.
- Algorithmic systems can “replicate historical patterns of discrimination or introduce new forms of discrimination because of the way a model is designed, implemented, and used.”

The CFPB requested all small entity feedback on the outline by April 8, 2022, and feedback from other stakeholders by May 13, 2022. The feedback the CFPB received included concerns regarding how small business entities can assess fair lending issues in AVMs or know if they are in violation of the law.

Issuance of a final rule is not on the immediate horizon. The CFPB will still need to issue a notice of proposed rulemaking, which will go through its own comment process, before issuing a final rule. In the outline, the CFPB notes that it is considering a 12-month implementation period once the final rule is issued.

Additionally, the Senate Banking Committee and House Financial Services Committee held hearings on March 24, 2022, to discuss the PAVE Action Plan and need for possible legislation. During the hearings, the draft bill, Fair Appraisal and Inequity Reform (FAIR) Act of 2022, was discussed. This bill proposes to amend FIRREA to establish an independent agency, the Federal Valuation Agency, which would be responsible for creating and maintaining a registry of appraisers.

Modifications to the UDAAP Examination Manual and the FTC’s Assertion That Discrimination Is “Unfair”

In March 2022, the CFPB announced that it will begin targeting discrimination as an unfair practice under its UDAAP authority, vastly expanding the reach of its anti-discrimination enforcement

beyond the limits of the ECOA. This policy action is unprecedented and represents a massive expansion of UDAAP applicability. The CFPB updated its UDAAP Examination Manual to reflect the expansion, providing details about the types of discrimination it intends to address under this new standard.

Though not explicitly mentioned by the CFPB, the updated UDAAP Examination Manual strongly indicates that the CFPB plans to use both disparate treatment and disparate impact analyses as a way of establishing “unfair” discrimination. For example, the manual urges Bureau examiners to consider whether a supervised entity has “a process to take prompt corrective action if the decision-making processes it uses produce deficiencies or discriminatory results.” Further, examiners must consider whether a supervised entity ensures that employees and third-party service providers “refrain from engaging in servicing or collection practices that lead to differential treatment or disproportionately adverse impacts on a discriminatory basis.” This appears to signal that the CFPB believes that the disparate impact doctrine now applies to every aspect of every financial services provider over which the Bureau has jurisdiction.

By expanding the reach of its unfair practices authority to include discrimination, the CFPB now has the power to examine potentially discriminatory practices in both new markets and involving activities outside of its authority under the ECOA. Under the ECOA, discrimination is prohibited only against “applicants” for credit. In its press release, the CFPB specifically noted that it would examine for discrimination in “all consumer finance markets,” including noncredit products like payments, consumer reporting, remittances, and deposit accounts.

In addition, the CFPB specifically highlighted targeted marketing, which typically is considered outside of the scope of the ECOA because viewers of advertisements are not “applicants.” The updated UDAAP Examination Manual states that transaction testing should determine whether a supervised entity “engages in targeted advertising or marketing



in a discriminatory way.” The manual also notes that a supervised entity’s policies, procedures, and practices should “not target or exclude consumers from products and services, or offer different terms and conditions, in a discriminatory manner.” Now, for the first time, the CFPB explicitly asserted that targeted marketing is discriminatory or actionable, although how the Bureau intends to assess targeted advertising remains unclear. Nevertheless, the Bureau’s revised exam manual clearly signaled that the Bureau will examine targeted advertising.

In response to the CFPB’s extraordinary policy action to expand its interpretation of UDAAP, the U.S. Chamber of Commerce, American Bankers Association, Consumer Bankers Association, and three other trade groups filed a lawsuit against the Bureau in September 2022 challenging the CFPB’s UDAAP Examination Manual modifications. See *Chamber of Commerce of the U.S.A., et al. v. CFPB, et al.*, Case No. 6:22-cv-00381-JCB (E.D. Tex. Sept. 28, 2022). The plaintiffs claim that the modifications should be disallowed because: (1) the update exceeds the CFPB’s authority under the Dodd-Frank Act because the Act only grants the CFPB authority to enforce anti-discrimination principles in certain circumstances; (2) the update is arbitrary and capricious; (3) the CFPB did not follow the Administrative Procedure Act’s notice and comment rulemaking procedures in adopting these sweeping policy changes; and (4) the update should be discarded because the CFPB’s funding structure violates the Appropriations Clause of the U.S. Constitution. Notably, in October 2022,

the Fifth Circuit Court of Appeals held that the funding mechanism for the CFPB is unconstitutional because the CFPB does not receive its funding from annual congressional appropriations. Unsurprisingly, defendants in enforcement actions are citing this decision as a basis for dismissal of the lawsuits brought against them and the CFPB has argued that the holding is neither controlling nor correct. The constitutionality of the CFPB’s funding is likely to continue to be a significant issue in 2023.

The Federal Trade Commission also officially took the position that discrimination is “unfair,” and therefore a violation of Section 5 of the FTC Act in a case brought and settled in October 2022, *FTC v. Passport Auto Group*, No. 8:22-CV-2670-GLS (D. Md.). As with the CFPB’s announcement, the FTC’s position opens up products and processes to discrimination claims that are not covered by the ECOA or other specific anti-discrimination statutes, and the FTC’s position is subject to many of the same arguments made by the U.S. Chamber and other trade associations in their lawsuit against the CFPB. We expect parties to push back on the interpretations of “unfair” adopted by both the CFPB and FTC in 2023.

Targeted Advertising

On June 21, 2022, the DOJ filed a lawsuit and a settlement “framework” with Meta Platforms, Inc. (previously known as Facebook) to resolve

allegations that Meta's advertising placement algorithms discriminate against Facebook users based on their race, color, religion, sex, disability, familial status, and national origin (protected characteristics) in violation of the Fair Housing Act. The DOJ action is a direct outgrowth of the discrimination charge filed by HUD against Facebook in 2019.

Specifically, the DOJ alleges:

- Meta enabled and encouraged advertisers to target their housing ads by relying on protected characteristics, or close proxies of such characteristics, to decide which Facebook users will be eligible or ineligible to receive housing ads, at least before 2019;
- Meta created an ad-targeting tool known as "Lookalike Audience," later changed to "Special Ad Audience," for housing, employment, and credit advertisements that uses a machine-learning algorithm that considers protected characteristics in finding Facebook users who share similarities with an advertiser's source audience, and thus are eligible to receive housing ads; and
- Meta's ad delivery system uses machine-learning algorithms that rely in part on protected characteristics to help determine which subset of an advertiser's targeted audience will actually receive a housing ad.

The DOJ's complaint alleges both disparate treatment and disparate impact discrimination under the FHA. The proposed settlement framework provides as follows:

- Meta must stop using the "Special Ad Audience" tool by December 31, 2022.
- Meta must, by December 2022, develop a new system for housing advertisements that addresses disparities for protected characteristics, measured by the disparities between eligible audience members of protected classes and users who actually see an advertisement.
- If the DOJ determines that the new system adequately addresses discriminatory disparities, then Meta must implement the system by December 31, 2022; if not, the settlement

agreement will terminate, and the parties will litigate the suit.

- Meta and the DOJ will select an independent, third-party reviewer to investigate and verify on an ongoing basis whether the new system is meeting agreed-upon compliance standards.
- Meta must not provide any targeting options for housing advertisers that directly describe or relate to protected characteristics and must notify the DOJ if it intends to add any targeting options.
- Meta must pay a \$115,054 civil money penalty, which is the maximum penalty available under the FHA.

Notably, the DOJ's allegations all appear to stem from the alleged actual use of protected characteristics or very close, obvious proxies to protected characteristics. There are disparate impact allegations that relate to the direct use of protected characteristics or the same close proxies. However, even though the allegations are more truly in the nature of disparate treatment, the settlement agreement, vague as it is, seems to adopt a disparate impact style of analysis to see if the problem has been solved by measuring whether ads are actually placed in a nondiscriminatory way based on race, ethnicity, or sex.

Additionally, the DOJ alleged that simply eliminating problematic variables will not solve the problem because the machine-learning algorithms would likely reach the same conclusions using the large amount of other data available to the Facebook ad-targeting algorithm.

Algorithmic Bias

Fair lending laws and their application to algorithmic systems have been a top priority for the CFPB and other federal and state regulators. Director Chopra has been particularly vocal about this topic, noting that "[c]ompanies are not absolved of their legal responsibilities when they let a black-box model make lending decisions," and that "[a]lgorithms can help remove bias, but black box underwriting algorithms are not creating a more equal playing field and only exacerbate the biases fed into them." At the end of 2021, we saw efforts from the White House, Congress, and state legislatures to address

algorithmic bias, and those efforts have continued into 2022.¹

On May 26, 2022, the CFPB issued a press release stating that federal consumer financial protection laws and adverse action requirements should be enforced regardless of the technology used by creditors.² The ECOA and Regulation B require that a creditor provide an applicant with a statement listing specific reasons for an adverse action against an applicant. It is insufficient to state that the adverse action was based on internal standards, policies, or the failure to achieve a qualifying score on the creditor's scoring system. Creditors cannot justify noncompliance with the ECOA based on the mere fact that the technology they used to evaluate credit applications is too complicated, too opaque, or too new in its decision-making. A creditor's lack of understanding its own credit decisioning model does not absolve a creditor of its requirement to list the actual reason(s) for an adverse action.

The District of Columbia has also shown an active interest in regulating algorithmic bias. On December 9, 2021, at the request of District of Columbia's Attorney General Karl Racine, Chairman Phil Mendelson introduced the Stop Discrimination by Algorithms Act of 2021 (B24-0558). The act would prohibit disparate impact, require extensive disclosures to consumers, require audits of models, and require users of models to file detailed reports of their audit results with the District of Columbia Attorney General. On September 22, 2022, dozens of industry participants, attorneys, and other stakeholders provided commentary at a public hearing on the proposed act.

The act, if passed, would prohibit covered entities from making an algorithmic eligibility determination or an algorithmic information availability determination on the basis of an individual's or class of individuals' actual or perceived race, color, religion, national origin, sex, gender identity or expression, sexual orientation, familial status, source of income, or disability in a manner that segregates,

discriminates against, or otherwise makes important life opportunities unavailable to an individual or class of individuals. In addition, any practice that has the effect or consequence of violating the above prohibition would be deemed to be an unlawful discriminatory practice.

The act also requires that each covered entity using an algorithm for decision-making:

- Audit its algorithmic eligibility determination and algorithmic information availability determination practices to determine, among other things, whether such practices are discriminatory;
- Annually send a report of the above-mentioned audit to the District of Columbia Attorney General's office;
- Send an adverse action notice to affected individuals if the adverse action is based in whole or in part on the results of an algorithmic eligibility determination;
- Develop a notice that details how it uses personal information in algorithmic eligibility determinations and algorithmic information availability determinations;
- Send the above-mentioned notice to affected individuals before its first algorithmic information availability determination and make the notice continuously and conspicuously available; and
- Require service providers by written agreement to implement and maintain measures to comply with the Act if the covered entity relies in whole or in part on the service provider to conduct an algorithmic eligibility determination or an algorithmic information availability determination.

The District of Columbia Attorney General's office would have enforcement authority for the act, including the ability to impose civil money penalties of \$10,000 for each violation. For individual claimants, the act includes a private right of action, where aggrieved persons may recover up to \$10,000 per violation. In addition, either action

¹ In October 2022, the White House Office of Science and Technology Policy released its "Blueprint for an AI Bill of Rights," a nonbinding white paper intended to support the development of policies and practices in the building, deployment, and governance of automated systems. In Congress, bills such as the Algorithmic Accountability Act and the Algorithmic Fairness Act were introduced, aimed at promoting ethical AI decision-making, and at the state level, at least 17 state legislatures introduced AI legislation in 2021.

² Consumer Financial Protection Bureau, Circular 2022-03 (May 26, 2022).



could result in the violating party paying punitive damages and/or attorney's fees.

Notable State Fair Lending Developments

During 2021-2022, the New York Department of Financial Services (NYDFS) demonstrated its continued focus on aggressively enforcing New York fair lending law,³ particularly in the auto finance space, against New York-chartered banks. The NYDFS' recent focus on fair lending enforcement in the indirect auto finance market occurred after announcing in 2018 that it would pick up where the CFPB left off in enforcing fair lending laws against indirect auto lenders after Congress curtailed those efforts by the Bureau.⁴

As background, in 2021, the NYDFS entered into consent orders with two relatively small New York-chartered trust companies, Adirondack Trust Company (Adirondack) and Chemung Canal Trust Company (Chemung),⁵ that engaged in indirect auto financing by serving as a source of auto

financing for a network of third-party auto dealers. NYDFS alleged that the companies' practices resulted in racial and ethnic minorities paying higher interest rates than non-Hispanic white borrowers for automobile loans. The companies set a risk-based interest rate (buy rate) for approved loan applications and dealers had the discretion to mark up the interest rates above the buy rate. The difference between the buy rate and the consumer's rate is the "dealer mark-up." Although the loan files did not contain information on the borrowers' race or national origin, the NYDFS assigned race and national origin probabilities to applicants by using the Bayesian Improved Surname Geocoding (BISG) proxy methodology (also used by the CFPB), which identified statistically significant disparities in dealer mark-up on the basis of race or national origin. The NYDFS alleged that, as a result of disparate impact caused by Adirondack's and Chemung's pricing policies, racial and ethnic minorities were charged a higher average dealer mark-up than non-Hispanic white borrowers. NYDFS required each bank to pay civil penalties, make restitution

³ New York Executive Law Section 296-a.

⁴ In 2018, Congress overrode the CFPB's 2013 auto finance fair lending bulletin through use of the Congressional Review Act. Specifically on May 21, 2018, President Donald Trump signed a joint resolution passed by Congress disapproving the CFPB's Bulletin 2013-02 titled "Indirect Auto Lending and Compliance with the Equal Credit Opportunity Act," which had provided guidance about the ECOA and its implementing regulation, Regulation B. Consistent with the joint resolution, the bulletin now has no force or effect.

⁵ Each bank had between \$1 billion and \$2 billion in assets.

to borrowers, and implement remedial measures. Specifically, Adirondack agreed to pay a \$275,000 penalty to New York state, restitution to impacted borrowers, and make a \$50,000 contribution to local community development organizations. Chemung agreed to pay a \$350,000 penalty, restitution to impacted borrowers, and agreed to undertake remediation efforts designed to increase Chemung's monitoring of dealers participating in its indirect automotive lending program.

Importantly, these two 2021 indirect auto lender settlements represent the first effort by a state regulator to pursue fair lending dealer mark-up charges against an assignee of retail installment sales contracts of which we are aware. Second, the forward-looking relief in the Chemung Canal Trust Company consent orders goes well beyond that required in the CFPB's auto finance consent orders. Adirondack Trust Company had exited the indirect auto finance business in 2017, but Chemung, which was still operating at the time of the settlement, was required under the NYDFS consent order to adopt a flat-fee pricing model, with no exceptions.

In October 2022, the NYDFS entered into a consent order with Rhinebeck Bank, a New York-chartered bank, to resolve similar allegations that the bank violated New York's Fair Lending Law and the ECOA by underwriting and purchasing indirect automobile loans from dealers where Black, Hispanic, and Asian borrowers were charged a higher average dealer mark-up than non-Hispanic white borrowers. Similar to the facts in the NYDFS 2021 consent orders, the dealers had discretion to increase dealer mark-up above the buy rate under Rhinebeck Bank's pricing policy. The NYDFS determined that the bank's policies permitted dealers to mark up applicants' interest rates, which resulted in a disparate impact on the basis of race and national origin. The bank agreed to pay a penalty of \$950,000, pay restitution to impacted consumers, and implement changes to its fair lending compliance program.

The CFPB has not publicly pursued auto finance pricing disparity issues since Congress overrode its 2013 fair lending auto finance bulletin in 2018, and even abandoned active matters it was pursuing in supervision and enforcement. Nonetheless, dealer mark-up issues could resurface as an area of CFPB focus in light of these NYDFS developments.

Looking Forward

We expect that the CFPB and DOJ, together with other federal financial institution regulatory agencies and the FTC, will continue to aggressively enforce the federal fair lending laws in 2023. Redlining investigations and enforcement actions will continue to be a top priority under the "Combating Redlining Initiative," and we are aware that many are currently in the pipeline. It will remain to be seen how the CFPB implements its policy to enforce discrimination as an unfair practice under UDAAP, and ideally, the Bureau should provide more guidance to the industry about its new UDAAP examination approach and appropriate risk mitigation measures. But regardless of how the CFPB uses UDAAP in the context of discrimination, there is no doubt that the Bureau will pursue claims under the ECOA with great vigor. The industry should also prepare for issuance of the CFPB's final rule implementing Section 1071 of the Dodd-Frank Act on small business lending data and reporting requirements, which is scheduled to be issued by March 2023, and which will present a new set of fair lending concerns and corresponding legal, regulatory, and reputational risks. Financial institutions and practitioners in the consumer financial services space should closely monitor these developments, as well as emerging fair lending and UDAAP issues, in this rapidly changing environment in which fair lending compliance and eradicating unfairness are top regulatory priorities.

FINTECH

Authors: James Kim, Jeremy T. Rosenblum, Caleb N. Rosenberg, Jeremy C. Sairsingh, Rene T. McNulty

Buy Now, Pay Later

Background

A now-ubiquitous segment of consumer credit is the “buy now, pay later” (BNPL) industry. BNPL is most widely associated with no-interest, four-payment installment loans or “Pay in 4” made available via integrations on online merchant websites and virtual cards generated in shopping apps offered by BNPL providers.

The prototypical example of a Pay in 4 is an extension of credit for the purchase of goods or services, typically in the \$50-\$1,000 range, from an online merchant. The customer pays 25% of the purchase, and the remaining balance is repaid every two weeks in three equal installments, and the customer pays no interest or fees if the obligation is repaid on time.

The range of products offered through companies regarded as BNPL providers is constantly growing, and—sometimes as part of a bank partnership—now include charge cards, interest-bearing closed-end loans, and direct-debit, non-credit payment products. Enabling in-store purchases has become an important focus for BNPL companies, variable down payment percentages are more common, and some previously “free” products now include origination charges and other fees. Nevertheless, it is the Pay in 4 product that has garnered the most attention from federal and state regulators, and remains synonymous with BNPL.

The sector experienced rapid growth over the past few years, with product usage accelerating in tandem with the pandemic-fueled surge in online shopping. As more American consumers began seeing one or more BNPL icons at online checkout screens, the CFPB and other regulators began taking notice of this popular “new” way to pay for online purchases. The extent to which Pay in 4 was in fact something novel, or whether it was just the latest iteration of a layaway, became a key

question for regulators. Some of the product’s core features — no interest or fees paid by the customer if the obligation is paid on time and no more than four payments — meant that Reg. Z closed-end disclosures were not required, something the CFPB would later characterize as “regulatory arbitrage.” Similarly, in contrast to credit cards, which are subject to substantive Reg. Z requirements such as ability to repay, dispute procedures, and late fee limits, no comparable uniform requirements govern Pay in 4 transactions at the federal level. While some states, like California, require licenses to offer Pay in 4-like products, many other state licenses are only triggered by interest or other finance charges. Additionally, BNPL providers began offering shopping apps that expanded the reach of Pay in 4 and other credit products to a much wider array of online merchants than those with whom the provider might have a direct relationship and site-level integration using the provider’s APIs.

In short, BNPL generally and Pay in 4 in particular have quickly become one of the most popular forms of everyday consumer credit. As demonstrated by the developments discussed below, increased regulation of this sector appears a near certainty.

CFPB Takes Notice: Industry Inquiries and Public Comment Requests

In 2020, the CFPB began an information gathering process that culminated in December 2021 marketing monitor orders issued to five of the largest BNPL providers. These orders bore some resemblance to orders sent to five “tech giants” in October 2021, but were directly focused on the BNPL providers’ Pay in 4 offerings, requesting detailed answers and responsive data to an extensive set of questions. In issuing these orders, the CFPB emphasized that its key concerns regarding the BNPL market were: (1) debt accumulation; (2) regulatory arbitrage; and (3) data harvesting.



The CFPB also solicited public input in January 2022, asking for comments responding to the following questions about the BNPL market:

- What is the buyer experience with BNPL?
- What are the benefits and risks?
- What is the merchant experience?
- What perspectives do regulators and attorneys general have with respect to BNPL products?
- Are there ways in which the BNPL market can be improved?

After analyzing responses from the five BNPL providers and public comments, the CFPB issued a report in September 2022 titled, “Buy Now, Pay Later: Market trends and consumer impacts.” Many of the key takeaways relate to the concerns around debt accumulation, regulatory arbitrage, and data harvesting that the CFPB had articulated in issuing its initial orders. Some of the report’s key takeaways are:

- The financial and operational benefits of the interest-free, accessible at your fingertips product over legacy credit products are real and sizable. According to the CFPB, however, those same benefits may lead to two forms of borrower overextension: loan stacking (the risk of overconsumption from BNPL usage at multiple concurrent lenders) and sustained usage (the risk of long-term BNPL usage causing stress on borrowers’ ability to meet other, non-BNPL financial obligations).

- Consumer reporting companies have been slow to develop credit reporting protocols with respect to BNPL. Mortgage and auto lenders have raised concerns that the growth of BNPL with no associated credit reporting makes it more challenging to know whether a borrower can afford a mortgage or auto loan.
- Credit performance is deteriorating on BNPL loans. In 2020, 2.9% of borrowers “charged off” a BNPL loan, while that number jumped to 3.8% in 2021. Public filings show this upward trend continuing through the first half of 2022.
- BNPL lenders often collect a consumer’s data, as well as deploy models, product features, and marketing campaigns based on that data, to increase the likelihood of incremental sales. The CFPB claims that in addition to general data harvesting risks, BNPL lenders’ use of consumer data for revenue-generating purposes can potentially increase overextension risks by engendering repeat usage.

In prepared remarks, CFPB Director Rohit Chopra acknowledged both the advantages and disadvantages of BNPL. “Since taking office, I have directed our staff to identify ways to invite more competition into markets for consumer financial products and services. Buy Now, Pay Later firms are challenging existing players and offering new options to retailers and borrowers.” Chopra noted, however, that “[m]any Buy Now, Pay Later lenders are not offering the same clear set of dispute protections that credit card issuers

have long been required to offer, which is creating chaos for some consumers when they return their merchandise or encounter other difficulties. Many Buy Now, Pay Later lenders do not offer clear and comparable disclosures of the terms of the loan like other lenders.”

The report and prepared remarks state actions the CFPB intends to take. These include:

- Identifying potential interpretive guidance or rules to issue to ensure that BNPL firms adhere to many of the baseline protections that Congress has already established for credit cards.
- Identifying data surveillance practices that may need to be curtailed – specifically, examining some of the types of demographic, transactional, and behavioral data collected for uses outside of the lending transaction, including for the purpose of sponsored ad placements, sharing with merchants, and developing user-specific discounting practices.
- Identifying options for appropriate and accurate credit reporting on these products.
- Ensuring that BNPL companies are subjected to appropriate supervisory examinations, just like credit card companies.
- Ensuring that the CFPB and the Federal Reserve System methodology used to estimate household debt burden reflects the reality of today’s market.

Chopra’s statement noted that “the report prepared by the CFPB staff does not seek to determine whether the rise of the Buy Now, Pay Later market is a positive or negative development. I believe that Buy Now, Pay Later can grow and serve consumers well if we can collectively address some of the gaps I’ve just outlined. If Buy Now, Pay Later lenders incorporate the protections and protocols that we observe in other financial products, this would go a long way to ensure that there is healthy competition where consumers have a baseline level of protections.”

CFPB Authority to Regulate BNPL Sector: Larger Participant Rule and Risk-Based Supervision

Because the CFPB lacks express supervisory authority over nonbank installment lenders,

including those offering point-of-sale purchase money loans, the CFPB had to rely on separate authority to gather detailed information about how American consumers were using this emerging form of credit. In requesting troves of data from these BNPL companies, the CFPB thus relied on its “marketing monitoring” authority under Section 1022(c) of the Dodd-Frank Act, which requires the CFPB to “monitor for risks to consumers in the offering or provision of consumer financial products or services, including developments in markets for such products or services.”

A future path to more direct supervision over BNPL providers would be a larger participant rule for installment lenders. The CFPB has previously promulgated larger participant rules for other industry sectors, bringing within the Bureau’s supervisory authority motor vehicle finance, student loan servicing, consumer reporting, consumer debt collection, and international money transfer market participants. In 2015, the CFPB under former Director Cordray had signaled its intent to develop a rule to define nonbank larger participants in the market for personal loans, but in 2018, under Acting Director Mick Mulvaney, the CFPB reclassified the larger participant rulemaking in this area as inactive. To date, the CFPB under Chopra has not revived the rulemaking, but there are increasingly calls for the Bureau to do so. For example, in September 2022, the Consumer Bankers Association and Center for Responsible Lending—strange bedfellows perhaps—filed a joint petition urging the Bureau to define larger participants in the market for personal loans.

Even if no such rule materializes in the near future, the CFPB may claim another basis for authority if it seeks to exercise supervisory authority over BNPL providers. In April 2022, the CFPB invoked a “dormant” legal authority to examine nonbank financial companies “that pose risks to consumers.” In short, the CFPB has previously unused authority to regulate nonbank entities when it “has reasonable cause to determine” that an entity providing consumer financial products or services “poses risks to consumers.” In 2013, the CFPB issued a rule addressing how such risks are assessed, but the authority has never been used to supervise a nonbank entity not otherwise subject to the Bureau’s supervisory authority. Given the CFPB’s

increased focus on the BNPL sector, it would not be surprising if the Bureau uses information acquired in its BNPL data gathering exercise to assert supervisory authority over one or more BNPL providers.

The extent to which Pay in 4 was in fact something novel, or whether it was just the latest iteration of a layaway, became a key question for regulators. Some of the product's core features –no interest or fees paid by the customer if the obligation is paid on time and no more than four payments – meant that Reg. Z closed-end disclosures were not required, something the CFPB would later categorize as “regulatory arbitrage.”

FTC Weighs In

In addition to the CFPB, the FTC has also focused its attention on BNPL. In September 2022, the FTC issued its own guidance titled, “Buy now, pay later – and comply with the FTC Act immediately.” Specifically, the FTC outlined three key principles that BNPL providers and other companies should consider in the course of making BNPL products available to consumers:

- All BNPL claims must be supported by reliable data and accurate for the typical consumer, not just for a subset of consumers. The FTC emphasized that the FTC Act's requirement

of truthfulness applies not just to “the cost of a product or the terms of the transaction, [but also] associated fees” For example, the FTC explained that a payment plan would be deceptive if it were advertised as “zero cost,” but the typical customer actually incurred fees.

- Avoid “[dark patterns](#)” (design practices that manipulate users into making choices they would not otherwise have made) by viewing the transaction through consumers’ eyes and focusing on the consumers’ understanding of the material terms. Given the vast amounts of data and information that companies can harvest about consumers’ demographics and habits, the FTC warns companies not to focus on “conversion” of getting consumers to become customers, as it risks hiding or obscuring material information from consumers. The FTC stated an example of this is a user interface that offers BNPL by requiring users to navigate a maze of screens, using nondescript dropdowns or small icons, or burying information in dense terms of service.
- If things go wrong, assume liability and do not disclaim it by pointing to others in the chain of commerce. For example, if a customer returns a product purchased through a BNPL plan, cancels the order, or has the order canceled by a retailer, the customer must get a timely refund or every “company that made misleading claims about what would happen in those circumstances” is liable under the FTC Act. Also, any delay or time spent getting the refund counts as an injury under the FTC Act, especially if the consumer had to wait a long time or do the legwork of calling a company several times.

State-Level Scrutiny and Regulation

At the state level, regulatory scrutiny of BNPL started in earnest in 2019 when the California DFPI formally took the position that Pay in 4 products, as offered by a number of key industry participants, were loans requiring a lending license. The result was a series of settlements with various providers, with providers of Pay in 4 products acceding to the BNPL view that these products are properly treated as loans under California law. In the ensuing years, a number of states have taken the position that Pay in 4 transactions fall within the scope of existing

lending laws, and several states have amended their lending statutes in a manner that directly addresses BNPL. For example, in 2022 New Mexico expanded its Small Loan law to cover certain loans that bear no finance charge.

As the CFPB was putting the BNPL industry under a magnifying glass, a number of states expressed urgency around increasing regulatory oversight of the sector. In March 2022, 19 state attorneys general (state AGs) responded to the CFPB's request for public comment, penning a letter in support of the CFPB's efforts and offering the following recommendations to the Bureau:

- First, the state AGs pointedly criticized BNPL companies for failing to provide robust underwriting or any consideration of a consumer's ability to repay the "loan." Consequently, the state AGs asked the CFPB to identify which steps, if any, these companies take to assess a consumer's ability to repay.
- Second, the state AGs encouraged the CFPB to analyze BNPL providers' relationships with credit reporting agencies to ensure that the companies are furnishing accurate information to credit bureaus and addressing consumer credit reporting disputes in a fair and timely fashion.
- Third, the state AGs recommended that the CFPB evaluate the disclosures that BNPL companies are making to consumers and, if necessary, make regulations to ensure proper disclosures of reasonable fees and charges.
- Fourth, because some BNPL companies may not provide the same protections as credit card companies related to returning and disputing faulty merchandise, the state AGs asked the CFPB to review the dispute resolution processes from BNPL providers.
- Fifth, recognizing the potential for consumers to be overwhelmed with payments, the state AGs encouraged the CFPB to review BNPL providers' debt collection practices when consumers default on their payments.

- Sixth, aligned with the CFPB's concern regarding data collection, the state AGs recommend that the CFPB review BNPL companies' privacy policies to determine how they collect, use, and protect consumer data.
- Finally, the state AGs urged the CFPB to examine partnerships between BNPL companies and providers of unaccredited online courses, such as "tech boot camps that have established partnerships with non-bank lenders."

Because of the current litigation challenging the constitutionality of the CFPB's funding from the Federal Reserve (rather than from congressional appropriations), states may increase their activity or coordinate with the CFPB in the BNPL space.

As the CFPB was putting the BNPL industry under a magnifying glass, a number of states expressed urgency around increasing regulatory oversight of the sector.

Significant Regulatory Changes in 2022 for Small Business Finance Providers

2022 brought a continuation of the consumerization of small business finance with significant state legislative and regulatory activity. This included California's disclosure regulations becoming effective, registration and disclosure requirements being imposed by Utah and Virginia, and revised proposed disclosure regulations in New York. Additionally, the CFPB announced a deadline for issuing a final rule under Section 1071.

California

After years of proposals, comments, and revisions, California's commercial financing disclosure regulations became effective on December 9, 2022. These regulations have been in the works since the passage of SB 1235 in 2018. As a result, California now requires consumer-like disclosures for certain commercial financing products such as small business loans, factoring contracts, and accounts receivable purchase transactions (commonly known as merchant cash advances, or MCAs). The disclosure requirements apply to those commercial financing transactions of \$500,000 or less. The statute contains exceptions for, among other things, depository institutions, commercial mortgages, transactions of \$50,000 or more with a motor vehicle dealer or rental company, and *de minimis* transactions. However, despite the exemption for depository institutions, the regulations expressly apply to certain partners of depository institutions. As a result, banks must determine applicability of the regulations to appropriately assess their partners' compliance practices.

The California regulations require providers of commercial financing to give businesses financing-specific disclosures in the precise language and format detailed by the regulations at the time the provider extends the commercial financing offer. The format requirements detail specific rows and columns that must be used for a disclosure table and the terms that must appear in each section of the table.

Despite significant pushback from industry groups during the rulemaking process, the regulations require an APR disclosure for all product types, including sales-based financing transactions such as merchant cash advances. The regulations provide information about how the APR disclosure must be calculated.

New York

In 2022, New York issued updated proposed regulations implementing the state's Commercial Finance Disclosure Law (CFDL). The CFDL and the proposed regulations are similar to California's now finalized disclosure requirements, including using similar disclosure format. However, there are several

notable differences in the states' requirements. For example, New York but not California requires disclosure of certain fees and of collateral.

New York completed accepting comments on the proposed regulations at the end of October 2022. The proposed regulations also provide a compliance date of six months after the publication of the Notice of Adoption of the regulations in the State Register.

Utah

Utah passed the Commercial Financing Registration and Disclosure Act (CFRDA) into law. Under the CFRDA, beginning January 1, 2023, commercial financing providers must register with the Utah Department of Financial Institutions (Department) and provide certain disclosures. The CFRDA requires a "provider" of commercial financing transactions to register annually with the Department and pay a fee, unless an exemption applies. A "commercial financing transaction" includes a commercial loan, a commercial open-end credit plan, and an accounts receivable purchase transaction. A "provider" is a person who offers more than five commercial financing transactions in Utah in any calendar year. While there are several exemptions from the CFRDA for certain entities and types of transactions, including depository institutions and certain subsidiaries, the term "provider" includes a person who, under an agreement with a depository institution, offers one or more commercial financing products provided by the depository institution via an online platform that the person administers.

To register, a provider must provide specified information through the Nationwide Multistate Licensing System and Registry (NMLS), including information about certain control persons relating to specified criminal convictions. The department may issue a rule requiring additional information.

The CFRDA requires a provider to give certain disclosures before consummating a commercial financing transaction. However, the disclosure requirements are far less burdensome than California and impending New York requirements,

and do not at present include APR or similar rate disclosures. Rather, for all commercial financing transactions, the CFRDA requires the following disclosures:

- The amount of funds provided to the business under the terms of the commercial financing transaction, and the amount disbursed to the business, if less than the amount of funds provided;
- The total amount to be paid to the provider;
- The total dollar cost of the commercial financing transaction, which is the difference between the amount provided to the business and the amount to be paid to the provider;
- The manner, frequency, and amount of each payment, or an estimated amount of an initial payment if the payments vary;
- Information about costs or discounts associated with prepayment; and
- Any amounts provided to the business under the agreement that will be paid by the provider to a broker.

The agreement also must include a description of the method of calculating any variable payments and the circumstances under which payments may vary.

For commercial open-end credit plans, the disclosures also must be provided after any

disbursement of funds. Those disclosure requirements apply to a commercial financing transaction consummated after January 1, 2023. The Department may also require additional disclosures in the future but has not yet issued regulations.

Virginia

Similar to Utah, Virginia passed a disclosure and registration law in 2022. However, Virginia limited its requirements to sales-based financing transactions of \$500,000 or less.

Effective November 1, 2022, Virginia registration requirements apply to both providers and brokers of sales-based financing. The law also requires disclosure of nine specific items, not including an annual rate, and regulations now require use of a model form.

Under the law, a provider is a person that extends a specific offer of sales-based financing to a recipient. It also includes a person that solicits and presents offers of sales-based financing under an exclusive contract or arrangement with a provider.

A broker is a person who for compensation or in the expectation of compensation obtains or offers to obtain sales-based financing from a provider for a recipient. However, regulations clarify that a broker does not include an employee of a provider.



The law also has exemptions for financial institutions (but not companies partnering with financial institutions), providers and brokers with no more than five sales-based financing transactions in 12 months, and individual sales-based financing transactions of more than \$500,000.

Section 1071

In July 2022, the CFPB agreed to a March 31, 2023 deadline to issue a final rule under Section 1071 of Dodd-Frank, which amended the Equal Credit Opportunity Act (ECOA) to impose significant data collection requirements on small business creditors. The CFPB accepted the deadline as part of a previously agreed litigation settlement initiated by The Democracy Forward Foundation regarding alleged delays in the rulemaking process. The court accepted the deadline and maintained jurisdiction over the matter to oversee compliance with the settlement and to address any potential requests for modification.

The Bureau also issued a summary of the proposed rule and a chart of the data points that the rule will require creditors to collect, and it accepted approximately 2,100 comments on the proposal in January 2022. After the end of the comment period, a number of Republican members of Congress sent a letter to Chopra, highlighting several “issues of particular concern.” The authors of the letter sought, among other things:

- An expansion of the *de minimis* exemption from compliance, which is proposed to be only 25 covered credit transactions;
- A longer implementation period than the proposed 18-month period;
- Elimination of a requirement for a financial institution to “collect at least one principal owner’s race and ethnicity (but not sex) via visual observation or surname” where the applicant chooses not to submit information on race, gender, or ethnicity ; and
- Clarity on what collected data will be made public before the data is collected.

In advance of the CFPB’s issuance of its final rule, it is unclear what, if any, changes will be made to the proposed rule.

Enforcement Proceedings

State Consent Orders and Enforcement Proceedings Against Participants in Bank-Model Lending Programs: 2022 and the end of 2021 saw significant developments in litigation and enforcement actions involving bank partnerships.

At the end of November 2021, the District of Columbia Attorney General (D.C. AG) announced a settlement with Opportunity Financial, LLC (OppFi) concerning OppFi’s high-rate loan program with FinWise Bank, a Utah state-chartered bank. Under the settlement, predicated on the contention that OppFi and not FinWise was the “true lender” for the loans in question, OppFi agreed to pay \$1.5 million to refund DC consumers charged rates in excess of DC limits, to waive over \$640,000 in interest owed by those consumers, and to pay \$250,000 to the district. Subsequently, in February 2022, the DC A.G. settled a similar “true lender” lawsuit against Elevate Credit, Inc. for at least \$3.3 million of consumer redress and \$300,000 of interest waivers, together with a \$450,000 payment to the district.

In March 2022, OppFi brought suit against the California Department of Financial Protection and Innovation (DFPI), seeking to block the DFPI from shutting down OppFi’s California high-rate installment lending program with FinWise Bank. OppFi argued that, under California law, state banks such as FinWise are not subject to usury limitations on loans that they make. FinWise was not a party to the lawsuit. In April 2022, the DFPI filed a cross-complaint against OppFi, arguing that OppFi, not FinWise, was the true lender and, accordingly, the loans were subject to California rate limitations. The cross-complaint sought to, among other things, permanently enjoin OppFi’s California activities, a declaration that all OppFi consumer loans made in violation of California law were void, an order requiring OppFi to make restitution to all borrowers under OppFi consumer loans made in violation of California law, disgorgement of payments of interest and other charges received by OppFi in connection with those loans, and a penalty of at least \$100 million.

OppFi moved to dismiss the DFPI cross-complaint based on FinWise's status as the bank making the loans. However, in September 2022, a California trial court denied the OppFi motion, ruling that the DFPI had sufficiently alleged that OppFi was the true lender. In doing so, the court effectively adopted the DFPI's view that the bank partnership was a "rent-a-bank ruse" based on the facts that: (1) OppFi had a "prearrangement" to purchase the loans shortly after origination; (2) the bank only funds the loans if "fully secured by OppFi"—including a purchase requirement insulating the bank from credit risk; (3) OppFi covered all of the bank's out-of-pocket expenses and paid a fee based on the principal amount of the loans; (4) the loans were solely available through OppFi; and (5) OppFi performed all marketing, underwriting, and servicing for the loans. Notably, the court brushed aside in a footnote prior federal-court decisions, *Sims v. Opportunity Fin., LLC*, 2121 WL 1391565 (N.D. Cal. 2021) and *Beechum v. Navient Solutions, Inc.*, 2016 WL 5340454 (C.D. Cal. 2016), which had refused to apply California usury laws to bank loans made in partnership with third-party nonbank agents. In the view of the DFPI trial court, the federal-court decisions were not persuasive. It is important to note that the DFPI decision was not a final decision on the merits and, also, did not directly address whether California usury laws were preempted here under Section 27 of the Federal Deposit Insurance Act.

FTC UDAP Consent Order Regarding "Dark Patterns": This past year, the Federal Trade Commission (FTC) entered into a consent order with a personal finance company to settle the FTC's claims that the company engaged in deceptive acts and practices in violation of Section 5 of the FTC Act. The FTC alleged that the company used misleading claims that consumers were "pre-approved" and had "90% odds" of being approved for credit to entice them to apply for offers, even though many of these consumers did not ultimately qualify for such offers. Under the FTC Act, the FTC has the authority to take action against companies for engaging in unfair and deceptive acts or practices. The order

required the company to pay \$3 million to the FTC to be used for consumer redress (and related administrative expenses).

The company provides services that allow consumers to monitor their credit scores and credit reports. To use the company's services, consumers must sign up for an account and become a member, which includes providing the company with personal information. The company uses this information to send targeted advertisements and recommendations to members for third-party financial products.

In its complaint, the FTC alleged that from February 2018 to April 2021, the company represented in advertisements and recommendations to members that they had been "pre-approved" for third-party financial products, despite the fact that nearly one-third of the consumers who received and applied for "pre-approved" offers were subsequently denied based on the financial product companies' underwriting review (i.e., the actual process by which approval is determined). The complaint alleged that the company knew that its prominent pre-approval claim conveyed false "certainty" to consumers and employed it deliberately to influence consumers' behavior. The FTC also alleged that to the extent the company revealed that consumers' likelihood of getting approval was anything less than certain, it did so by making additional false claims that consumers' likelihood of approval was 90%, or by using buried disclaimers.

The complaint claimed that the company knew that its purported "pre-approvals" and "90% odds" language conveyed false "certainty" to consumers based on the results of experiments, also known as A/B testing, showing that consumers were more likely to click on offers saying "pre-approved" than those saying they had "excellent" odds of being approved. When user interfaces are designed to trick consumers into taking actions in a company's interest and that lead to consumer harm, such design tricks have been described as "dark



patterns.” The complaint alleged that the company deployed dark patterns to misrepresent that consumers were “pre-approved” for credit offers.

In addition to paying \$3 million to the FTC, the consent order prohibited the company from deceiving consumers about whether they are approved or pre-approved for a credit offer, as well as about the odds or likelihood that a consumer will

be approved for a credit offer, and also required the company to preserve records of any market, behavioral, or psychological research, or user, customer, or usability testing, including any A/B or multivariate testing, copy testing, surveys, focus groups, interviews, clickstream analysis, eye or mouse tracking studies, heat maps, or session replays or recordings, to help prevent further use of deceptive dark patterns.

MORTGAGE

Authors: Jon S. Hubbard, Jason E. Manning, Megan E. Burns, Nicole K. ElMurr, Jonathan M. Kenney, Arien N. Parham, Mark J. Windham

The Inconvenient Direction of Convenience Fee Litigation

As an alternative to traditional payment by mail, mortgage lenders and servicers generally offer several different payment options to customers seeking to make their monthly mortgage payments, including online payment, payment through mobile applications, automatic ACH payment, and payment by telephone—either via a live customer representative or via interactive voice recognition. In recent years, mortgage servicers have come under increasing scrutiny as a result of fees charged for providing many of these payment services. Plaintiffs’ attorneys have seized on what are commonly termed “convenience fees” to fuel class action litigation across the country, aimed at numerous financial services industries, including mortgage servicing. Until this year, no federal circuit court had weighed in on the validity of convenience fees under federal or state law, and federal district courts had issued a variety of conflicting decisions. On January 19, 2022, the Fourth Circuit issued its decision in *Alexander v. Carrington Mortgage, LLC*, 24 F.4th 370 (4th Cir. 2022), ruling that under the Maryland Consumer Debt Collection Act, which incorporates the Fair Debt Collection Practices Act (FDCPA), a mortgage servicer is a “collector,” and the \$5 convenience fee charged was an “amount” being collected. To avoid liability, the court held the fees must be specifically authorized in the mortgage contract.

The FDCPA prohibits “[t]he collection of any amount (including any interest, fee, charge, or expense incidental to the principal obligation) unless such amount is expressly authorized by the agreement creating the debt or permitted by law.” 15 USC § 1629f(1). Federal district courts have reached conflicting results when faced with motions to dismiss convenience fee claims on the grounds that a fee paid for the convenience of making payment over the phone or online

is not a “debt” or “claim” and not “incidental to the principal obligation” because it arises from a separate optional service contract. For example, in *Caldwell v. Freedom Mortg. Corp.*, 2020 U.S. Dist. LEXIS 147456 (N.D. Tex. Aug. 14, 2020), the court held that a convenience fee was incidental to the principal debt; simply making the fee optional does not insulate it against a relationship to the principal obligation. *Id.*; *Williams v. Lakeview Loan Servicing LLC*, 2020 U.S. Dist. LEXIS 240472, *8 (S.D. Tex. Dec. 22, 2020) (same); *Fuentes v. AR Res., Inc.*, 2017 U.S. Dist. LEXIS 48923, at *25 (D. N.J. March 31, 2017) (it is immaterial that the fee was optional and disclosed, noting that the majority of cases in the circuit have held that such fees are incidental to the principal obligation).

Other courts have held that optional service fees are not “debts” or “claims” being collected by the mortgage servicer, and therefore, are not “incidental to the principal obligation.” In *Thomas-Lawson v. Carrington Mortg. Servs., LLC*, 2021 U.S. Dist. LEXIS 65841 (C.D. Cal. April 5, 2021), for instance, the court held that nothing in the FDCPA prohibited an offering to enter into a new contract with the debtor for the added convenience of paying by phone. This new contract did not result in a debt or claim being collected. *Id.*; see *Austin v. Lakeview Loan Servicing, LLC*, 2020 U.S. Dist. LEXIS 231824 (D. Md. Dec. 10, 2020) (pay-to-pay fees were not a debt that the defendant sought to collect); see also *Turner v. PHH Mort. Corp.*, 2020 U.S. Dist. LEXIS 87839 (M.D. Fla. Feb. 24, 2020), *reconsideration denied* 2020 U.S. Dist. LEXIS 87841 (M.D. Fla. Mar. 19, 2020) (convenience fees are not debts under the FDCPA and Florida analogue; they are an optional service the plaintiff voluntarily incurred); *Bardak, et al. v. Ocwen Loan Servicing*, 2020 U.S. Dist. LEXIS 158847 (M.D. Fla. Aug. 12, 2020) (holding that the subject convenience fees were not a debt owed another and were, therefore, not actionable under either the FDCPA or FCCPA).

In *Alexander*, the Fourth Circuit held that the convenience fees at issue qualified as an “amount” under the FDCPA and that the fees need not be “incidental to the principal obligation” to be actionable: “[A]ny amount’ means what it says any amount, whether or not that amount is incidental to the principal obligation.” The court also held that the \$5 convenience fees were not “permitted by law” under the FDCPA. While the district court looked to the mortgage documents to determine whether the fees were expressly prohibited, the Fourth Circuit looked to those same documents to determine whether the fees were expressly *permitted*. Thus, the court — while disclaiming any requirement that the “amount” be incidental to the principal obligation — actually held that convenience fees are incidental to the underlying debt obligation. The court also held that the mortgage contract must specifically authorize the fees.

“[A]ny amount’ means what it says any amount, whether or not that amount is incidental to the principal obligation.”

The *Alexander* opinion is expected to have wide-ranging implications for consumer-facing companies operating in Maryland and in other states with similar consumer protection laws because it espouses a broad reading of both the Maryland statute and the FDCPA. Numerous states have similar consumer protection statutes on the books, opening the door to more class action litigation, as well as regulatory scrutiny. And indeed, in May 2022, Maryland’s Office of the Commissioner of Financial Regulation published a bulletin in response to the decision. See *Notice to Lenders and Servicers: Court Decision on So-Called “Convenience Fees” (Fees for Loan Payments Might Not Be Collectable)*, Md. Comm. Fin. Reg. (May 12, 2022). As the office observed: “[A]ttempts to circumvent this fee restriction by directing consumers to a payment platform associated with the lender or servicer that collects a loan payment fee ... could also violate Maryland

law.” *Id.* On June 29, 2022, the Consumer Financial Protection Bureau (CFPB) went further, issuing an advisory opinion focused on consumer debt collectors and the convenience fees they charge for some payments, such as online or by phone. The CFPB is focusing its charge against convenience fees, relying on the FDCPA. The bulletin essentially adopts the reasoning in *Alexander* that debt collectors may collect convenience fees only if the underlying contract or state law expressly authorizes those fees.

The result in *Alexander*, as well as the increased regulatory scrutiny that has followed, requires mortgage servicers to reconsider their practices of charging fees for the convenience of making payment over the phone or online. The legal and regulatory environment has grown considerably more hostile, leading a number of leading mortgage servicers to stop charging such fees. As the CFPB bulletin also advises: “Debt collectors may violate [the] FDCPA ... when using payment processors who charge consumers pay-to-pay fees.” Although several cases have rejected this proposition, see *Shami v. National Enterprise Systems*, No. 09-722, 2010 U.S. Dist. LEXIS 99838 (E.D.N.Y. Sept. 23, 2010) (the relevant standard under Section 1692f(1) is whether the processing fee was being passed through from a third party), nothing in the language of the FDCPA appears to actually support this result. Given the current trend against convenience fees, servicers should also be aware that the increasing scrutiny may extend to the payment processors servicers often use to facilitate payments.

“[A]ttempts to circumvent this fee restriction by directing consumers to a payment platform associated with the lender or servicer that collects a loan payment fee ... could also violate Maryland law.”

District Court Vacates CFPB Rules Exempting Small-Volume Lenders From Reporting Requirements Under the HMDA

In September 2022, Judge Beryl A. Howell of the U.S. District Court for the District of Columbia issued an order in *National Community Reinvestment Coalition v. Consumer Financial Protection Bureau*, No. 1:20-cv-02074-BAH (D.D.C. Sept. 23, 2022), vacating CFPB regulations that had expanded the number of small-volume lenders deemed exempt from Home Mortgage Disclosure Act (HMDA) reporting requirements.

The HMDA requires covered lenders to collect specified data on mortgages and mortgage applications, and it mandates public disclosure of this information to provide communities and public officials with sufficient information to determine whether depository institutions are fulfilling their obligations to serve the housing needs of the communities and neighborhoods in which they are located. The required disclosures include details about individual loans, such as the purpose, amount, interest rate, and collateral, as well as demographic information about loan applicants (HMDA data). Financial institutions with total assets below a specific annually adjusted amount — currently \$50 million — are exempted from these collection and reporting requirements. For nonexempt institutions, HMDA rules require reporting of HMDA data for loans that institutions originate or purchase during each fiscal year based on two separate reporting thresholds — one for closed-end mortgage loans and the other for open-end lines of credit.

In 2015, the CFPB set the closed-end threshold at 25 closed-end mortgage loans in each of the two preceding calendar years, and the open-end threshold at 100 open-end lines of credit in each of the two preceding calendar years. After multiple adjustments to these numerical thresholds, in 2020, the CFPB acted to address “considerable burdens associated with reporting” this data: (1) by increasing the threshold of exempt institutions to 100 closed-end mortgage loans in each of the two preceding calendar years and (2) by setting the permanent threshold for open-end lines of credit at 200 open-end lines in each of the two preceding calendar years, starting in calendar year 2022 (collectively, the 2020 Rule).

In 2020, a group of five nonprofits — plus the city of Toledo, Ohio — sued the CFPB, challenging the 2020 Rule. The plaintiffs raised two main challenges. First, the plaintiffs argued that the 2020 Rule exceeded the CFPB’s statutory authority under the HMDA, which authorizes the agency to make adjustments and exceptions for any class of transactions, as in the judgment of the CFPB are necessary and proper to effectuate the purposes of the HMDA. The CFPB defended against the claim by arguing that the 2020 Rule was within the scope of its authority under the HMDA, and the CFPB’s interpretation was entitled to deference under *Chevron U.S.A., Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842–43 (1984).

Second, the plaintiffs argued that the cost-benefit analysis underlying the 2020 Rule was flawed because the CFPB exaggerated the benefits of increasing the loan-volume reporting thresholds by failing adequately to account for comments suggesting that the savings would in fact be much smaller than estimated, as well as by relying on overinflated estimates of the cost savings to newly exempted lending institutions with smaller loan volumes. The plaintiffs also argued that the CFPB miscalculated the costs of the 2020 Rule by failing to consider the nonquantifiable harms of raising the reporting thresholds, as well as the disproportionate impacts of those harms. The CFPB countered that its cost-benefit analysis was reasonable and accounted for all the relevant factors in assessing the benefits and costs to covered persons and consumers that would result from increasing the HMDA reporting thresholds.

On September 23, 2022, Judge Howell issued her opinion, invalidating the closed-end loan exemption expansions. The court found that promulgation of the 2020 Rule did not exceed the CFPB’s statutory authority since HMDA grants broad discretion in the judgment of the agency to create exceptions to the statutory reporting requirements, but that the CFPB failed adequately to explain or support its rationales for adoption of the closed-end reporting thresholds under the 2020 Rule, rendering this aspect of the rule arbitrary and capricious. The court vacated and remanded the closed-end mortgage loan reporting threshold to the CFPB, which is expected to issue guidance on how to comply with the HMDA

reporting requirements affected by the ruling in the near future. In the meantime, small-volume lenders originating or acquiring more than 25 loans per year should be aware that HMDA disclosures are required.

Supreme Court of California Finds Lender Does Not Owe a Borrower a Tort Duty in Mortgage Modification

In March 2022, the Supreme Court of California issued a decision, settling the issue of whether a tort duty exists in a mortgage modification that has divided California courts for years.

In *Sheen v. Wells Fargo Bank, N.A.*, plaintiff Kwang K. Sheen asserted that defendant Wells Fargo owed him a duty of care “to process, review, and respond carefully and completely to the loan modification applications plaintiff submitted.” The plaintiff further alleged that defendant Wells Fargo breached this duty, causing him to “forgo alternatives to foreclosure.” Wells Fargo demurred and argued that it owed the plaintiff no such duty. The court of appeal affirmed the lower court’s decision, sustaining the defendant’s demurrer, but noted that this issue has divided California courts for years. Now, the Supreme Court of California has settled the issue and sided with Wells Fargo. The court held that when a borrower requests a loan modification, a lender owes no tort duty sounding in general negligence principles to “process, review, and respond carefully and completely to” the borrower’s application.

The plaintiff grounded his negligence claim in the common law, but the court ultimately found that the economic loss rule barred the plaintiff’s negligence claim. The economic loss rule, in general, provides that there is no recovery in tort for negligently inflicted “purely economic losses” unaccompanied by property damage and personal injury. It functions to bar claims in negligence for purely economic losses when the parties have a contractual relationship. In other words, the plaintiff was barred

from asserting his negligence claim because it was not independent of the original mortgage contract. Instead, it was based on an asserted duty that was contrary to the rights and obligations clearly expressed in the loan contract. The court looked to other jurisdictions, such as Montana and Connecticut, to support its decision. Further, the court found that mortgage lending and modification did not share the special characteristics associated with certain contexts exempted from the reach of the economic loss rule.

The court found that a lender’s involvement in the loan modification process is part of its assessment regarding how best to recoup the money it is owed. Thus, such involvement, without more, does not exceed the scope of an institution’s conventional role as a mere lender of money. Additionally, the court found that there does not need to be a viable breach of contract claim for the economic loss rule to apply. The court reasoned that the factors identified in *Biakanja v. Irving* to be used in determining the existence of a duty of care were not applicable when the parties are in contractual privity, and the plaintiff’s claim is not independent of the contract. *Biakanja* involved a will that was not properly attested. The plaintiff there sued the defendant notary for the interest she would have received had the will been valid. Unlike the facts in *Biakanja*, the parties in this matter had a contractual relationship. Accordingly, the court applied the “general rule” stated in *Nymark v. Heart Fed. Savings & Loan Assn.*, which holds that financial institutions owe no duty of care to a borrower when the institution’s involvement is merely as a lender of money.

Courts have already begun to apply *Sheen*, holding that lenders do not have any duty to a borrower to process, review, and respond carefully and completely to the borrower’s loan modification application. The decision creates a clear rule in California regarding whether a lender owes a tort duty of care in the mortgage modification process.

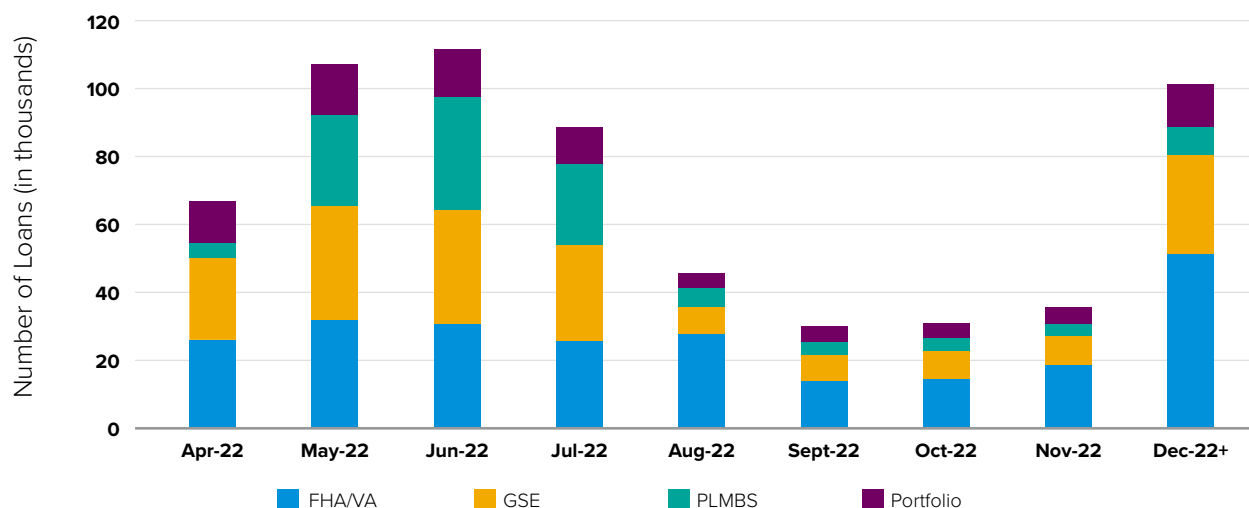
Loss Mitigation Concerns: The Aftermath of COVID-19 on Mortgage Servicers

In the wake of the COVID-19 pandemic, mortgage servicers face continued difficulty with enforcement and compliance. The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) foreclosure moratorium and subsequent CFPB protections significantly limited foreclosure activities from March 2020 through January 1, 2022. From January through March 2022, foreclosures began to increase and approach pre-pandemic numbers. Now that moratoriums have long ended, coupled

with an increase in the cost of living and a potential recession on the horizon, mortgage servicers should expect a larger swell of foreclosures.¹

In anticipation of increased foreclosures, mortgage servicers should begin preparing loss mitigation programs to help borrowers avoid losing their homes. Loss mitigation is the process of borrowers and mortgage servicers working together to create a plan to avoid foreclosure. Potential plans include forbearance, repayment plans, loan modification, short sale, and deed-in-lieu of foreclosure.

Figure 1: Projected Forbearance Exits as of April 7, 2022



Sources: Black Knight Data & Analytics, LLC; RADAR

A report released by the Federal Reserve Bank of Philadelphia confirmed around 2.15 million mortgages were in forbearance or past due as of April 7, 2022.²

This data, and other data similarly collected, show the number of borrowers potentially facing foreclosure who will require loss mitigation

programs. With this number of borrowers at issue, mortgage servicers should expect the following:

- Increased government scrutiny;
- Increased number of contested foreclosures and lawsuits; and
- Requirement to allocate more resources to loss mitigation.

¹ See [“Six top concerns for mortgage bankers,”](#) ABA Banking Journal, May 4, 2022.

² See [“Nearly Half of All Delinquent Mortgages on Loss Mit Plans,”](#) DSNews, April 27, 2022.

Government scrutiny is likely to increase as some government officials have begun distributing letters to mortgage servicers, reminding them of their obligation to assist borrowers facing foreclosure to ensure there is sufficient time to implement loss mitigation programs.³

As foreclosure filings are predicted to increase, so too are the number of homeowners contesting foreclosure actions. Most of these contested foreclosure actions will be brought under Title 12 of the Code of Federal Regulations, Section 1024.41—the loss mitigation provisions of the Real Estate Settlement Procedures Act.⁴ With proper documentation regarding loss mitigation activities and foreclosure for each borrower, mortgage servicers can protect themselves from potential liability.

The best way for mortgage servicers to start preparing now for the predicted increase in loss mitigation activity include the following:

- Begin documenting prior and current loss mitigation practices;
- Improve borrower communication and documentation;
- Provide borrower education opportunities for loss mitigation options; and
- Increase training for staff.

A Look Ahead

This year saw a 40-year high in inflation and an accompanying rise in mortgage rates, with the global economy headed to remain fragile in 2023. It is expected that housing affordability and the fallout from rising rates will be prominent issues in the mortgage industry. According to Mike Fratantoni, senior vice president and chief economist at the Mortgage Bankers Association (MBA), the MBA forecasts a recession in the first half of 2023, and it expects the unemployment rate to rise to nearly 5.5% by the end of next year.

While rising interest rates and unemployment may have obvious consequences on the average loan seeker, rising rates are predicted to affect foreclosures as well, creating challenges for the industry, which now must determine methods to prevent losses to both borrowers and lenders. In the recent past, low interest rates have enabled lenders to prevent foreclosures through loan modifications – with mortgage-backed security (MBS) issuers buying loans out of pools and modifying them to lower monthly payments and capitalize delinquent mortgage payments. As pool issuers buy loans from an MBS pool, they typically finance the purchase of the mortgages with their corporate assets. If an issuer buys a loan out of an MBS to modify its loan, the interest rate offered to the borrower generally increases by the same amount the issuer's funding costs increased. Rapidly rising rates present a unique challenge for certain issuers as a lower mortgage rate than debt rate may prevent the issuer from being able to afford the loan and, thus, will not have an effective means of loss mitigation to offer the borrower. As mortgage servicers begin to contend with an influx of foreclosures, anticipated increases in loss mitigation practices are sure to follow. As foreclosures increase, government scrutiny and contested foreclosure lawsuits are likely to rise. Mortgage servicers should consider promptly improving loss mitigation practices to avoid liability in the future.

From a regulatory perspective, mortgage servicers will see a new rule going into effect, requiring them to maintain certain fair lending data elements, including the borrower's age, race, ethnicity, gender, and preferred language. The rule, announced by the Federal Housing Finance Agency (FHFA), will go into effect on March 1, 2023, and will require servicers to store this information in a searchable format that must transfer with servicing throughout the loan. In response to the FHFA's announcement, Freddie Mac issued Bulletin 2022-17 and Fannie Mae issued Servicing Guide Announcement SVC-2022-06, which specifies that the data elements, if obtained during the origination process,

³ See ["Attorney General James Again Warns Mortgage Servicers of Obligation to Assist Homeowners in Need of COVID-19 Relief,"](#) New York State Attorney General (ny.gov), December 13, 2021.

⁴ See ["The State of Post-Pandemic Loss Mitigation Facing Servicers,"](#) Selene (seleneadvantage.com), July 27, 2022.



must be recorded and transferred for all loans originated on or after March 1, 2023. Fannie Mae and Freddie Mac also note that servicers may, but are not required to, update these data elements in a subsequent transfer of ownership or assumption of the loan. Servicers are not required to implement these changes until March 1, 2023. However, many have already begun doing so, and servicers are encouraged to implement these policies immediately to avoid potential enforcement actions.

2023 will also see the end of the LIBOR index for adjustable-rate mortgages, which is expected to create conflicts of interest among lenders, borrowers, investors, and others. In an effort to develop a transition plan that minimizes these conflicts, the Alternative Reference Rates Committee has proposed transitioning to the Secured Overnight Financing Rate (SOFR) and rely on a five-year median difference between LIBOR and SOFR to create an adjusted benchmark.

AARC's proposal is a departure from mortgage lender's usual practice of setting loan prices based on the contemporaneous values of benchmark indices and not their values over a historical time period. The challenges of developing a new plan will likely continue until mid-2023.

While a recession appears unavoidable, a potential upside is that it likely will bring rates down. Indeed, the MBA expects rates to fall to 5.4% by the end of 2023. However, the mortgage industry cannot rely on falling rates to alleviate concerns with borrowers losing their homes. As the market has seen in recent years, historically low interest rates can increase rapidly and significantly. The mortgage industry must develop innovative tools that will allow borrowers to be successful homeowners through what is predicted to be tough economic times in 2023.

PAYMENT PROCESSING AND CARDS

Authors: Keith Barnett, Taylor R. Gess, Carlin A. McCrory, Samer A. Roshdy

Payment Processing

Money Transmission. In September 2021, the Conference of State Bank Supervisors (CSBS) released the Model Money Transmission Modernization Act (the Act) to set a single nationwide standard for state money transmission requirements.

This set the stage for state adoption of the Act in 2022. West Virginia enacted pieces of the Act in March 2022. In May 2022, Arizona adopted the Act. Arizona previously did not have an explicit agent of the payee exemption in its statutes. By adopting the Act, Arizona now formally recognizes agent of the payee. West Virginia had already adopted the agent of the payee exemption.

West Virginia adopted the portion of the Act that expressly includes payroll processing in money transmission, but Arizona did not.

Case Law Against a Payment Processor

On June 29, 2022, the Consumer Financial Protection Bureau (CFPB) issued an advisory opinion on pay-to-pay fees, also known as convenience fees. While the opinion largely addresses fees charged by debt collectors, there is a section that addresses pay-to-pay fees charged by processors. The opinion gives an example that debt collectors may violate Section 808(1) of the Federal Debt Collection Practices Act (FDCPA) and Regulation F, 12 CFR 1006.22(b) when a third-party payment processor charges a pay-to-pay fee and remits any portion of the fee to a debt collector.

On July 29, 2022, the Federal Trade Commission (FTC) filed a complaint and executed a stipulated order with payment processor First American Payment Systems, LP (First American) and companies that market its services – Eliot

Management Group LLC (Eliot) and Think Point Financial LLC (Think Point) (collectively, the defendants). The FTC alleged that the defendants violated Section 5 of the Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45, and Section 4 of the Restore Online Shoppers' Confidence Act (ROSCA), 15 U.S.C. § 8403, arising out of the marketing of First American's payment processing services to merchants, and the alleged failure to provide clear and conspicuous contractual terms in the online application and agreement between First American and the merchants.

Section 5 of the FTC Act prohibits unfair and deceptive acts and practices by businesses against consumers. ROSCA is also a consumer protection statute that, among other things, prohibits businesses from charging consumers for goods or services sold in transactions effected on the internet through a negative option feature unless the business: (1) clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information; (2) obtains the consumer's express informed consent before making the charge; and (3) provides simple mechanisms that allow consumers to stop recurring charges.

Although First American provides its payment processing services to small businesses, the complaint refers to the small businesses as "consumers" even though they are not consumers (some of the merchants, however, are sole proprietors). While it is not unprecedented for the FTC to sue a business for alleged violations of the FTC Act made against other businesses, this lawsuit represents the first time that the FTC has sued a payment processor for alleged violations of the FTC Act arising out of alleged false statements concerning payment processing services that are marketed and provided to other businesses.

Similarly, ROSCA only applies to business-to-consumer transactions. Although automatic renewal clauses stating that the agreement will automatically renew unless terminated a certain number of days before the end of the current term are common in the payment processing industry, the FTC alleged that the automatic renewal (also known as a negative option) in First American's agreements violated ROSCA. The FTC alleged that First American violated ROSCA by failing to disclose all material terms of the transaction clearly and conspicuously, failing to obtain the merchants' express informed consent before charging them (after termination), and failing to provide simple mechanisms for the merchants to cancel the contract. The ROSCA violations also included: (1) allegations that the processor's sales agents did not discuss the automatic renewal with the merchants before the parties executed the agreements; and (2) allegations that the merchants could not review all of the terms and conditions of the agreement without clicking on several hyperlinks embedded throughout the online merchant agreement.

The FTC has sent a signal that it will label small businesses as "consumers," and payment processors must be cautious in their business practices.

Instant Payments

In 2022, we saw rapid adoption of the use of instant payment services within the United States, with many participating through the real-time payments network, known as RTP, administered by The Clearing House (TCH), which is a network owned by some of the world's largest financial institutions. Instant payment services provide businesses and consumers with the ability to send and receive payments in real time in an efficient and secure manner, with payment recipients having full access to funds immediately, ultimately giving users of instant payments greater flexibility to manage their finances and provide time-sensitive payments. The Federal Reserve announced this year that it is expecting to launch its own instant payments network, the FedNow Service, in May to July 2023, and the Federal Reserve pushed out a new rule in May 2022 to govern funds

transfers through the anticipated FedNow Service. The launch of the FedNow Service will serve to provide increased access to financial institutions of any size, helping broaden the reach of instant payments to communities throughout the nation. Looking ahead, we expect that the growing use of innovative instant payments services will correspond with increased regulatory rulemaking in this area—particularly in how consumer protections provided in Regulation E are examined. Indeed, in conjunction with its announcement of the May 2022 rule, the Federal Reserve noted that it "believes strengthening consumer protections related to instant payments broadly is a desirable goal and supports commenters' suggestions for examining Regulation E as a potential tool."

Payment Cards

On May 2, 2022, the Consumer Financial Protection Bureau (CFPB) released its *Supervisory Highlights* report on legal violations discovered during examinations. The report details issues identified by CFPB examination teams across a wide number of segments of the consumer financial services industry, including credit card account management and prepaid accounts.

Credit Card Account Management

- The CFPB found violations related to Fair Credit Billing Act (FCBA) disputes. These errors related to nearly every aspect of dispute handling:
 - Failing to mail or deliver written acknowledgments to consumers within 30 days of receiving a billing error notice.
 - Failing to resolve disputes within two complete billing cycles after receiving a billing error notice.
 - Failing to reimburse consumers after billing errors were determined to have occurred as consumers asserted.
 - Failing to mail or deliver correction notices to consumers resolving billing errors in their favor.
 - Failing to conduct reasonable investigations

after receiving billing error notices due to human errors and system weaknesses.

- Providing inaccurate explanations to consumers as to why the creditor denied the consumers' billing error claims in whole or part or failing to provide explanations at all.
- Failing to provide consumers with the evidence the creditor relied upon to determine no billing error occurred. The CFPB required issuers to make system improvements, perform enhanced monitoring, create additional controls for consumer complaints, and revise applicable policies and procedures.

The CFPB reports that the supervised entities are enhancing training materials, making system improvements, enhancing monitoring, designing new controls for consumer complaint management, and revising applicable policies and procedures to address the discovered violations.

- The CFPB found supervised entities failed to reevaluate annual percentage rates (APRs) on credit cards under the CARD Act after increasing a consumer's APR. Specifically, these violations were found when a creditor acquired preexisting credit card accounts from other creditors.
 - One set of violations related to the failure to reduce APRs because the data required to conduct the reevaluation analysis was not gathered during the acquisition.
 - In a second set of violations, creditors failed to conduct reevaluations of rate increases once every six months after certain APR increases on acquired accounts because the creditors did not accurately record a data review in their system so those accounts were not included in the reevaluation process.
 - Finally, the CFPB found violations when creditors considered certain minimum rates that previously applied to their credit card accounts but no longer applied at the time of reevaluation such that the factors considered in the reevaluation were not appropriate.

The CFPB required remediation for the consumer harm caused by being charged a higher rate than should have been imposed, development of new rate reevaluation controls, removal of any inappropriate factors when determining the reevaluated APR and improved monitoring to ensure consumers are being charged the proper APR.

- The CFPB also concluded that supervised entities engaged in deceptive acts or practices by: (1) advertising the interest-free feature of their credit card without disclosing the preconditions for obtaining the financing; and (2) failing to process refunds in accordance with their cardholder agreements.

Prepaid Accounts

The CFPB found that institutions failed to honor valid stop payment requests when payments originated through bill pay systems at a merchant and the prepaid account manager's system. The CFPB also found that creditors were not properly and timely submitting their agreements and other required information to the CFPB as required by Regulation E. Finally, the error resolution documentation notice used by a creditor did not note the consumer's right to request the documentation the institution relied on in making its error determination after determining that no error or a different error occurred and failed to provide consumers with requested documentation.

On August 12, 2022, the Consumer Financial Protection Bureau (CFPB) posted a blog reporting on various factors impacting interest rates. The factors discussed are: (1) a record low charge-off rate; (2) persistence of higher rates despite a relatively unchanged percentage of subprime borrowers; and (3) low prime rates. The blog concludes by claiming the profits in the credit card industry are "outsized," and asserting that the credit card market is dominated by a handful of players that make the industry "anti-competitive." This signals heightened CFPB scrutiny of the credit card industry.

Credit Cards

We saw renewed scrutiny in 2022 over the Durbin Amendment, which is a provision in the Dodd-Frank Act of 2010 best known for its cap on debit card interchange fees (the transaction fees that are charged for the use of a card) as well as: (1) requiring debit card issuers to provide at least two unaffiliated payment card networks to process electronic debit transactions, thereby preventing network exclusivity; and (2) prohibiting card issuers from inhibiting merchants from directing the routing of an electronic debit transaction over any network that may process that transaction. Together, the prohibition on exclusivity and routing inhibition means merchants processing electronic debit card transactions can choose from at least two unaffiliated payment card networks when processing debit card transactions. Building off of the debit card competition reforms found in the Durbin Amendment, U.S. Senate Majority Whip Dick Durbin (D-IL) and U.S. Senator Roger Marshall, M.D. (R-KS) introduced in July 2022 the bipartisan Credit Card Competition Act of 2022 (CCCA), which would extend some of the Durbin Amendment protections to credit card transactions. The CCCA would, like the restrictions imposed on certain debit card issuers in 2010, direct the Federal Reserve to ensure that, with certain exceptions, large credit card issuing banks offer a choice of at least two networks over which an electronic credit transaction may be processed, at least one of which must be outside of the top two largest networks (currently, Visa and Mastercard). According to Senator Durbin, the proposed legislation would bring “real competition to credit card networks” and “help reduce swipe fees and hold down costs for Main Street merchants and their customers.” The CCCA is currently sitting with the U.S. Senate Committee on Banking, Housing, and Urban Affairs, and we expect senators to continue pushing for its enactment in 2023 as well as other rulemaking efforts to address rising interchange fees for credit card transactions.

In March, the CFPB released a report detailing its concern over the revenue produced by late fees for credit card issuers that primarily serve customers with low credit scores and in low-income neighborhoods, along with fee increases due to inflation adjustments. In July, the CFPB solicited

comments on an Advance Notice of Proposed Rulemaking regarding credit card late fees. The current rules in the Credit Card Accountability Responsibility and Disclosure Act of 2009 (CARD Act) and Regulation Z limit late fees to an amount that “represents a reasonable proportion of the total costs incurred by the card issuer as a result of that type of violation.” In the alternative, an issuer may charge the safe harbor fee amounts found in Reg. Z that have been deemed reasonable and proportional. With adjustments allowed for inflation, the current safe harbor amounts are \$30 for a first late payment and \$41 for subsequent late payments within the next six billing cycles. In the Advance Notice of Proposed Rulemaking, the CFPB asked for comments on the following: (1) factors used by card issuers to set late fee amounts; (2) card issuers’ costs and losses associated with late payments; (3) the deterrent effects of late fees; (4) cardholders’ late payment behavior; (5) methods that card issuers use to facilitate or encourage timely payments, including autopay and notifications; (6) card issuers’ use of the late fee safe harbor provisions in Regulation Z; and (7) card issuers’ revenue and expenses related to their domestic consumer credit card operations. We anticipate that the CFPB may take further action on the topic of credit card late fees in the coming year.

Debit Cards

The movement to place restrictions on credit card transactions was not the only piece of the Durbin Amendment that was revisited this year. On October 3, 2022, the Federal Reserve Board finalized amendments to Regulation II, the implementing regulation for the Durbin Amendment, to specifically require debit card issuers to provide at least two unaffiliated payment card networks to process card-not-present debit card transactions (such as online purchases). When the original rule was initially issued in July 2011, a solution supporting multiple networks for card-not-present debit card transactions was not fully settled by the market. Since that time, however, technological advancements have been made to address these issues, and now these amendments to Regulation II serve to formalize the requirement for card-not-present debit card transactions. The amendments are set to be effective July 1, 2023.

SMALL DOLLAR LENDING

Authors: Jason M. Cover, Mark J. Furletti, Jill K. Dolan, Taylor R. Gess

2022 CFS Year in Review and Look Ahead: Small Dollar Lending

Small dollar lending encompasses the short-term, small-dollar credit market, sometimes referred to as “payday lending.” These loans are typically marketed as a way to bridge a cash-flow shortage between paychecks or benefits payments. Borrowers must typically repay loan proceeds quickly, and they usually require that a borrower give the lender access to repayment through a debit to the borrower’s deposit account.

Fifth Circuit Finds CFPB Funding Structure Unconstitutional

On October 19, 2022, a Fifth Circuit Court of Appeals three-judge panel found the funding mechanism for the Consumer Financial Protection Bureau (CFPB or Bureau) to be unconstitutional. Specifically, the court in *Community Financial Services Association of America, Ltd. v. Consumer Financial Protection Bureau* held the CFPB’s funding violates the Constitution because the Bureau does not receive its funding from annual congressional appropriations like most executive agencies, but instead receives funding directly from the Federal Reserve based on a request by the Bureau director. The court rooted its decision in the foundational precepts of the Federalist Papers and the Federal Convention of 1787, at one point quoting George Mason in support of its decision: “The purse & the sword ought never to get into the same hands.”

Background

Plaintiffs Community Financial Services Association of America and Consumer Service Alliance of Texas challenged the validity of the CFPB’s 2017 Payday Lending Rule, specifically the payment provisions, which prohibit lenders from initiating additional payment transfers from consumers’ accounts after two consecutive attempts have

failed for insufficient funds, unless the consumer authorizes additional payment transfers. The district court granted summary judgment in favor of the Bureau. The plaintiffs appealed on multiple grounds, including: (1) the rule’s promulgation violated the Administrative Procedure Act; (2) the rule was promulgated by a director unconstitutionally insulated from presidential removal; (3) the Bureau’s rulemaking violates the nondelegation doctrine; and (4) the Bureau’s funding mechanism violates the Constitution’s appropriations clause. The Fifth Circuit affirmed the district court’s entry of summary judgment in favor of the Bureau on each of the first three issues. But importantly, the court found “Congress’s cession of its power of the purse to the Bureau violates the Appropriations Clause and the Constitution’s underlying structural separation of powers” and reversed on that issue, invalidating the Payday Lending Rule.

The Decision

The court focused on what it characterized as the Bureau’s double insulation from Congress’s appropriation power. Not only does the Bureau receive its funding via request by the director to the Federal Reserve, but also the Federal Reserve itself falls outside the appropriations process by receiving its funding by way of bank assessments. Moreover, funds derived from the Federal Reserve System are not subject to review by the House or Senate Committee on Appropriations. As the court found: “[T]he Bureau’s funding is double-insulated on the front end from Congress’s appropriations power. And Congress relinquished its jurisdiction to review agency funding on the back end.” The court held this relinquishment to be even more problematic, given the agency’s expansive authority. “An expansive executive agency insulated (no, double-insulated) from Congress’s purse strings, expressly exempt from budgetary review, and headed by a single Director removable at the President’s pleasure is the epitome of the unification

of the purse and the sword in the executive ...”. Ultimately, the court held that while Congress properly authorized the Bureau to promulgate the rule, the CFPB lacked the wherewithal to exercise that power via constitutionally appropriated funds. The plaintiffs were thus harmed by the Bureau’s improper use of unappropriated funds to engage in the rulemaking at issue and were entitled to a “rewinding” of the Bureau’s action.

“[T]he Bureau’s funding is double-insulated on the front end from Congress’s appropriations power. And Congress relinquished its jurisdiction to review agency funding on the back end.”

Going Forward

As of the time of the drafting of this summary, the case is expected to be appealed to a full Fifth Circuit hearing, and after that, it has a good chance of heading to the Supreme Court.

While it stands, this holding renders all CFPB actions from inception of the Bureau, as well as its current activities, susceptible to challenge. Like the 2017 Payday Lending Rule, none of the CFPB’s actions, from rulemaking to enforcement, could have occurred absent the unconstitutional funding. Beyond the Payday Lending Rule, the CFPB has issued rules under the Fair Debt Collection Practices Act (Regulation F) and the Fair Credit Reporting Act (Regulation V). The CFPB has also adopted mortgage-related amendments and other changes to Regulation Z under the Truth in Lending Act, and rules governing prepaid accounts in Regulation E under the Electronic Fund Transfer Act, among others.

The same appropriations argument is being made in a number of other litigation matters involving the CFPB, including several enforcement cases pending in courts in the Fifth Circuit and elsewhere, as well as in the U.S. Chamber of Commerce case challenging the CFPB’s authority to prohibit discrimination under its UDAAP authority, which is also pending in a Fifth Circuit district court.

In late October 2022, defendants in two separate CFPB enforcement actions cited the Fifth Circuit’s decision as a basis for having their actions dismissed. In response, the CFPB has characterized the decision as “neither controlling nor correct” and “mistaken.” In a response filed in an Illinois action, the CFPB argued that the decision is not supported by law, the court erred in finding that the CFPB’s funding through the Federal Reserve System makes it insulated from congressional oversight, and the decision’s holding finds no support in the Dodd-Frank provision that states funds transferred to the CFPB “shall not be construed to be Government funds or appropriated monies.” The CFPB also noted that although the Fifth Circuit described the CFPB’s funding as “novel” and “unprecedented,” it is not meaningfully different from numerous other agencies funded in ways other than annual spending bills. The CFPB requested that the court reject the Fifth Circuit analysis and “instead join every other court to address the issue – including the *en banc* D.C. Circuit – in upholding the Bureau’s statutory funding mechanism.” Separately, in a letter to the Ninth Circuit, the CFPB focused on the remedy in stating that “[t]he court didn’t consider whether ‘the [CFPB] would have acted differently’ ‘but for’ its statutory funding mechanism. Here, applying *Collins* yields a straightforward answer: the case should not be dismissed because there is no evidence the [CFPB] ‘would have acted differently’ with different funding.”

In November 2022, the CFPB filed a petition for a writ of certiorari to the U.S. Supreme Court, requesting not only that the Court hear the case, but also that it be decided on an expedited basis during the Court’s current term.

“[T]he court didn’t consider whether ‘the [CFPB] would have acted differently’ ‘but for’ its statutory funding mechanism. Here, applying Collins yields a straightforward answer: the case should not be dismissed because there is no evidence the [CFPB] ‘would have acted differently’ with different funding”.

New Mexico Enacts 36% APR Cap on Loans of \$10,000 or Less

On March 1, 2022, New Mexico Governor Michelle Lujan Grisham signed House Bill 132, creating a 36% APR cap on loans up to \$10,000 made under the New Mexico Bank Installment Loan Act of 1959 (BILA) and the New Mexico Small Loan Act (SLA). The bill also expands the SLA anti-evasion provision. These changes take effect on January 1, 2023.

In calculating the 36% APR cap, the following must be included:

- Finance charges under Regulation Z;
- Charges for any ancillary product or service sold or any fee charged in connection or concurrent with the extension of credit;
- Charges for credit insurance premium fees; and
- Charges for single premium credit insurance and any other insurance-related fees.

These charges must be included even if they would be excluded under the Regulation Z finance charge calculation. Fees paid to a public official relating to the extension of credit, including fees to record liens, are excluded.

The SLA anti-evasion provision was expanded to target nonbank participants of bank model programs. The anti-evasion provision applies the SLA to “a person who seeks to evade its application by any device, subterfuge or pretense whatsoever” to include:

- Making, offering, assisting, or arranging a debtor to obtain a loan with an APR exceeding 36% through any method, including mail, telephone, internet, or any electronic means, regardless of whether the person has a physical location in the state; and
- A person purporting to act as an agent, service provider, or in another capacity for another entity that is exempt from the SLA, if, among other things, the APR on the loan exceeds 36%, and:
 - The person holds, acquires, or maintains, directly or indirectly, the predominant economic interest in the loan;
 - The person markets, brokers, arranges, or facilitates the loan and holds the right, requirement, or first right of refusal to purchase loans, receivables, or interests in the loans; or
 - The totality of the circumstances indicates that the person is the lender, and the transaction is structured to evade the requirements of the SLA considering all relevant factors, including where the person: (1) indemnifies, insures, or protects an exempt entity for any costs or risks related to the loan; (2) predominantly designs, controls, or operates the loan program; or (3) purports to act as an agent, service provider, or in another capacity for an exempt entity, while acting directly as a lender in other states.

A similar 36% APR cap proposal failed to make the November 2022 ballot as an initiative in Michigan.



CFPB Report Finds Payday Borrowers Continue to Pay Significant Rollover Fees, Despite State-Level Protections and Payment Plans

On April 6, 2022, the CFPB published a report, finding that few payday loan borrowers are taking advantage of no-cost extended payment plans, which are required to be offered to borrowers in the majority of states that do not prohibit payday lending. Instead of utilizing these plans, borrowers apparently have continued to pay for expensive loan rollovers.

Noting that no-cost extended payment plans are meant to help borrowers exit the cycle of rollovers and fees, the CFPB contends that payday lenders could be steering borrowers to rollovers to ensure borrowers are charged additional fees, thus ensuring incoming revenue. Extended payment plans, by contrast, are no-cost plans that typically allow a borrower to repay only the principal and fees already incurred, while dividing the balance over a number of months.

There are 26 states where payday lending is not prohibited, and 16 of those states require payday lenders to offer no-cost extended payment plans. The CFPB's report found substantial differences among the terms of no-cost extended payment plans in those 16 states. While terms of the extended payment plans vary between states, usage rates for extended payment plans remain low in all states. Additionally, for states that tracked such information, loan rollover and default rates substantially exceeded extended payment plan usage rates.

The CFPB noted in the report that consumers may not take advantage of extended payment plans because they may be unaware of the existence of the plans or unaware of the benefits of the plans. The Bureau plans to continue to monitor lender practices that discourage consumers from taking extended payment plans, taking action as necessary.

STUDENT LENDING

Authors: Dave Gettings, Courtney T. Hitchcock

Although the pandemic has upended many areas of law, few areas have received as much attention as student lending. This makes sense, as student loans are often extremely large, can be difficult to pay, and impact a large portion of the population. On the federal level, student loans have been politically charged, with politicians campaigning on the issue of student loans and federal courts weighing in on the Biden Administration's ability to forgive those loans. The CFPB has also chimed in, becoming increasingly active in the student lending space. On the state level, many states are jumping into the fray, passing legislation and leading enforcement actions related to student loan servicers. Although 2022 was extremely active in the student lending space, 2023 might be even more active if the economy takes a downturn, as many expect.

Student Lending at the Federal Level

As in 2021, the year 2022 saw many developments in the area of federal student loan repayment programs, showing the continuing effects of the pandemic as well as the increasing policy changes surrounding federal student loans.

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which was signed into law on March 27, 2020, provided relief to borrowers of federally held student loans at the start of the COVID-19 pandemic. While the CARES Act's pause on student lending payments was initially set to expire on September 30, 2020, the Department of Education (DOE) has continued to extend the pause on the repayment of student loans. On August 24, 2022, the DOE announced what it labeled as the "final" extension of the pause on student loan repayment, interest, and collections, to end on December 31, 2022. The DOE indicated that borrowers should be expected to resume payments in January 2023. However, following the ongoing litigation surrounding the Biden Administration's Student Debt Relief Plan, the DOE again extended loan repayment through no later

than June 30, 2023, or 60 days after the lawsuits which seek to block relief are resolved.

The DOE's most recent pauses on student loan repayments were meant to accommodate the administration's Student Debt Relief Plan. The plan provides up to \$20,000 in debt relief to Pell Grant recipients with loans held by the DOE and up to \$10,000 in debt relief to non-Pell Grant recipients. Borrowers are eligible for this relief if their individual income is less than \$125,000 or \$250,000 for households in either the 2020 or 2021 tax year. The application period for the debt cancellation will run through December 21, 2023. Loans disbursed to borrowers on or after July 1, 2022, are not eligible for cancellation. As a result of the ongoing litigation, the DOE has halted applications for debt relief. However, for those who applied before the halt, the DOE has begun sending notices of approval to eligible borrowers should the program go forward.

Still, the future of the debt relief plan is uncertain, as the plan remains paused as a result of litigation in the federal courts. While the administration has obtained some victories in federal courts against various states, individuals, and organizations, the plan is still facing legal delays.

On November 10, 2022, U.S. District Judge Mark Pittman of the Northern District of Texas vacated the plan as unconstitutional, and the Fifth Circuit has declined to overturn this decision. Meanwhile, the plan was already temporarily halted by the Eighth Circuit following appeal by the attorneys general for the states of Nebraska, Missouri, Arkansas, Iowa, Kansas, and South Carolina. On November 14, 2022, a three-judge panel for the Eighth Circuit issued a permanent injunction on the discharge of student loan debt under the plan, solidifying its prior decision. That injunction will remain in effect until either the full Eighth Circuit or the Supreme Court rule on the matter. Following an appeal from the Biden Administration, the Supreme Court has agreed to hear the matter for oral argument in February 2023.

While the Supreme Court has not made a final determination as to the standing of the states to bring the lawsuit, the DOE is currently prohibited from providing debt relief to borrowers qualifying under the plan. Given the end of the pause on student loans, and as the litigation surrounding the relief plan continues to play out, we expect that there will be a sharp increase in litigation related to student loans, as borrowers are forced to make payments and possibly attempt to obtain relief under the plan.

CFPB Focus on Student Lending

The CFPB has also remained active in the student lending space in 2022. Throughout the year, the CFPB's actions demonstrated a clear concern as to the impact of student debt on American financial stability and the Bureau's continued focus on collection practices associated with private student loan debt.

At the start of the year, the [CFPB announced](#) it would begin examining the operations of entities that originate institutional student loans, or private education loans extended directly to students by the school. While higher education institutions, such as for-profit colleges, have not historically been subject to the same oversight as traditional lenders, the CFPB's concerns stem from past issues like the lending practices the CFPB investigated at Corinthian College and ITT Tech. In its examination of schools offering institutional loans, the CFPB intends to expand its review of the general lending practices to include a focus on actions that only schools can take against students. Practices that are now under review include: restricting enrollment; withholding transcripts; improperly accelerating payments upon withdrawal; failing to issue refunds upon withdrawal; and maintaining improper lending relationships.

In September, the CFPB released a special edition of its [Supervisory Highlights](#) focused on student loan servicing, and particularly, on institutional loans. The report's findings echo the CFPB's continued concern regarding institutional loans and the power schools exercise over a student's educational and financial future. Concurrently with

its *Supervisory Highlights*, the CFPB also updated its Education Loan Examination Procedures, in part to instruct examiners that absent three exceptions, the CFPB may exercise its supervisory authority over institutions that extend credit expressly for postsecondary education expenses. The CFPB's activity solidifies the messaging that it will continue to devote its attention to examining schools that maintain their own credit programs and the collection practices associated with those programs.

The CFPB's attention to the relationship between consumers and higher education institutions extends beyond the higher education loan sphere, as the CFPB has been similarly critical of the practices surrounding student credit card lending. In the CFPB's [12th Annual Report to Congress](#) on college credit card agreements, the CFPB reviewed more than 650,000 student accounts in partnership with 462 higher education institutions. A key highlight was that marketing efforts directed at students consistently promoted accounts that imposed more costs than comparable accounts, even comparable accounts offered by the same financial services provider. The CFPB review also found hundreds of schools had not posted the required disclosures regarding agreements between the school and financial services providers on their websites. In light of the report, the DOE also released a Dear Colleague Letter, which reminded institutions of their obligations in overseeing arrangements with financial institutions.

The year also saw the CFPB pursue enforcement efforts against student loan servicers in a push that has continued its work from the prior year. In March, the CFPB [entered into a consent order](#) with student loan servicer Edfinancial Services to resolve the Bureau allegations that Edfinancial violated UDAAP by making misrepresentations to borrowers with Federal Family Education Loan Program (FFELP) loans. According to the Bureau findings, the alleged misrepresentations concerned the availability of Public Service Loan Forgiveness (PSLF) to FFELP borrowers and the borrowers' eligibility for PSLF, whether certain jobs were eligible for PSLF, and whether payments made on loans would count toward PSLF. In the Consent Order, Edfinancial agreed to pay a \$1 million civil penalty. In addition,

the order requires Edfinancial to develop training and monitoring for its representatives in future communications with FFELP borrowers regarding PSLF; communicate with borrowers about the PSLF limited waiver; and update its website to provide information about PSLF eligibility.

In conjunction with the CFPB announcement, the DOE released a letter describing the settlement to FFELP servicers. In it, the department states that the issues were not unique to Edfinancial and warns that the CFPB can be expected to pursue further oversight related to these issues. The letter also reminds servicers that they are required to provide FSA's guidance to borrowers, with this requirement including "actively informing borrowers about available programs for debt relief, any changes to these programs, and providing complete information in response to inquiries and complaints."

This continued focus on student debt is further exemplified in the CFPB published report titled, [Student Loan Borrowers Potentially At-Risk when Payment Suspension Ends in April](#). The report

identifies five risk factors that indicate a borrower may struggle to make scheduled loan payments when they ultimately resume. The Bureau reports that around 15 million borrowers have at least one risk factor and over 5 million have at least two. This report is yet another indication that the CFPB is pursuing a more aggressive conversation with consumers and financial institutions about student debt. In fact, April also saw the CFPB publish blog posts on: things to keep in mind now that the Biden Administration has extended the federal student loan pause; and bankruptcy myths, private student loans, and the fact that student loans are dischargeable. In its [bankruptcy blog post](#), the CFPB went so far as to argue that certain private student loans can be discharged upon a showing of undue hardship. The CFPB has clearly focused on the practices of higher education lenders, with the Bureau looking to correct what it views as improper practices in student lending.



The Bureau's activity demonstrates its concern with the economic hardship that the resumption of student loan payments may place on consumers and the threat that subsequent defaults would pose to financial stability. It also indicates that the bureau is following the administration's willingness to take action where it concerns student debt.

State-Level Regulation of Student Lending and Servicing

On the state level, it was a relatively slow year, but some states pushed forward with efforts to regulate student loan servicers and lenders.

For example, the California Department of Financial Protection and Innovation proposed regulations to implement the Student Loan Servicing Act and the Student Loans: Borrower's Rights law. The proposed regulations attempt to define many of the terms utilized in the act, and provide further guidance regarding the state's licensing requirements for servicers and when a loan servicer is required to respond to a qualified written request. Significantly, the regulations broaden the definition of a student loan to include nontraditional education financing products, such as income share agreements and installment contracts, as those have increased in popularity in recent years.

The Oregon Department of Consumer and Business Services' Division of Financial Regulation also finalized its regulations requiring licensure of student loan servicers. The new regulations primarily address state licensure requirements, including requirements for a bond, annual reports, and certain liquidity and operating reserves. However, they also seek to impose new affirmative duties modeled after already existing requirements in the mortgage loan servicing industry, such as promptly crediting borrower payments and assessing fees, promptly correcting servicing errors, and responding to written inquiries from borrowers by a given deadline.

Modeling student loan servicing regulations after mortgage loan servicing regulations remains popular. In June, Louisiana enacted two new

laws, one which requires student loan servicers to respond to borrower complaints and written inquiries within a certain time frame (similar to the qualified written request duties imposed on mortgage loan servicers under federal law), another which requires private education lenders to register with the state and regularly report on their activities.

Kentucky also enacted a student loan servicing law in April, which requires student loan servicers to obtain a state license and established several reporting requirements. However, the law falls short of imposing additional servicing duties, such as a duty to respond to certain borrower inquiries.

Another issue still developing at the state level concerns whether student loan debt forgiveness is taxable under state law. Although the 2021 American Rescue Plan Act exempted student loan forgiveness from federal income taxes through 2025, states have taken diverging positions on whether there will also be a state-level tax exemption. Some states, like Virginia and New York, have unequivocally stated that debt forgiveness will not be taxable under state law. Others, such as Indiana, Mississippi, and North Carolina, have confirmed that the debt forgiveness *will* be taxable. Depending on the outcome of the federal Student Debt Relief Plan, this may become a hot issue next year in state legislatures where the taxability of debt forgiveness remains undecided.

Developments in Student Lending and Bankruptcy

For many years, one of the hot-button issues in student lending was the standards bankruptcy courts apply when assessing whether a student loan is dischargeable. Although the standard has remained the same, in 2022, the Department of Justice (DOJ), in coordination with the Department of Education, implemented a new [process](#) for DOJ attorneys to follow when making recommendations to bankruptcy judges about whether to grant a student loan discharge.

Specifically, Congress has set a relatively high bar for discharging student loan debt in bankruptcy when compared to other types of debt. A debtor must prove, in the context of an adversary proceeding, that the student loan debt has created an undue hardship. Although the DOJ does not decide whether a loan is dischargeable in a bankruptcy case, it often makes a recommendation to the court in the context of a federal student loan. In November 2022, the Biden Administration issued guidance on when the DOJ, in conjunction with the DOE, should recommend discharge to the court.

Under this guidance, the DOJ will have a debtor complete an attestation form that describes the hardship the loan will create. The Justice Department will then work with the DOE to evaluate multiple “undue-hardship factors.” They include the following:

- Present ability to pay: The DOJ will use standards developed by the IRS to calculate the debtor’s expense to income ratio. Depending on the outcome, the Justice Department may determine that the debtor does not have the present ability to pay.

- Future ability to pay: The Justice Department will also evaluate whether the debtor’s present inability to pay is likely to continue into the future. The department’s attorney will look at factors like retirement age, disability, employment, among others. Depending on the presence, or nonexistence, of the factors, the DOJ will assess future ability to pay.
- Good faith efforts: The DOJ will also evaluate the debtor’s efforts to earn income, manage expenses, and repay the loan. Using many factors, the department will assess whether the debtor has made a good faith effort to repay, rather than seeking bankruptcy protection prematurely.

Based on these factors, the DOJ will decide whether to recommend a student loan discharge to the bankruptcy judge. In its press release, the department described this new process in the following way: “By simplifying the process and establishing clear standards, the agencies hope to significantly reduce the burden on borrowers and government attorneys, provide a clear path for borrowers to seek discharges and add safeguards to promote consistency and predictability.”



TELEPHONE CONSUMER PROTECTION ACT

Authors: Virginia Bell Flynn, Chad Fuller, Brooke K. Conkle, Susan N. Nikdel, Sarah E. Siu

Looking Back

2022 saw a shift in litigation and compliance concerns for the Telephone Consumer Protection Act (TCPA). The fallout of the Supreme Court's definition of an automated telephone dialing system (ATDS) began to lessen the exposure for everyday TCPA cases, but meant that new issues came to the forefront for consumer-facing companies. First, plaintiffs' attorneys began to utilize lesser-litigated regulations related to the TCPA, including regulations on the established business relationship and the National Do Not Call Registry. Second, allegations related to prerecorded messages continued an upward trend. Where the *Facebook* decision decreased exposure for cases predicated on use of an ATDS, the decision did not touch potential liability related to messages with a prerecorded or artificial voice.

Developments in Litigation

Post-Facebook Fallout Continues: Circuit Courts Weigh In

The Supreme Court's decision in *Facebook v. Duguid*, 141 S. Ct. 1163 (2021), which defined what constitutes an ATDS under the TCPA, celebrated its one-year anniversary in April 2022. In the wake of that ruling, the question remained how lower courts, particularly circuit courts of appeal, would apply the opinion, especially when some district courts interpreted Footnote 7 of the opinion to extend the definition of ATDS to devices that randomly order pre-produced lists of phone numbers, at least in early stages of litigation. A review of the early district court decisions can be found [here](#).

The Ninth Circuit was the first court of appeal to address the question. In a succinct, emphatic opinion issued on January 19, 2022, in *Meier v. Allied Interstate LLC*, No. 20-55286, 2022 WL 171933 (9th Cir. Jan. 19, 2022), the court quietly rejected one of the last remaining arguments made

by plaintiffs, attempting to neutralize the *Facebook* opinion. Echoing Footnote 7 of *Duguid*, Meier alleged that Allied Interstate's click-to-dial, HCI system – the LiveVox platform – was an ATDS under the TCPA because the system stores telephone numbers using a sequential number generator and produces them to be dialed in the same order as provided. Rejecting the infamous Footnote 7 argument, it affirmed a district court's grant of summary judgment to the defendant and held that a system that stores a pre-produced list of numbers does not qualify as an ATDS under the statute. The court explained that “[u]nder Meier’s interpretation, virtually any system that stores a pre-produced list of telephone numbers would qualify as an ATDS (if it could also autodial the stored numbers ...).” The court also found that the LiveVox system at issue was not an ATDS because it does not have the capacity to automatically dial telephone numbers, and though Meier highlighted the system’s ability to switch from “dialer” functions to click-to-dial functions, the court nevertheless concluded that the system was not an ATDS.

“Under Meier’s interpretation, virtually any system that stores a pre-produced list of telephone numbers would qualify as an ATDS (if it could also autodial the stored numbers ...).”

The Eighth Circuit followed suit in March 2022, upholding separate district court decisions finding that a system that sends promotional text messages to phone numbers randomly selected from a database of customer information is not

an ATDS under the TCPA. *Beal v. Outfield Brew House, LLC*, 29 F.4th 391 (8th Cir. Mar. 24, 2022). The concise opinion espouses a commonsense reading of the word “produce,” finding that the word requires an ATDS to generate a random number, rather than to select a number randomly. Not only did the Eighth Circuit conclude that the Txt Live system under scrutiny “is exactly the kind of equipment *Facebook* excluded” from the definition of an ATDS, the court also rejected the Footnote 7 argument. Where the appellants’ attorneys argued that Footnote 7 of the *Facebook* decision saved its argument that the Txt Live system was an ATDS because it stored numbers to be dialed at a later time, the court disagreed. “Like other courts, we do not believe the [Supreme] Court’s footnote indicates it believed systems that randomly select from non-random phone numbers are Autodialers.” Rather, the system is simply one “that merely stores and dials phone numbers.” The opinion was one of the first major opinions applying the Footnote 7 argument specifically to text messaging systems, as the majority of Footnote 7 arguments have been directed toward predictive dialers.

Text Messages Are Not Prerecorded Messages

Although the *Facebook* decision made it more difficult for plaintiffs to prevail on ATDS claims, plaintiffs have continued to explore new potential avenues for litigation. One recent theory is that text messages qualify as “artificial or prerecorded voice messages” under the TCPA, which would mean that marketing text messages could not be sent without prior express consent. In *Eggleston v. Reward Zone USA LLC*, No. 2:20-cv-01027-SVW-KS (C.D. Cal. Jan. 28, 2022), one of the first lawsuits to address this question on the merits, the U.S. District Court for the Central District of California soundly rejected the argument.

The plaintiff in *Eggleston* argued that text messages meet the statutory definition because “‘artificial’ means ‘humanly contrived, often on a natural model’; ‘prerecorded’ means ‘to set down in writing in advance of presentation or use’; and ‘voice’ means ‘an instrument or medium of expression.’”

The District Court rejected this argument as being “beyond the bounds of common sense” and in “conflict with a primary principle of statutory interpretation — that words in a statute should generally be given their most natural understanding unless circumstances suggest otherwise.” The court explained that the most natural understanding of “voice” refers to sounds from a vocal system, and that if Congress had intended to capture text messages, “it could have easily chosen clearer, more literal terms to do so, such as ‘medium of expression’ or ‘communication.’”

Revocation of Consent: The Art of Saying No

In April 2022, two separate district courts declined to issue dispositive rulings based on a revocation of consent theory, holding that because the plaintiffs had not expressly revoked their consent, the sufficiency of the revocation was an issue of fact for a jury.

In *Carroll v. Medicredit, Inc.*, No. 2:20-cv-01728-KJD-EJY (D. Nev. Mar. 18, 2022), the court denied the parties’ cross-motions for judgment on the pleadings as to claims under the TCPA (and the Fair Debt Collection Practices Act) that arose out of collection calls placed after the parties had agreed to settle the underlying debt. With regard to the TCPA claim, Medicredit admitted that it was liable to Carroll if she could show that she revoked her prior express consent to receive such calls. The parties agreed that Carroll had given consent when negotiating with Medicredit, but Carroll asserted that she revoked her consent by settling the underlying debt. In denying both parties’ motions for judgment on the pleadings, the court held that without evidence showing how Carroll had initially given her consent, it could not determine as a matter of law that merely settling the underlying debt was enough to show revocation.

Similarly, a Kentucky district court judge granted in part and denied in part a defendant’s motion for summary judgment under the TCPA in *Barnett v. First National Bank of Omaha*. The court held that the plaintiff’s request to have information sent to him via the mail instead of over the phone, along

with the plaintiff's refusal to talk to a collector when the defendant called after choosing mailed delivery, gave rise to a genuine issue of fact as to whether the plaintiff revoked consent to be contacted, even without explicit revocation. While the court agreed with defendant that the defendant had not used an ATDS, it noted that the TCPA is "silent on whether and how a consumer may revoke previously-granted consent." The court ultimately, looking at the "totality" of the circumstances, found that revocation of consent was a disputed issue of fact for a jury.

Eleventh Circuit Finds TCPA Class Members Must Have Standing

In July 2022, the Eleventh Circuit vacated a district court's certification of a TCPA class action in *Drazen and Godaddy.com, LLC v. Pinto*, with a reminder that class action plaintiffs do not get a free pass on constitutional standing requirements. Although the parties had not briefed the issue before the Eleventh Circuit, the court ruled that the class definition did not meet Article III's standing requirements and remanded the case to the district court to give the parties an opportunity to revise the definition. In so ruling, the court also held that courts should apply their own jurisdiction's standing analysis to unnamed plaintiffs in nationwide class actions, even where the standing question is the subject of a circuit split.

The district court certified a nationwide class that may or may not have received more than one text message, despite the Eleventh Circuit's ruling in *Salcedo v. Hanna* that a single unwanted text message is insufficient to give rise to Article III standing. The district court reasoned that only the named plaintiff in the litigation needed standing and, further, that unnamed class members who fell short of *Salcedo*'s requirements might still have standing in other circuits.

On appeal, the Eleventh Circuit re-raised the issue of subject matter jurisdiction *sua sponte*. Relying on the U.S. Supreme Court's decision in *TransUnion LLC v. Ramirez*, the Eleventh Circuit concluded that to recover individual damages, all plaintiffs within the class definition—named or unnamed—must have standing. The court harmonized its

earlier *Cordoba* decision with *Ramirez*, explaining that *Cordoba* did not stand for the principle that unnamed class members could rely solely on the standing of the named class representative, but only that the standing analysis for class members should take place at the class certification stage, rather than as a preliminary inquiry. The Eleventh Circuit also rejected the district court's approach to nationwide class standing, holding that a jurisdiction cannot "check our Article III requirements at the door" and must apply its own standing precedents to all class members regardless of the law of their domicile.

Ninth Circuit Finds "Residential" Phones Can Encompass Business Phones for Purposes of Checking the National Do Not Call Registry

In October 2022, the Ninth Circuit reversed the dismissal of a TCPA suit on the grounds that TCPA statutory protections extend not only to individuals, but also to business entities. The litigation involved claims that the defendants violated the TCPA by using an automatic telephone dialing system to send 7,527 text messages to plaintiff home improvement contractors with purported client leads. Fifteen of the 51 plaintiffs had registered their numbers with the National Do Not Call Registry. The defendants moved to dismiss, contending, among other things, that the plaintiffs lacked statutory standing because the TCPA protects only individuals from unwanted calls. The Idaho district court judge agreed.

The Ninth Circuit rejected this argument, noting that 47 U.S.C. § 227(b) provides that a "person or entity" may recover money damages or obtain injunctive relief under the statute. "Using a plain language analysis and reading the statutory language in context, we conclude that under the most natural reading of the term, 'entity' includes a business. Section 227(b) thus covers calls to the cell phones of businesses as well as individuals."

The defendants next argued that those 15 plaintiffs who subscribed to the National Do Not Call Registry and who brought additional claims under Section 227(c) do not qualify for its protection as they used their cell phones for both business and personal purposes, and the implementing regulations apply

only to “residential” telephone subscribers. The court noted that in response to a 2003 petition, the Federal Communications Commission (FCC) declined to explicitly exempt calls made to “home-based businesses” from protection, but instead said it would “review such calls as they are brought to our attention to determine whether or not the call was made to a residential subscriber.” Based on this FCC guidance and district court findings around the country, the Ninth Circuit held that cellphones on the registry are presumptively residential phones and can still be considered residential when used for both personal and business purposes.

The court said that the FCC has yet to clarify when a mixed-use phone ceases to become a residential phone and becomes a business phone, so the defendants could overcome the presumption that the disputed phones are residential later in the litigation by showing after discovery “that plaintiffs use their cell phones to such an extent and in such a manner that the presumption is rebutted.” The court elaborated that in determining whether the presumption has been rebutted, it would look at: (1) how plaintiffs hold their phone numbers out to the public; (2) whether plaintiffs’ phones are registered with the telephone company as residential or business lines; (3) how much plaintiffs use their phones for business or employment; (4) who pays for the phone bills; and (5) other factors bearing on how a reasonable observer would view the phone line.

The majority additionally stated that the FCC “is free in future regulations or orders to interpret § 227(c) differently. If the FCC does so, we will of course defer to its interpretation, provided that the interpretation is consistent with a reasonable understanding of the statutory language.”

Developments in Regulatory Oversight

Indiana Attorney General Kicks Off 2022 by Reiterating Policy Priority to Aggressively Pursue Robocallers

Indiana Attorney General (AG) Todd Rokita began 2022 by announcing his intention to continue aggressively pursuing robocallers and summarizing the actions taken by his office in

2021. This included calling on the FCC to revise its rules to increase accountability, implementing new technologies to shorten the time for the AG to investigate complaints concerning robocalls, and litigating to ensure that consumers are protected against robocalls.

Shortly after announcing his 2022 policy priority, Attorney General Rokita joined 50 other AGs in responding to the FCC’s public notice to support its proposal to stem the tide of foreign-originated illegal robocalls by increasing obligations on “gateway providers” – i.e., the first U.S.-based provider in the call path of a foreign-originated call that transmits the call directly to another intermediate provider or a termination voice service provider in the United States. Among other issues, the AGs specifically supported the FCC proposals to require gateway providers to implement STIR/SHAKEN caller ID authentication to verify foreign-originated calls that use U.S.-based phone numbers.

However, Attorney General Rokita is not simply waiting for the FCC to promulgate regulations addressing the foreign-originated illegal robocalls. Indeed, he initiated a lawsuit styled *State of Indiana v. Startel Comm., LLC*, No. 3:21-cv-00150, in the Southern District of Indiana against individuals and entities that allegedly provided substantial assistance to foreign robocallers that made millions of such illegal calls. The AG concedes that it is “a first-of-its-kind lawsuit,” but if it survives dismissal, we expect that it will not be the last.

State AGs Establish Anti-Robocall Litigation Task Force to Target Facilitators of Foreign Illegal Robocalls

In August 2022, state AGs announced that they established a nationwide Anti-Robocall Litigation Task Force. The task force comprises AGs from all 50 states and will investigate and prosecute companies suspected of allowing or using illegal robocalls from foreign entities. The task force will be led by North Carolina Attorney General Josh Stein, Indiana Attorney General Todd Rokita, and Ohio Attorney General Dave Yost.

While the states have a long history of engaging in telemarketing enforcement, this effort represents

a new level of commitment. The task force has issued over 20 civil investigative demands to over 20 companies.

This endeavor builds on the FCC's latest efforts to reduce the numbers of scam calls. In May 2022, the FCC voted to require telecommunications providers to take steps to block illegal calls coming from outside the United States, noting that most of the illegal robocalls to United States consumers originate overseas or come through gateway providers. The FCC signed memoranda of understanding with 36 states and the District of Columbia at that time, with all pledging to investigate robocalls. With the creation of the task force, the remaining states have come on board.

While the breadth of the task force remains to be seen as it continues to ramp up, companies should be prepared to see an increase in enforcement efforts.

Looking Forward to 2023

We anticipate that the following trends will take shape in 2023:

- **Continued emphasis on prerecorded messages.**

While *Facebook* provided significant clarity for the definition of an ATDS, it did not alter TCPA jurisprudence on prerecorded messages. At the same time, companies are struggling with labor shortages and are looking to use prerecorded or IVR technology in their communications with customers. Look for prerecorded message claims to continue as the major source of TCPA litigation.

- **Added interest in TCPA regulations.**

In another consequence of *Facebook*, plaintiffs who once challenged companies' use of ATDSs are now challenging companies' failure to comply with TCPA regulations, including failure to check the National Do Not Call Registry. We anticipate that affirmative defenses, such as the established business relationship, will gain more traction as courts navigate the post-*Facebook* world.

- **Even more activity at the state level.**

The Florida Telemarketing Sales Act (FTSA) has served as a model for various states, including Washington and Oklahoma, to step into the void left by the *Facebook* decision. Look for even more states to follow the trend, potentially requiring a patchwork scheme for federal and state compliance strategies.



TRIBAL LENDING

Authors: David N. Anthony, Harrison Scott Kelly, John (Jed) Komisin, Meagan Anne Mihalko

Lawsuits involving tribal lending continued in 2022. The enforceability of arbitration provisions remained a hot topic, with the Ninth Circuit Court of Appeals vacating a previous ruling that found a tribal arm's provision to be enforceable. The Ninth Circuit also rejected a constitutional challenge to the Consumer Financial Protection Bureau's (CFPB) structure and held that a tribal lender's CEO may be potentially liable individually. Nevertheless, other courts generated more positive developments in the tribal lending space, including decisions granting motions to dismiss claims against tribal lenders as entitled to sovereign immunity as the "real party in interest" and due to their status as economic arms of the tribe. These decisions indicate that courts will not necessarily give the green light to every case filed against a tribal lending entity, and instead, will scrutinize the efficacy of these claims appropriately in the context of a well-placed challenge.

Ninth Circuit Rejects Tribal Lender's Challenge to Constitutional Structure of CFPB and Holds CEO Individually Liable

The U.S. Court of Appeals for the Ninth Circuit issued an opinion on May 23, 2022, rejecting a tribal lender's constitutional challenge to the CFPB's structure. *Consumer Fin. Prot. Bureau v. CashCall, Inc.*, 35 F.4th 734 (9th Cir. 2022). The Ninth Circuit also affirmed the district court's finding of liability against the corporate defendants and CEO for engaging in deceptive practices in violation of the Consumer Financial Protection Act (CFPA). The Ninth Circuit ordered the district court to reassess the civil penalty and vacated the district court's decision to deny restitution.

In 2016, the California federal district court granted the CFPB's motion for partial summary judgment, holding that the lending entity was the "true lender" on the loans, and the corporate defendants engaged in a deceptive practice within the meaning of the CFPA when servicing and collecting on the loans by creating the false impression that the loans were enforceable and that borrowers were

obligated to repay the loans according to the terms of their loan agreements.

The defendants argued that the CFPB lacked authority to bring the original action due to its unconstitutional structure, as restrictions on the removal of the CFPB's director violated the separation of powers. However, the Ninth Circuit rejected that argument, finding that Director Kraninger formally ratified the CFPB's decisions to file the "original and amended complaints against Defendants, and to file the notice of appeal to the [Ninth Circuit]." The court reasoned that a "party challenging an agency's past actions must ... show how the unconstitutional removal provision actually harmed the party," and found that there was no suggestion of actual harm in the case. The court also declined to consider the argument that the CFPB structure violated the appropriations clause, finding that the argument had not been timely asserted.

The defendants also appealed the district court's finding that the CEO could be held individually liable under the CFPA on the basis that the CEO participated directly in and could control the corporate defendants' conduct. The Ninth Circuit affirmed the district court, however, rejecting the CEO's argument that he "lacked the necessary mental state because he relied on advice of counsel." The Ninth Circuit found this was not a "valid defense on the question of knowledge required for individual liability," and continuing to collect after September 2013 was reckless, regardless of any advice from counsel.

The Ninth Circuit also found "[the tribal entity's] involvement in the transactions was economically nonexistent and had no other purpose than to create the appearance that the transactions had a relationship to the Tribe." The Ninth Circuit affirmed the district court's decision, refusing to give effect to the choice-of-law provision and to applying the law of the borrowers' home states, which resulted in the loans being invalid.

Finally, while not holding that “restitution is necessarily appropriate in this case” or what amount of restitution would be appropriate, the Ninth Circuit held the district court made a legal error by: (1) finding “bad faith” was required to order restitution; and (2) incorrectly outlining the legal framework to determine the amount of restitution.

Ninth Circuit Vacates Prior Ruling Finding Delegation Clause Enforceable

In *Brice v. Plain Green, LLC*, 13 F.4th 823 (9th Cir. 2021), the Ninth Circuit held on September 16, 2021, that “an agreement delegating to an arbitrator the gateway question of whether the underlying arbitration agreement is enforceable must be upheld unless *that specific delegation provision* is itself unenforceable.” The decision created a circuit split with the Second, Third, and Fourth circuits that previously held certain arbitration agreements to be unenforceable. Judge Fletcher, who sat on the original three-judge panel, strongly dissented and argued that under the Federal Arbitration Act, arbitration agreements are invalid if they effectively waive a party’s right to pursue justice. Over Judge Fletcher’s dissent, the Ninth Circuit remanded the case with instructions to proceed with arbitration.

In June 2022, however, the Ninth Circuit vacated the opinion and agreed to a rehearing *en banc*. After the original decision was vacated, the parties ultimately agreed to settle the action on a class basis. The case is in the process of final settlement and dismissal.

Eleventh Circuit Poised to Weigh In on Prospective Waiver Doctrine Scope

On December 10, 2020, Judge William F. Jung of the Middle District of Florida found an arbitration clause that: (1) made federal law applicable and (2) designated AAA or JAMS to arbitrate the dispute, was substantively unconscionable because the agreement precluded the consumer from vindicating Florida state law via arbitration. *Dunn v. Global Trust Mgmt., LLC*, 506 F. Supp. 3d 1214 (M.D. Fla. 2020). The court found Florida law applicable notwithstanding a tribal choice-of-law provision. It also acknowledged

the prior precedents invalidating arbitration agreements based upon choice-of-law provisions waiving *federal* law, and it recognized that the decision represented an extension of existing law invalidating tribal loan agreements.

The defendants appealed that decision to the Eleventh Circuit Court of Appeals, and oral argument was heard on March 9, 2022 (link to audio of the oral argument available [here](#)). The court is poised to weigh in on the scope of the prospective waiver doctrine and determine whether lack of access to a specific state’s law renders a delegation clause in an arbitration agreement unenforceable. The defendants argued that if you cannot contractually waive application of a specific state’s law, then there is no point to a choice-of-law provision. The plaintiff argued that the ban on access to state law regimes renders the delegation clause unworkable. A decision is expected shortly.

First Circuit Finds Tribes Are Not Exempt From Bankruptcy Stay

The U.S. Court of Appeals for the First Circuit furthered a circuit court split on May 6, 2022, when a divided panel found the U.S. Bankruptcy Code “unequivocally strips tribes” of their sovereign immunity to suit. *Coughlin v. LAC Du Flambeau Band (In re Coughlin)*, 33 F.4th 600 (1st Cir. 2022). The decision reversed a bankruptcy court’s ruling that a tribal lender was immune to claims for attempting to collect a debt after a debtor filed for Chapter 13 bankruptcy protection.

The tribal lender argued that it was immune from the debtor’s suit for the stay violation. The case addressed the definition of “government unit” in the Bankruptcy Code. While the bankruptcy court found the tribe to be immune, the First Circuit found that the waiver of sovereign immunity for the federal government, any state or city in the country, and “other foreign or domestic government” included tribes. The decision has been appealed to the U.S. Supreme Court. Briefing on the petition for a writ of certiorari was fully submitted as of November 22, 2022, and was distributed for a January 6, 2023 conference (link to docket [here](#)).

Florida Court Dismisses Tribal Lending Suit

In May 2022, a Florida state court judge dismissed a complaint against Mobiloans – a tribal lending entity wholly owned by the Tunica-Biloxi Tribe of Louisiana – alleging that Mobiloans operated a predatory lending scheme under the semblance of a tribal affiliation with the Tunica-Biloxi Tribe of Louisiana. *Reyes v. Mobiloans LLC, et al.*, No. 2020-16482-CODL (Volusia Cnty. Apr. 11, 2022). The court found that the Tunica-Biloxi Tribe appeared to help run the business.

The judge granted sovereign immunity to Mobiloans, finding it was an appropriate tribal affiliate, and dismissed tribal and company officials also named as defendants. While sovereign immunity typically does not extend to individuals, lawsuit allegations accused the individual defendants of misdeeds in their official capacities, and therefore, the “real party in interest” was Mobiloans.

In reaching its decision, the court found that because some of Mobiloans’ revenue went to the Tribe’s school and social services, finding no sovereign immunity under these circumstances would “defeat the intended purposes of ‘encouraging tribal self-sufficiency and economic development’” The court found that Mobiloans met the definition of a tribal entity under the six-prong test established by the Tenth Circuit in *Breakthrough Management Group, Inc. v. Chukchansi Gold Casino & Resort*.

The plaintiff’s attorneys have strategically tried to avoid sovereign immunity defenses by targeting individual defendants within a tribal government or arm of the tribe entity. This case, as well as the presentation of a “real party in interest” argument, helped avoid that pleading gambit and ensure appropriate respect for independent and sovereign interests.

Eastern District of Virginia Grants Motion to Dismiss

In *Mao v. Global Trust Management, LLC*, No. 4:21-cv-0065 (E.D. Va. Mar. 31, 2022), the Eastern District of Virginia dismissed various claims against a tribal lender, including claims under the Fair Debt Collection Practices Act (FDCPA) and violations of the Racketeer Influenced and Corrupt Organizations Act.

Regarding the FDCPA claim, the court recognized that while “efforts to collect debt that is unenforceable under state law can [state] a claim under the FDCPA,” the plaintiffs failed to allege facts making it plausible, instead of merely possible, that the debt was unlawful. The court noted that the plaintiffs failed to comprehensively identify the allegedly violated state statutes and failed to provide necessary specifics about the loans to support the contention that they violated each statute. The court further noted the plaintiffs’ failure to sufficiently allege a legal relationship between the defendants and downstream debt collectors to establish vicarious liability.

The court also dismissed a RICO conspiracy claim on the grounds that the allegations purportedly establishing an agreement to participate in the enterprise were “conclusory rather than factual.” The court reasoned that a RICO conspiracy requires factual allegations, showing the “when or where the agreement took place, or the specific substance of any communications. ... Simply stating that the parties ‘agreed’ ... is not sufficient.”

Mao serves as a good reminder that testing the sufficiency of pleadings is a good tool for litigants to consider in the context of tribal lending suits. Not every case will automatically survive a challenge under Rule 12(b)(6).

UNIFORM COMMERCIAL CODE AND BANKING

Authors: Bill Mayberry, Mary C. Zinsner, Elizabeth M. Briones, Caleb N. Rosenberg

Looking Back at 2022

Financial institutions continued to see a steady increase in fraud-related litigation in 2022, including wire transfer cases implicating UCC defenses and scams involving the elderly. We also saw a continued rise in mass arbitrations as well as some significant Supreme Court opinions interpreting the Federal Arbitration Act. The Consumer Financial Protection Bureau (CFPB) was busy in the enforcement arena, focusing on dark patterns, consumer deposit account activity including garnishments, and overdraft charges. The year was a busy one for bank litigation and regulatory attorneys.

Fraud Litigation

Courts Examine Duty of Care

In 2022, courts regularly examined the issue of whether a duty of care was owed and whether a bank owes duties outside of the contract of deposit to detect fraud. This frequently arises in the context of fraud cases in which the bank allows a transaction involving a customer to proceed, and the plaintiffs claim the bank either knew or should have known the transaction was fraudulent. For example, in a case (No. 22-1143, 2022 WL 2356776 (E.D. Pa. June 30, 2022)), the plaintiff was not a customer of the defendant bank, yet alleged that the bank owed it a duty of care when the bank was notified of potential fraud and allowed its customer to withdraw funds from its deposit account. The question presented was whether the bank affirmatively created a duty of care to the plaintiff by allegedly agreeing to freeze the funds pending a fraud investigation. The court noted the substantial precedent disavowing any duty owed to noncustomers. The court ultimately dismissed the case, finding that under state law, mere knowledge of a dangerous situation, even by one who can intervene, is not sufficient to create a duty to act.

Courts also reaffirm the established principle that banks generally do not owe noncustomers a duty of care. In a case (No. 3:22-cv-00025-MMD-CLB, 2022 WL 3648033 (D. Nev. Aug. 24, 2022)), the plaintiff brought an action against the bank for the losses he suffered when hackers convinced him to wire \$30,000 into an account at the bank. The bank filed a motion to dismiss arguing that banks process billions of transactions and imposing a duty of care to noncustomers would subject banks to limitless and unpredictable liability, creating a zone of risk that would be impossible to define. The court agreed and granted the bank's motion to dismiss.

Courts Recognize a UCC Privity Requirement in Wire Fraud Cases

Federal courts are increasingly finding that the UCC contains a privity requirement, allowing a sender of a payment order to seek a refund only from the bank with which it has a banking relationship.

In a case involving a national bank (No. 2:21-cv-12835 (ES) (LDW), 2022 WL 16706948 (D.N.J. Oct. 3, 2022)), the U.S. District Court for the District of New Jersey found that a lack of privity between the plaintiff that issued the wire transfer and the bank that released the funds to the beneficiary was a bar to recovery. There, the plaintiff, a law firm, fell victim to a wire transfer scheme. On November 25, 2019, the law firm received a bank check in the amount of \$119,000 from a potential new client. The law firm deposited the check with its bank. The next day, the plaintiff law firm received instructions from the potential new client to wire \$118,550 to an account at the defendant bank allegedly belonging to "Diamond PLC." The law firm directed its bank to initiate the wire transfer, but there was a discrepancy between the account name and the account number on the payment order. The defendant bank, as intermediary bank, then processed the payment

order for the plaintiff's bank pursuant to the order's instructions and wired the funds to Access Bank PLC (formerly Diamond Bank PLC) instead of to Diamond PLC. The plaintiff's bank later informed the plaintiff that the initial check was fraudulent and likely part of a scam to defraud the law firm. The law firm sued the defendant bank to recover the wired funds. The defendant bank moved to dismiss the one cause of action against it arguing, among other things, that the law firm lacked privity with the bank. The court agreed that privity is required, and because the plaintiff failed to allege it, the plaintiff lacked standing to assert a claim under Article 4A.

In *Approved Mortgage Corporation v. Truist Bank*, No. 1:22-cv-00633-JMS-TAB, 2022 WL 16635290 (S.D. Ind. Nov. 2, 2022), the plaintiff was infiltrated by hackers, which set off a chain reaction of events resulting in the wiring of more than \$500,000 to depositors at the bank. The plaintiff, who was not a bank customer, sued the bank asserting UCC and negligence claims, maintaining that the bank failed to detect the suspicious activity and accepted the wire transfers despite signs of fraud. The court determined that the UCC contains a privity requirement allowing each sender of a payment order to seek refund only from the bank with which it has a banking relationship. The court also found that the plaintiff's negligence claim was preempted by the UCC and granted the motion to dismiss.

Commercial Reasonableness of Security Procedures Under the UCC

In *Rodriguez*, 46 F.4th 1247 (11th Cir. 2022), when the plaintiffs opened their personal and commercial bank accounts at the bank branch, the plaintiffs and their bank agreed to use specific security protocols for the online wire transfer system. The security protocols included a multiple-factor verification. A fraudster, impersonating plaintiffs, contacted the bank, bypassed the procedures, wired funds out of the accounts, and changed the password to the accounts. When plaintiffs discovered the unauthorized transfers, they sued the bank, arguing that its security procedures were not commercially reasonable under UCC Article 4A-202 despite the fact that plaintiffs had agreed to the protocols at the time the accounts were opened. The Eleventh

Circuit acknowledged that the UCC provides banks with a safe harbor from refunding fraudulent wire transfers if the bank and the customer had agreed upon "commercially reasonable" security procedures, and the bank followed those procedures in good faith. However, the appellate court also found that whether a security procedure is commercially reasonable is a question of law to be determined by considering all of the following factors: (1) the circumstances of the customer known to the bank (including the size, type, and frequency of payment orders); (2) alternate security procedures offered to the customer; and (3) security procedures in general use by customers and similarly situated receiving banks. The case was remanded to the district court to determine whether the bank's procedures were commercially reasonable based on those factors.

In *Deaconess Associations, Inc., N.A.* No. 3:21-cv-01854-YY, 2022 WL 7690568 (D. Or. Sept. 19, 2022), the plaintiff fell victim to a scam and wired more than a million dollars to a fraudster. In an attempt to evade the UCC, the plaintiff brought a negligence claim against the bank for failing to design and maintain security procedures and internal controls that complied "with applicable banking law, regulations, and commercially reasonable banking practices," and for failing to detect the signs of inconsistencies and potential, fraudulent activity associated with the fraudulent wire transfer. The court rejected this attempt, finding the alleged "post-transfer" conduct fell within the confines of the UCC.

A federal district court in New Jersey dismissed a complaint against a bank filed by a commercial customer duped by an incident involving compromised business email. In *Harborview Capital Partners, LLC v. Cross River Bank*, 600 F. Supp. 3d 485 (D.N.J. 2022), the email account of the Harborview CEO was hacked. The fraudster, purporting to be the CEO, emailed Harborview's account manager, instructing her to initiate four wires totaling \$1.4 million to various accounts at a financial institution in Hong Kong. The account manager complied, and upon receipt of each wire transfer order, the bank contacted the account manager to confirm the details of the transaction.

After the fraud was uncovered, Harborview sued the bank, asserting that it accepted unauthorized wire transfer orders and failed to maintain and/or adhere to commercially reasonable security procedures, seeking to hold the bank liable for the payment of the transfers under the UCC. The court found that even though the customer was tricked by a fraudster into initiating the transfers, the wires were authorized by the customer's account manager who approved and confirmed the transactions. The court concluded that the question of whether the bank complied with commercially reasonable security procedures under Uniform Commercial Code Section 4A-202(2) is not reached if the transfers are authorized.

Banks Propose Response to Rise in Zelle Class Actions

2022 brought a continued increase in actions by consumers alleging harms stemming from use of Zelle. We have seen consumers alleging EFTA violations and state consumer protection claims related to known fraud vulnerabilities. Consumers have also asserted they were misled due to a failure to disclose risks associated with the service and certain advertising claims about the service being secure. Banks are vigorously defending these claims.

Banks have also announced they are working to establish improved network rules to address fraudulent transactions on the Zelle network. The proposed rules would require reimbursement of consumers where it is determined that the consumer has been scammed, by requiring the receiving bank to return the funds to the originating bank to issue a refund to the consumer. The final details of the plan are still being ironed out, and smaller financial institutions have expressed concerns about the costs of refunds.

The new network rules are in response to congressional and CFPB pressure. The CFPB is preparing guidance under Reg. E that would seek to prod banks to reimburse consumers in more circumstances than what occurs in current standard

practice. That CFPB proposal sparked criticism from industry groups, which highlighted the significant fraud controls financial institutions have already implemented to protect consumers from P2P payment scams. Although the details remain in flux, we expect banks to take concrete steps to address consumer and regulatory concerns in 2023.

Arbitration

The Threat of Mass Arbitration Continues as Do Attempts to Mitigate Against It

The influx of consumer mass arbitrations continued in 2022, but this year we also saw companies beginning to proactively draft arbitration agreements to mitigate against that risk. For example, we saw arbitration clauses providing for the selection of certain arbitrators based on fees, less liberal cost-sharing provisions as a default, and provisions for consolidated actions to address common issues of law or fact.

Naturally, we also saw litigation arise out of this type of provision. For example, in *Uber Technologies, Inc. v. American Arbitration Association, Inc.*, Uber sued the AAA over fees arising out of more than 31,000 similar consumer arbitrations. 2022 WL 1110550 (N.Y. App. Div. April 14, 2022). In the parties' agreement, the fee schedule provided that for each case, Uber would be responsible for a \$500 filing fee, a \$1,400 case management fee, and a \$1,500 arbitrator fee. The court ruled against Uber's attempts to avoid paying these fees, noting that "it made the business decision to preclude class, collective, or representative claims in its arbitration agreement with its consumers, and AAA's fees [were] directly attributable to that decision." *Id.* at *70 (citations omitted).

The Supreme Court Weighs In on the FAA

This year saw the Supreme Court decide multiple cases brought pursuant to the Federal Arbitration Act (FAA). In *Morgan v. Sundance, Inc.*, the Court unanimously rejected the rule that waiver of the



right to arbitrate requires a showing of prejudice in addition to conduct inconsistent with the right to arbitrate. 142 S. Ct. 1708 (2022). The Court concluded that this rule was inconsistent with federal waiver law generally and was not justified by the policy favoring arbitration. While the opinion left several issues unresolved, including alternative theories like forfeiture, estoppel, or laches, and the role of state law in analyzing these issues, the safest course of action continues to be pursuing a motion to compel arbitration from the outset of any court.

In *Badgerow v. Walters*, the Supreme Court significantly limited the jurisdiction of federal courts to confirm or vacate arbitral awards under Sections 9 and 10 of the FAA. 142 S. Ct. 1310 (2022). The Court confirmed its prior rulings that the FAA itself does not create subject matter jurisdiction and held that a federal court must have an “independent jurisdictional basis” to confirm or vacate an award. The ruling will likely result in parties turning to state courts for confirmation of arbitral awards in ostensible federal question cases.

Additionally, in *Viking River Cruises v. Moriana*, the Court held that the FAA preempts the California

Labor Code Private Attorneys General Act of 2004 (PAGA), explaining that “state law cannot condition the enforceability of an arbitration agreement on the availability of a procedural mechanism that would permit a party to expand the scope of arbitration by introducing claims that the parties did not jointly agree to arbitrate.” 142 S. Ct. 1906 (2022). The *Moriana* decision may increase the likelihood that arbitration agreements will be enforced based on FAA preemption of state law.

CFPB Enforcement Actions

The Electronic Funds Transfer Act (EFTA)

In April, the CFPB filed a lawsuit jointly with the New York Attorney General against MoneyGram International, Inc. and related entities. The Bureau asserted violations of the Remittance Rule and Reg. E, as well as UDAAP claims based on alleged failures to provide accurate disclosures, promptly investigate errors and appropriately respond to consumers, provide required fee refunds, maintain appropriate error resolution policies, and have sufficient record retention policies to show

compliance with the Remittance Rule and the EFTA. In October, the CFPB filed two more EFTA actions, including one against Choice Money Transfer, raising similar issues.

The CFPB also filed an action against Active Network LLC based on its alleged use of “digital dark patterns” in enrollment practices. The CFPB alleged that the company tricked consumers who attempted to sign up for a fundraising or community event by inserting an additional page into the online registration that enrolled the consumer in a “free trial,” which automatically converted into a paid subscription membership. The CFPB alleged these practices violated the EFTA and Reg. E because the company increased membership fees without sending consumers written notice of the amount and date of the transfers at least 10 days prior to the transaction.

Garnishments

The CFPB’s activity in the garnishment area has also spurred banks to revisit cross-border garnishment practices and review deposit agreements for provisions that the CFPB may deem unfair or deceptive practices.

Deposits and Prepaid Account Activity


Throughout 2022, the CFPB also made clear that it would continue to focus on financial institutions’


deposit and prepaid account activities, including sustained attention on overdraft fees. For example, in its *Supervisory Highlights*, the CFPB noted financial institutions charging overdraft fees after failing to lift initial automatic holds on mobile check deposits. The CFPB is calling for revised policies and procedures governing holds controls to monitor for and detect instances of duplicate holds. The *Supervisory Highlights* also addressed various issues related to prepaid accounts, including financial institutions’ failure to appropriately submit agreements to the CFPB, to honor stop-payment requests, and to communicate error resolutions.

Looking Forward to 2023


This year, we expect fraud and wire transfer litigation to continue to proliferate, especially cases involving third-party scams against the elderly. Bank litigators should continue to rely on lack of privity and other defenses available under the UCC, and in elder fraud cases, various state and federal safe harbor provisions for reporting elder fraud. Additionally, banks should consider the risk of mass arbitration when drafting consumer contracts and include provisions to mitigate against that risk. Finally, we anticipate that the CFPB will continue with robust enforcement activity in the deposit banking arena and other transactions implicating individual consumers. Troutman Pepper attorneys are here to help financial institutions with these issues.

CONSUMER FINANCIAL SERVICES LAW MONITOR




Home About Our Team Events + Webinars Contact Subscribe 


FCRA FDCPA Mortgage Lending, Servicing + Banking Privacy + Cyber Regulatory Enforcement + Compliance TCPA [All Topics](#) [Podcasts](#)



Consumer Financial Services LAW MONITOR

Monitoring the financial services industry to help companies navigate through regulatory compliance, enforcement, and litigation issues


 The Latest [All Entries >](#)



CMS Publishes Final Rule Increasing Government Authority to Recover Overpayments from Medicare Advantage Plans


By [Harry Liberman](#), [Virginia Bell Flynn](#) & [Tina Safi Felahi](#) on February 2, 2023

On February 1, the Centers for Medicare & Medicaid Services (CMS) [published](#) a final rule strengthening their authority to recover...




Virginia Considering Legislation to Permit Remote Work for Employees of Licensed Mortgage Lenders and Brokers

February 2, 2023



CFPB Proposes to Dramatically Cut Safe Harbor for Credit Card Late Fees

February 1, 2023



Year-End Report Reveals Continuing Trend of Increased FCRA and Decreased FDCPA and TCPA Filings in 2022

February 1, 2023

The Consumer Financial Services Law Monitor blog offers timely updates regarding the financial services industry to inform you of recent changes in the law, upcoming regulatory deadlines, and significant judicial opinions that may impact your business. We report on several sectors within the consumer financial services industry, including payment processing and prepaid cards, debt buying and debt collection, credit reporting and data brokers, background screening, cybersecurity, online lending, mortgage lending and

servicing, auto finance, and state AG, CFPB, and FTC developments.

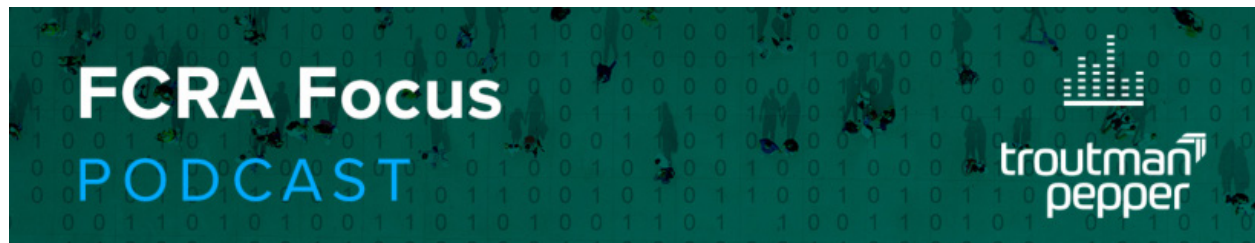
We aim to be your go-to source for news in the consumer financial services industry, helping you navigate through regulatory compliance, enforcement, and litigation issues. Please email cfslawmonitor@troutman.com to join our mailing list to receive periodic updates, or visit the blog at www.consumerfinancialserviceslawmonitor.com.

CONSUMER FINANCIAL SERVICES PODCASTS



Troutman Pepper's ***The Consumer Finance Podcast*** provides reliable, insightful, and entertaining industry-specific content central to consumer financial services. Supplementing our current webinar, advisory and blog thought leadership, this weekly podcast features industry experts, insiders, and other Troutman Pepper attorneys delivering easily digestible analyses on a variety of thought-provoking topics, covering:

- Debt Collection
- Fintech
- Student Lending
- Auto Finance
- Privacy and Cybersecurity
- Litigation Trends
- Fair Lending
- Federal and State Regulation and Enforcement



FCRA Focus is dedicated to discussing “all things” related to the Fair Credit Reporting Act, which regulates the collection of consumers’ credit information and access to their credit reports. Each episode explores an interesting aspect of credit reporting, with the aim of providing new insights that help consumer finance businesses do their jobs better. Guests from the industry and lawyers for consumers as well as business insiders join us *monthly* in this podcast series.

Both podcasts are available on the Troutman Pepper website; our blog, *The Consumer Financial Services Law Monitor*; Google Podcast; Spotify; Apple iTunes; and various other podcast platforms.

CONTACTS

Consumer Financial Services Practice Group Leader

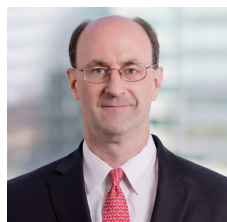


Michael E. Lacy

Partner

michael.lacy@troutman.com
804.697.1326

Additional Contacts



David N. Anthony

Partner

david.anthony@troutman.com
804.697.5410



Justin D. Balser

Partner

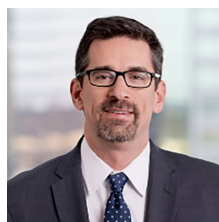
justin.balser@troutman.com
949.622.2443



Keith J. Barnett

Partner

keith.barnett@troutman.com
404.885.3423



Andrew B. Buxbaum

Counsel

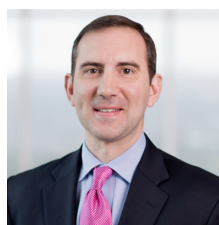
andrew.buxbaum@troutman.com
804.697.1436



Jason M. Cover

Partner

jason.cover@troutman.com
215.981.4821



D. Kyle Deak

Partner

kyle.deak@troutman.com
919.835.4133



Molly DiRago

Partner

molly.dirago@troutman.com
312.759.1926



Virginia B. Flynn

Partner

virginia.flynn@troutman.com
804.697.1480

CONTACTS



Chad R. Fuller

Partner

chad.fuller@troutman.com
858.509.6056



Mark J. Furletti

Partner

mark.furletti@troutman.com
215.981.4831



David M. Gettings

Partner

dave.gettings@troutman.com
757.687.7747



Cindy D. Hanson

Partner

cindy.hanson@troutman.com
404.885.3830



Jon S. Hubbard

Partner

jon.hubbard@troutman.com
804.697.1407



Stefanie H. Jackman

Partner

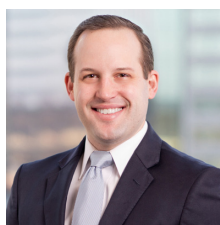
stefanie.jackman@troutman.com
404.885.3153



Anthony C. Kaye

Partner

tony.kaye@troutman.com
470.832.5565



Scott Kelly

Partner

scott.kelly@troutman.com
804.697.2202



James Kim

Partner

james.kim@troutman.com
212.704.6121



Kalama M. Lui-Kwan

Partner

kalama.lui-kwan@troutman.com
415.477.5758

CONTACTS



John C. Lynch

Partner

john.lynch@troutman.com
757.687.7765



Jason E. Manning

Partner

jason.manning@troutman.com
757.687.7564



Bill Mayberry

Partner

bill.mayberry@troutman.com
704.916.1501



Ethan G. Ostroff

Partner

ethan.ostroff@troutman.com
757.687.7541



Kim Phan

Partner

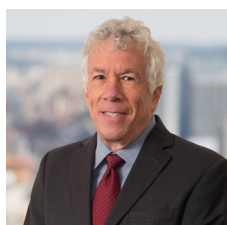
kim.phan@troutman.com
202.274.2992



Ronald I. Raether

Partner

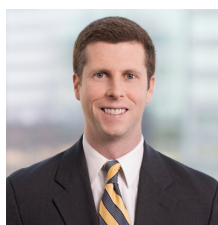
ronald.raether@troutman.com
949.622.2722



Jeremy T. Rosenblum

Partner

jeremy.rosenblum@troutman.com
215.981.4867



Timothy J. St. George

Partner

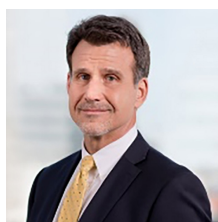
tim.st.george@troutman.com
804.697.1254



Lori J. Sommerfield

Partner

lori.sommerfield@troutman.com
612.327.0322



James K. Trefil

Counsel

james.trefil@troutman.com
804.697.1864

CONTACTS



Christopher J. Willis

Partner

chris.willis@
troutman.com
404.885.3157



Alan D. Wingfield

Partner

alan.wingfield@
troutman.com
804.697.1350



Mary C. Zinsner

Partner

mary.zinsner@
troutman.com
202.274.1932