troutman pepper

2021 Consumer Financial Services Year in Review & A Look Ahead

Consumer Financial Services Practice

January 2022

troutman.com

2021 Consumer Financial Services

Year in Review, January 2022

Table of Contents

Executive Summary 03

About Us 04

Auto Finance 05

Background Screening 08

Bankruptcy 17

Consumer Class Actions. 20

Consumer Credit Reporting 25

Cybersecurity and Privacy 37

Debt Collection 62

Fair Lending. 73

Key Trends and Legislation in Health Care 77

Mortgage 79

Payment Processing and Cards 84

Predatory Lending 86

Student Lending 90

Telephone Consumer Protection Act 96

Tribal Lending 101

Uniform Commercial Code and Banking 104

Consumer Financial Services Law Monitor 110

Consumer Financial Services Webinar Series 111

Contacts 112

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

2021 was a transformative year for the consumer financial services world. As we navigate an unprecedented amount of industry regulation, Troutman Pepper is uniquely positioned to help its clients find successful resolutions and stay ahead of the curve.

In this report, we share developments on auto finance, background screening, bankruptcy, consumer class actions, consumer credit reporting, cybersecurity and privacy, debt collection, fair lending, key trends and legislation in health care, mortgage, payment processing and cards, predatory lending, student lending, the Telephone Consumer Protection Act (TCPA), tribal lending, and the Uniform Commercial Code (UCC) and banking.

By remaining up to date on the latest industry trends and regulatory developments, clients seek out and rely on Troutman Pepper as a trusted resource to help tackle today's issues, while preparing for what lies ahead. We hope this report brings you value.

ABOUT US

Troutman Pepper's Consumer Financial Services Practice Group consists of over 100 attorneys 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 out of a single legal issue, such as compliance solutions and regulatory strategies developing out of contentious litigation.

Our nationwide reputation in consumer litigation derives from our attorneys' extensive experience representing clients in consumer class actions involving the Fair Credit Reporting Act (FCRA); Fair Debt Collection Practices Act (FDCPA) and state law debt collection claims; 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) statutes; Unfair, Deceptive, and Abusive Acts and Practices (UDAAP); mortgage foreclosures, mortgage lending and servicing; Electronic Funds 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); Federal and State Odometer Acts; FTC Holder Rule; Home Affordable Modification Program (HAMP); Home Owner's Equity Protection Act (HOEPA); home warranties; Magnuson-Moss Warranty Act; cybersecurity and privacy; Racketeer Influenced Corrupt Organizations Act (RICO); and the Servicemembers Civil Relief Act (SCRA).

Our regulatory enforcement team comes well prepared to respond to regulators' oversight inquiries, civil investigative demands (CIDs), audit, supervision, examination, and enforcement actions. We have spent years handling similar claims and CID, audit, supervision, examination, and enforcement proceedings. We also are well equipped to handle Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) investigations concerning a variety of matters, including consumer privacy and data security breaches. At Troutman Pepper, we move seamlessly from negotiation to litigation with a team of highly skilled litigators with extensive experience in regulatory enforcement litigation matters.

We regularly advise and proactively prepare our clients 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

The COVID-19 pandemic continued to present considerable instability for automotive retailers throughout 2021, with high-growth volumes in the used vehicle finance market. Enforcement actions and litigation concerning discriminatory lending, disparate impacts, and fraudulent and deceptive origination practices remained among the most prevalent issues for lenders.

Highlights from 2021

NYDFS Settles with State Banks Over Alleged Fair Lending Violations Related to Vehicle Loans[1]

In June 2021, the New York Department of Financial Services (NYDFS) settled with two state banks—Adirondack Trust and Chemung Canal Trust Company—for violations of New York's fair lending law related to the banks' indirect automobile lending programs. Specifically, NYDFS alleged discriminatory practices in the banks' endorsement of dealer markup. NYDFS found that Adirondack Trust, from January 2016 through October 2017, had charged Black borrowers 57 basis points more, Hispanic borrowers 40 basis points more, and Asian borrowers 30 basis points more in discretionary dealer markup than white borrowers. Similarly, NYDFS found that Chemung Canal Trust Company, from January 2016 to August 2020, charged Hispanic borrowers on average 20 to 27 basis points more in discretionary dealer markup than non-Hispanic white borrowers.

NYDFS noted that, while no evidence showed intentional discrimination by the banks, the banks' practice and policies of allowing dealers to impose markup without any credit-related justification resulted in a disparate impact on the basis of race and national origin. The settlements required each party to pay a civil money penalty and provide restitution.

The NYDFS settlements echo last year's FTC settlement with Bronx Honda. In that settlement, the FTC similarly targeted disproportionate dealer markup for African-American and Hispanic customers, among several other fair lending abuses. Current CFPB Director Rohit Chopra also submitted a statement on the Bronx Honda settlement in his capacity as an FTC commissioner, advocating for the FTC to use its rulemaking authority under the Dodd-Frank Act to target "auto market abuses," including discriminatory practices and issues facing military consumers.[2] Between the NYDFS settlements and the aftermath of the FTC Bronx Honda matter, it is clear that fair lending is going to be a top priority for federal and state regulators going forward.

Arizona District Court Rules Dealership's Advertising Violated TILA and Consumer Leasing Act

A federal district court in Arizona held in *FTC v. Tate's Auto Center of Winslow Inc.* that the Federal Trade Commission (FTC) proved several automobile dealerships' (collectively, Tate's Auto) advertising failed to include legally required credit information in violation of the Truth in Lending Act (TILA) and the Consumer Leasing Act (CLA). The court declined to grant summary judgment on the FTC Act claims, alleging misleading advertisements and deceptive information on car loan applications.

In July 2018, the FTC brought this action against Tate's Auto and co-owners Richard Berry and Linda Tate. The FTC alleged that Tate's Auto and the owners violated TILA and CLA by failing to include legally required credit information in their advertisements, and that the defendants' advertising misled consumers in violation of the FTC Act and inflated consumers' financial information on car loan applications in violation of the FTC Act. Tate's Auto stipulated to a permanent injunction and

[1] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202106291
[2] https://www.ftc.gov/system/files/documents/public_statements/1576002/bronx_honda_final_rchopra_bronx_honda_statement.pdf

monetary damages, but Berry and Tate remained as defendants. The FTC moved for summary judgment against the individual defendants.

The court did not grant the FTC's request for summary judgment on the FTC Act claims, which prohibit "unfair or deceptive acts or practices." The court concluded that the alleged deceptive advertisements did not meet the standard for it to grant summary judgment; instead the advertisements appeared ambiguous. On the second FTC Act claim, Berry and Tate submitted declarations that many of the consumers knew the down payment or income information was misrepresented on the loan applications. As such, the court could not hold as a matter of law that Berry and Tate's practices misled customers.

Department of Justice Enters Into Consent Order for Violations of the Servicemembers Civil Relief Act

On September 29, the DOJ entered into a consent order with American Honda Finance Corporation (AHFC) for alleged violations of the Servicemembers Civil Relief Act (SCRA). Under the SCRA, a residential or motor lessee has the option to terminate the lease in certain circumstances. For example, a person who enters a lease, then subsequently enters military service during the lease period, may thereafter terminate the lease. Likewise, a servicemember already in military service may terminate the lease upon notice of permanent change of station, deployment, or death or serious injury. Once terminated, the lessor must refund any advance payments on a pro rata basis.

The DOJ's allegations against AHFC centered on the refund of advance vehicle lease payments. In connection with their leases with AHFC, some lessees paid an up-front value at lease signing in the form of cash payments, credit for vehicle trade-in, and/or other rebates. The DOJ alleged that AHFC refused to refund the portion of funds attributable to the servicemember's vehicle trade-in value. The consent order required AHFC to refund over $1.58 million to 714 servicemembers. The consent order also required AHFC to pay a civil money penalty of nearly $65,000, and to modify its internal policies and provide training on SCRA compliance.

The DOJ's consent orders are another example of increased regulatory interest in enforcing military consumer protection laws.

SDNY Rules No Waiver of Arbitration Clause After Lender Commences Court Collection Action

In *Murray v. DCH Toyota City*, the Southern District of New York ruled that an auto lender that commenced an action in state court to collect on a borrower's breach of an underlying auto financing agreement did not waive its rights to arbitrate the borrower's subsequently filed fraud claims against the lender in a subsequent court action. *See Murray v DCH Toyota City*, 20-CV-07383 (PMH), 2021 WL 1550074, at *1 (S.D. N.Y. Apr. 20, 2021).

In June 2020, DCH Toyota City brought a civil action against the borrower in the Supreme Court of the State of New York, County of Westchester, to recoup

the balance on the financing, asserting causes of action against the borrower for, *inter alia*, breach of contract and unjust enrichment. In September 2020, the borrower—who was represented by legal counsel—commenced a federal action in the Southern District of New York alleging that DCH Toyota City (i) violated the Truth in Lending Act, 15 U.S.C. § 1601 et. seq. (TILA), (ii) violated Federal Reserve Board Regulation Z, 12 C.F.R. § 1026, promulgated pursuant thereto, (iii) violated New York General Business Law (GBL) § 349 (known as the NY Deceptive Practices Act), and (iv) committed common law fraud arising out of the RISC transaction because DCH Toyota City did not credit and itemize plaintiff's $500 deposit in the RISC.

In response to the plaintiff's federal complaint, DCH Toyota City moved to compel arbitration pursuant to the financing agreement, which contained an arbitration provision. Ultimately, Judge Philip M. Halpern rejected the plaintiff's opposition to arbitration and ruled:

> The [state court action] does not address the same [breach of contract] issues as those in [p]laintiff's federal court complaint, as the state court action] is principally a breach of contract matter in which [d]efendants seek to recover payment for the [v]ehicle.... This [federal court] action, however, involves a truth-in-lending claim; and claims alleging misleading and fraudulent conduct related to the down payment he provided for the [v]ehicle that he contends was not included in the RISC. Though the transaction underlying both this action and the [s]tate [c]ourt [a]ction are the same, they are simply not the same dispute and do not embrace the same or even similar legal issues.

Accordingly, the Southern District of New York granted the defendant's motion to compel and stayed the action pending arbitration.

CFPB Releases Report on Subprime Auto Lending[3]

In September 2021, the Consumer Financial Protection Bureau (CFPB) released a report that compared auto loan outcomes with different lenders in the subprime market. In the report, the CFPB found that banks and credit unions typically lend to borrowers with higher credit scores than finance companies and "buy here pay here" dealerships (BHPH). As a result, banks tend to charge lower interest rates. Specifically, banks charge an average interest rate of 10% for subprime borrowers, compared to 15% for finance companies and 20% for BHPH. The disparity in borrower credit scores also appeared to lead to a disparity in default rates. For example, the CFPB found that the likelihood of a borrower's subprime auto loan becoming at least 60 days delinquent within three years is approximately 15% for banks and between 25% and 40% for finance companies and BHPH. Through regression analysis, the CFPB found that default risk alone doesn't explain differences in interest rates charged by different types of auto lenders. Rather, other factors likely contributed, including variation in borrowers' down payments, vehicle values, access to information, and financial sophistication and variation in lenders' practices and incentives when originating and servicing loans. The CFPB concluded the report by calling for more research on auto loan borrowers' objectives, how they shop for auto loans, and how their objectives and shopping behavior influence borrower and loan outcomes.

Looking Forward to 2022

As courts continue to reopen and the Biden Administration's policies begin to expand, expect consumer-friendly regulators to increase their attention on practices and procedures in consumer lending, particularly as the auto finance industry climbs out of the COVID-19 pandemic. Fair lending, disparate impact, and fraud-in-origination will likely be central themes for regulators as well as for private litigants in 2022.

[3] https://files.consumerfinance.gov/f/documents/cfpb_subprime-auto_data-point_2021-09.pdf

BACKGROUND SCREENING

Introduction

Following a trend from previous years, 2021 included a significant number of initiated actions and court decisions involving violations of the Fair Credit Reporting Act (FCRA), including substantial developments in the area of background screening. In late 2020, the Eleventh Circuit held a consumer reporting agency did not violate the FCRA by reporting a sex-offender record without matching the record to that subject consumer because it notified the user the record needed further investigation before being attributed to the individual. The U.S. District Court for the District of Massachusetts found a background screening agency did not negligently or willfully violate the FCRA by reporting outdated eviction records based on both a lack of individual damages and the company's reasonable reliance on its vendor. Further, the Supreme Court of Arkansas found in favor of Professional Background Screening Association (PBSA) in its suit against Benton County, AR's clerk of court, holding the PBSA was entitled to court records under Arkansas' Freedom of Information Act (FOIA). On remand from the Ninth Circuit, the U.S. District Court for the District of Oregon granted partial summary judgment to a defendant on the disclosures it provided with an employment application. There also has been an uptick in state fair chance and "ban-the-box" laws. Finally, the last year brought an onslaught of rules and regulations that applied (and may still apply) to the tenant screening industry due to the COVID-19 pandemic.

Eleventh Circuit Appellate Ruling Says FCRA Permits Reporting Unmatched Criminal Records in Certain Circumstances

Addressing a recurring issue bedeviling the background screening industry, the U.S. Court of Appeals for the Eleventh Circuit confirmed that it is not inaccurate for a CRA to report a criminal or sex-offender record without matching the record to a subject consumer, so long as the CRA notifies the user that the record needs further investigation before being attributed to an individual.

This seemingly technical ruling under the FCRA goes to the heart of criminal background screening by CRAs in the United States since criminal records in the U.S., in a great majority of cases, do not contain definitive identifying information, such as Social Security numbers or even specific dates of birth. This means that some providers of criminal background screenings provide records in response to a screening without matching to a specific individual, leaving it to the user of the data to conclude whether the record applies to a given individual. This practice has been challenged across the country in private lawsuits; and late last year, the Eleventh Circuit weighed in, validating that reporting unmatched results can comply with the FCRA in certain circumstances.

In reaching this ruling, the Eleventh Circuit paradoxically rejected a lenient legal test on the standard for "inaccuracy" in favor of a more stringent one accepted by a plurality of other federal appellate courts. Nevertheless, the court held the report containing unmatched records passed muster even under that more stringent test.

This precedential decision may become a leading case, defining the duties of CRAs and users of unmatched criminal records under the FCRA. The case is styled *Erickson v. First Advantage Background Services Corp.*, No. 19-11587 (11th Cir. Dec. 4, 2020).

Background

While applying to coach his son's Little League team, Keith Erickson consented to a background check prepared by First Advantage Background Services Corporation. At the time of his application, Erickson's name was "Keith Dodgson" — a name he shared with his long-estranged father. Unfortunately for Erickson, his namesake was a registered sex offender in Pennsylvania. Further complicating matters, Pennsylvania only records the birth year of

registered sex offenders, rather than a full date of birth. In such cases, First Advantage's policy is to search by name only, inform the report's user that any matched record is based on the name alone, and instruct the user to conduct further research before taking action against the subject of the report.

Erickson's background check uncovered his father's sex-offender record. First Advantage sent a report, including the record to Little League, explaining the record was a name-only match, and Little League's "further review of the State Sex Offender website is required in order to determine if this is your subject." First Advantage also sent a letter to Erickson, informing him his background check revealed he shared a name with a registered sex offender. The letter emphasized Little League was "aware this record may not be yours" and would investigate further. Erickson immediately disputed the record with both First Advantage and Little League. Humiliated, he voluntarily chose not to coach his son's team. He and his wife even went so far as to change their family name to avoid any future association with his father.

Erickson filed suit in federal court, claiming First Advantage violated the FCRA's requirement that a consumer reporting agency "follow reasonable procedures to assure maximum possible accuracy" of information included in a consumer report. First Advantage initially disputed the applicability of the FCRA in a summary judgment motion, which the district court denied, and the case moved to trial. After Erickson presented his case at trial, the court granted judgment as a matter of law in favor of First Advantage. The court held Erickson failed to show either the report was inaccurate, or he was harmed — two essential elements of his claim. Erickson appealed.

On appeal, First Advantage did not challenge the district court's denial of its summary judgment motion, so the threshold question of the FCRA's applicability was not an issue. Addressing the inaccuracy element of Erickson's claim, the Eleventh Circuit first discussed the problem of unmatched records in background screenings generally. The court acknowledged it is not uncommon for screening databases to include a sex-offender record without an underlying record of conviction, and some state sex-offender registries, like Pennsylvania's, include only the offender's name and year of birth. This sets the stage for background screeners to regularly face the problem of imperfectly matched records.

First Advantage deals with this problem in three ways. First, in instances where a state registry includes only a birth year, First Advantage conducts a search based on the subject's name only, completely avoiding any partial birth date matches. Second, it notifies the user at the outset that searches in these jurisdictions are based on name only. Third, when a name-only match is found, First Advantage not only includes it in the report, but also instructs the user that further research is required to confirm whether the record belongs to the subject.

Court Adopts "Factually Correct and Free From Potential Misunderstanding" Standard of "Inaccuracy"

The court grappled first with the meaning of "maximum possible accuracy" under the FCRA — a thorny question evaluated by several other circuits. The court rejected a more lenient standard followed by some courts requiring only "technical accuracy." The technical accuracy standard requires only that the information in the report not be factually incorrect. Under this standard, so long as the report does not contain any objective untruth or inaccuracy, there can be no liability.

A plurality of the circuit courts — including the Fourth, Fifth, Sixth, and Ninth circuits — hold that "maximum possible accuracy" means more than mere technical accuracy. These courts typically describe the standard as requiring a report to be neither factually inaccurate nor "materially misleading." The Eleventh Circuit chose to follow this course, finding the statutory text "demands" more than mere technical accuracy. The court focused on the literal definitions of the phrase "maximum possible accuracy" and concluded "information must be factually true and unlikely to lead to a misunderstanding" to meet that standard.

Importantly, the Eleventh Circuit emphasized that whether a report is potentially misleading is an objective inquiry. A reviewing court must "look to the objectively reasonable interpretations of

the report." A report that is "objectively likely to cause the intended user to take adverse action" is objectively misleading, whereas one "that some user somewhere could possibly squint at … and imagine a reason to think twice about its subject" is not. The focus on the "intended user" of the report means the court must consider the reasonable expectation and understanding of a person in the position of that user to determine if the user would likely be misled.

The Eleventh Circuit holds that the CRA's report met its articulated standard because a reasonable user would understand that the record was not matched.

After defining this standard, the court held "the only objectively reasonable interpretation of [First Advantage's] report was one that was not misleading." The report never claimed the record was a certain match; instead, it explained it was a name-only match, and "cautioned that the record might not be Erickson's at all." Furthermore, a reasonable user of the report in Little League's shoes would not be so misled as to take adverse action based on the report alone. Adding further support for this conclusion was the fact that First Advantage's report reminded Little League that "further review of the State Sex Offender Website" was required. Because "the only reasonable understanding" of the report was that "someone with Erickson's name was a registered sex offender in Pennsylvania," no reasonable user would be misled.

The court was careful to caution that a CRA cannot "caveat [its] way out of liability" for a clearly misleading report simply by providing a fine-print disclaimer or "vague equivocations." But where the language of the report makes clear what the report is and what it is not, and where it is prepared "consistent with the expectations of the requester," such a report is not misleading.

Key Takeaways

The key message of this decision is that it is not inaccurate for a CRA to report unmatched records — so long as a reasonable user would understand the records are, in fact, unmatched. This decision also provides some potential compliance tips for CRAs seeking to assure "maximum possible accuracy." CRAs can note, for example, the notifications First Advantage gave to the users of its reports, which the court found to be clear.

On the flip side, the decision implies that the argument that a "technically accurate" report can give rise to inaccurate understandings will not pass muster under the FCRA, according to the Eleventh Circuit, if a reasonable user would not be misled.

While the decision appeared to recognize name-only matching as an acceptable, reasonable procedure in certain situations where disclosures are used, those takeaways were tempered by the Consumer Financial Protection Bureau's (CFPB) November 4, 2021 advisory opinion (Opinion). The Opinion explained that a CRA engaged in name-only matching violates Section 1681e(b) of the FCRA. Although styled as an advisory opinion, the Opinion is considered an "interpretive rule" issued under the CFPB's authority to interpret the FCRA. It will be published at 12 C.F.R. Part 1022 and is effective as of the date of publication.

According to the CFPB, "[I]t is not a reasonable procedure to use name-only matching to match information to the consumer who is the subject of the report in preparing a consumer report." The Opinion reasoned that there was a "high risk that name-only matching will result in the inclusion of information that does not pertain to the consumer who is the subject of the report," and there was a relative lack of burden on a CRA to utilize additional identifiers or to simply not include name-only matched information in a consumer report.

The Opinion cited census data regarding the frequency of common names to conclude "it is not unlikely that thousands, or even tens of thousands, of consumers, might share a particular first and last name combination." The Opinion highlighted a potential increased risk of inaccuracy when name-only matching is used for Hispanic, Asian, and Black consumers based on census data, showing less last-name diversity in these populations. The Opinion also indicated that for consumers with common names, even using an additional identifier, such as a date of birth or address, may still allow for a "heightened risk" of inaccuracy because "commonly named individuals might share the same first and last name and date of birth or address." Although many CRAs have moved away from pure name-only matching, the Opinion asserts that some CRAs continue to engage in this practice, and any CRAs that may have been encouraged by the Eleventh Circuit's decision should reconsider procedures that rely on name-only matching.

District Court Grants Summary Judgment for Background Screener for Both Negligent and Willful 1681e(b) Claims Related to Reporting of Outdated Eviction Records

In July 2021, the U.S. District Court for the District of Massachusetts granted summary judgment to a background screening company regarding the reporting of allegedly outdated eviction records. This case, *McIntyre v. RentGrow, Inc.*, No. 18-CV-12141 (D. Mass. 2021), involved a background screening report prepared in connection with the plaintiff's application for housing. That report contained allegedly misleading information given that it did not include subsequent developments in multiple eviction cases reported about the plaintiff, such as dismissals or satisfactions of judgments from those actions.

While the court held there were disputed issues of fact regarding accuracy and reasonable procedures, the court ruled the plaintiff's FCRA claim did not survive summary judgment based on the plaintiff's inability to establish causation (relevant only to actual damages) and willfulness.

Concerning the element of inaccuracy, the court reasoned a jury could find the report contained inaccurate information for each of the eviction cases at issue because the report: (1) did not state where the judgment had been satisfied and paid in full; (2) did not state where a case had been withdrawn and dismissed; and (3) did not state where a judgment had been vacated. Instead, the report listed the plaintiff's various public records with open amounts that "inaccurately suggests that Plaintiff owed money to her former landlords," and/or that the case was still pending. The court further explained "a reasonable jury could find that a screening report that omits that a landlord-tenant case had been withdrawn without prejudice or that a judgment was vacated is materially misleading because it could suggest that a case is still open and pending against a consumer, when, in fact, the opposite is true."

Regarding the element of reasonableness of procedures to assure maximum possible accuracy,

the court reasoned, although it was a close call, that "factual questions exist as to whether Defendant's reliance on [its vendor's] civil court records was reasonable." The court reasoned the defendant was "unaware of the processes [its vendor] uses to obtain and/or update that data," which could lead a jury to find the defendant did not use reasonable procedures to assure maximum possible accuracy.

Turning to damages issues, the court granted summary judgment on the plaintiff's negligence claim because of her failure to show she suffered any actual damages based on the defendant's reporting. The plaintiff argued that the defendant caused the following harms: (1) loss of a rental housing opportunity; (2) loss of time resolving the problems on her screening report; and (3) emotional distress, specifically a loss of sleep. Regarding (1), the court reasoned the housing provider did not deny the plaintiff due to the inaccurate information, rather it denied all applicants with "any housing court history." Relating to (2) and (3), the court stated the plaintiff failed to "put forth sufficient evidence to survive summary judgment." Instead, the plaintiff relied "solely on her own deposition testimony, which is insufficient to withstand summary judgment in this case." Thus, the court held the plaintiff did not sufficiently demonstrate any cognizable actual damages.

Next, the court analyzed the remaining possibility for statutory and punitive damages, which are only available in the case of willful violations of the FCRA, and which would have served as the most likely basis for class certification. The court held the defendant put forth sufficient evidence to show it did not act willfully as a matter of law. Specifically, the defendant testified, prior to this lawsuit, that it "has never been sued by anyone regarding the accuracy of its civil case eviction information and that no federal or state regulator has ever fined, sued, or investigated Defendant regarding its eviction litigation reporting procedures." The defendant also considered its vendor to be the "gold standard" in the public records space. Accordingly, the court stated "there is no evidence that Defendant was on notice that [vendor's] civil court data was inaccurate and then ignored such warnings. The record also demonstrates that once Plaintiff disputed the inaccurate records, the [report] was updated within a month." Thus, the court held that a reasonable jury could not find that the defendant willfully violated the FCRA, such that the plaintiff is not entitled to statutory or punitive damages.

Lastly, because the court granted summary judgment to the defendant, the plaintiff's individual claims were resolved, and the fully briefed motion for class certification was denied as a matter of course without further analysis.

This decision is an important win for background screeners that rely on vendors for certain public record information. However, this decision shows that companies should carefully consider how vendor data is vetted and analyzed.

Arkansas Supreme Court Backs Professional Background Screening Association Against County Clerk

In a case of first impression, the Supreme Court of Arkansas found in favor of Professional Background Screening Association (PBSA) in its suit against Benton County, AR's clerk of court. PBSA requested court records under Arkansas' Freedom of Information Act (FOIA). The request was denied by Clerk of Court Jennifer Jones who claimed that the background screeners' requests for "any and all court records which relate to" a certain individual was a request for "compiled information" under Arkansas Supreme Court Administrative Order Number 19 (Order 19).

Order 19 requires a license agreement and specifical certifications of use for "compiled information," which the order defines as "information that is derived from the selection, aggregation or reformulation of information from more than one court record." After its request was denied, PBSA filed suit and challenged the clerk's interpretation of Order 19. PBSA argued the clerk's interpretation deprived background screeners of their right to access court records under the FOIA. The Arkansas Supreme Court entered summary judgment in favor of PBSA, holding background screeners' record requests are not requests for compiled information for purposes of Order 19 and thus, not subject to access limitations imposed by the clerk of court.

The decision handed down by the Arkansas Supreme Court is a win for background screeners and their customers who rely on public records, such as court records, to make important decisions about consumers in a variety of different areas.

On appeal, the Arkansas Supreme Court noted the case presented an issue of first impression. The Supreme Court also sided with PBSA, holding requests for "all court records" as it pertains to a specific individual are not requests for compiled information. The Supreme Court provided insight into its decision, emphasizing it "liberally construe[s] the FOIA to accomplish its broad and laudable purpose that public business be performed in an open and public manner." The Supreme Court recognized "[t]he process described by Jones that is needed to identify and copy all existing court records relating to a specific person may be tedious and require multiple steps; however, this is not akin to selecting certain information from multiple cases and then aggregating or reformulating that information into a new court record." The Supreme Court also recognized the clerk of court's "antiquated" computer system does not change the nature of the information requested by PBSA or somehow transform existing records into "compiled information" and triggering compliance with Order 19.

The decision handed down by the Arkansas Supreme Court is a win for background screeners and their customers who rely on public records, such as court records, to make important decisions about consumers in a variety of different areas.

Update on State Fair Chance Laws Across the Country

State fair chance and "ban-the-box" laws have seen a significant uptick over the past few years and seem to show no signs of slowing down anytime soon. According to the National Employment Law Project (NELP), as of July 2021, 36 states and more than 150 cities and counties have "ban-the-box" or like laws, including, at a city level, New York City, Austin, Baltimore, Buffalo, Chicago, Los Angeles, Philadelphia, San Francisco, Seattle, and St. Louis.

"Ban the box" is a catch phrase for initiatives that seek to advance employment opportunities for people with prior criminal convictions by eliminating any inquiry into a candidate's criminal history on the job application. This relates to the check box (or question) on a job application that requires the candidate to disclose their criminal history. Many ban-the-box laws require employers to consider the specific nature of a criminal conviction and its impact on the specific job at issue. This may require more customization of an employer's criminal history criteria. In fact, some fair chance laws give the applicant a specific opportunity to address convictions before a decision. Tenant screeners need to ensure any "decision" on an applicant is consistent with these rights.

Local governments, listed below, have passed ordinances, imposing stricter paperwork and reporting requirements on employers and landlords, especially concerning eviction records and criminal history records:

- Seattle: Fair Chance Housing Ordinance, effective May 2020
- Oakland: Fair Chance Housing Ordinance, effective February 2020
- Illinois: Human Rights Act, effective March 2021
- New York City: The Fair Chance Act, amendments effective July 2021
- Maine: Ban the Box, effective October 2021
- New York City: Fair Chance for Housing Act (being considered)

Additionally, states have passed laws shortening the period of time following a criminal conviction or arrest during which such conviction or arrest may be reported.

New York City, Oakland, and Seattle have new laws that may reach background check companies through potential "aiding-and-abetting" liability. An example of aiding and abetting potentially includes making an approval decision based on criminal history by advising an employer to approve or deny an applicant based on a list of conviction histories that the employer wishes to exclude.

A brief background on a few of the state fair chance laws can be found below:

- **New York City:** The Fair Chance Act amendments (effective July 29, 2021) require potential employers to separately request and review noncriminal history of applicants. Background check companies will be asked to separate background reports by criminal and noncriminal information.
- **Seattle:** Fair Chance Housing Ordinance states that it is an unfair practice to consider or require disclosure of criminal history, subject to narrow exceptions, and that landlords may not reject an applicant simply because he is on a sex offender registry without conducting an individualized assessment and providing written notice. This ordinance applies to background screening companies and "any person" who assists in providing prohibited information.
- **Oakland:** Oakland's ordinance takes Seattle's requirements one step further and requires that if an adverse action is taken, the applicant must be given instructions on how to file a complaint with the city, a list of legal service providers, a copy of his criminal history and the basis for the decision, and an opportunity to respond. This ordinance applies aiding-and-abetting liability to nonlandlords, including background screening companies.
- **Illinois:** Illinois' New Substantive Limitations and Procedural Obligations on the Use of Criminal Conviction Records in Employment Decisions took effect on March 23, 2021. The Illinois Human Rights Act (IHRA) protects a person from being discharged, disciplined, denied employment, or denied promotions because of a conviction record without notice and an interactive assessment that must be conducted or provided by certain employers.

Ban-the-box legislation has blossomed in recent years that may impose additional disclosure, notice, timing, and adverse action requirements that may well differ from federal FCRA requirements, posing a significant compliance challenge for employers.

District Court's FCRA Decision Offers Guidance for Employers on "Clear and Conspicuous" Disclosures and Willfulness

After the District Court for the District of Oregon dismissed an FCRA suit filed against Fred Meyer, Inc., the Ninth Circuit Court of Appeals partially reversed, holding Fred Meyer had failed to comply with FCRA's "standalone" requirement by providing an extraneous explanation of the applicant's rights in its background check disclosure — even though the extraneous explanation was in good faith. On remand, the district court granted partial summary judgment to Fred Meyer, holding that (1) Fred Meyer's disclosure notice was "clear and conspicuous" as required under the FCRA, and (2) Fred Meyer's failure to comply with the FCRA's "standalone" requirement was not willful.

In the appeal, the Ninth Circuit examined "as a matter of first impression" what information may be included in a background check disclosure. The court held that beyond a plain statement, disclosing a consumer report may be obtained for employment purposes, and the disclosure also may include a concise explanation of what a consumer report is, how it will be obtained, and the type of employment purposes for which it may be used. The court held additional information regarding a consumer's rights under federal and state law — although likely included by Fred Meyer in good faith — was extraneous. The court remanded to the District of Oregon to determine whether the "remaining language" of the disclosure was "clear and conspicuous."

On remand, the district court held Fred Meyer's disclosure was clear and conspicuous because it was reasonably understandable and noticeable to the consumer. On the question of willfulness, the court held Fred Meyer's failure to comply with the FCRA's "standalone" requirement was not willful. The court noted the Ninth Circuit had stated it was addressing an issue of first impression, and therefore, Fred Meyer's disclosure was not based

on an "objectively unreasonable" interpretation of the FCRA at the time the plaintiff had applied for his position. Further, although the Ninth Circuit held the extraneous information regarding plaintiff's legal rights should have been provided in a separate document, it noted that the information appeared to have been included "in good faith." Accordingly, the violation was not willful.

Although Fred Meyer succeeded in demonstrating that its noncompliance in this case was not willful, employers utilizing background screenings should note that the Ninth Circuit's decisions in *Gilberg* and *Walker* now provide notice that strict compliance with the FCRA's standalone requirement is vitally important.

COVID-19 Regulations Affecting the Tenant Screening Industry

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was signed into law on March 27, 2020, and provided $500 billion in direct payments to Americans, $208 billion in loans to major industry, and $300 billion in Small Business Administration loans. The CARES Act also added credit reporting requirements related to borrowers receiving assistance due to COVID-19. In particular, if a data furnisher has granted an "accommodation" (*i.e.*, forbearance, partial payment, modification, etc.) as a result of COVID-19, the data furnisher must report the account as follows:

- If the account was current before the accommodation, the account is still reported as current (Account Status Code 11).
- If the account was delinquent before the accommodation, the account should be reported as delinquent.

The CFPB modified some of its enforcement policies due to the pandemic — at least initially. On April 1, 2020, the CFPB issued a statement that it would consider the individual circumstances of each CRA or furnisher in determining compliance with the FCRA, particularly for smaller or less sophisticated lenders. This change suggested a less-than-strict approach to the 30-day reinvestigation deadline. However, on June 16, 2020, the CFPB rescinded the portion of the statement that suggested it would be flexible in enforcing compliance with the FCRA. It stated it believed "consumer reporting agencies and furnishers have had sufficient time to adapt to the pandemic and should be able to regularly meet their obligations under FCRA … ."

The CFPB's April 1, 2020 statement was met with criticism from consumer advocates and state attorneys general, which issued a statement stating, "Consumers and CRAs should know that even if CFPB refuses to act, our states will continue to enforce the FCRA's deadlines against companies that fail to comply with the law."

In response to the pandemic, several states enacted their own legislation pertaining to tenant screening. For example:

- **New York:** Former Governor Andrew Cuomo signed legislation extending protections prohibiting evictions, foreclosure proceedings, and negative credit reporting related to the COVID-19 pandemic until August 31, 2021. These protections were extended to January 15, 2022.
- **California:** California also extended its consumer relief protections, including an eviction moratorium, until September 30, 2021; notice requirements and waiting periods for federal and private forbearance denials until December 1, 2021; and no negative credit reporting for borrowers taking advantage of this relief. Beginning November 1, 2021, landlords may sue tenants for any unpaid rent owed.
- **Oregon:** The Oregon Legislature passed a law prohibiting landlords from reporting nonpayment of rent, charges, and fees accrued from April 1, 2020, through June 30, 2021, to a CRA. The law also prohibits landlords from considering eviction actions arising from April 1, 2020, through February 28, 2022, or unpaid rent accrued from April 1, 2020, through February 28, 2022, when screening tenants.
- **Pennsylvania:** Pennsylvania enacted the PA CARE Package, which requires financial institutions and banks to offer additional assistance to Pennsylvanians facing financial hardship due to impacts of the COVID-19 pandemic. This includes:
    - Expansion of small and medium business loan availability;
    - 90-day grace period for mortgages (at least);
    - 90-day grace period for other consumer loans, such as auto loans;
    - 90-day window for relief from fees and charges, such as late and overdraft fees;
    - Foreclosure, eviction, or motor vehicle repossession moratorium for 60 days; and
    - No adverse credit reporting for accessing relief on consumer loans.

On July 1, 2021, the CFPB released an FCRA Tenant Screening Enforcement Compliance Bulletin, outlining its enforcement focus areas as the country transitions to a post-pandemic rental market. The CFPB stated that it "intends to look carefully at the accuracy and dispute-handling practices of [CRAs] that report rental information, including whether their procedures to match information to consumers are reasonable; whether they report eviction information that is inaccurate, incomplete, or misleading (such as may result from a failure to have reasonable procedures to report information about the disposition of an eviction filing, to prevent the inclusion of multiple entries for the same eviction action in the same consumer report, or to prevent the inclusion of eviction information that has been sealed or expunged); and whether they conduct timely and reasonable investigations of consumer disputes[.]"

While these concerns may not be directly related to the COVID-19 pandemic, they may reflect concerns about how the pandemic disproportionately affected certain minority groups.

BANKRUPTCY

Supreme Court Holds Retaining Property After Bankruptcy Does Not Violate Automatic Stay

On January 14, 2021, the U.S. Supreme Court decided *Chicago v. Fulton*, holding that mere retention of a debtor's property after the filing of a bankruptcy petition does not violate the automatic stay provided by §362(a) of the Bankruptcy Code.

The City of Chicago impounded respondents' vehicles for failure to pay fines for motor vehicle infractions. After their vehicles were impounded, each respondent filed a Chapter 13 bankruptcy petition and requested the return of their vehicle. The city refused, and the bankruptcy court in each case found the city's retention of the vehicle violated the automatic stay. The Court of Appeals for the Seventh Circuit affirmed, holding that by retaining the vehicles after each respondent had declared bankruptcy, the city had "exercised control" over respondents' property in violation of §362(a)(3).

The Supreme Court vacated the judgment and held that "merely retaining possession of estate property does not violate the automatic stay." The Court observed that the Bankruptcy Code suggests that "§362(a)(3) prohibits affirmative acts that would disturb the status quo of estate property as of the time when the bankruptcy petition was filed."

In doing so, the Court concluded that any ambiguity in the text of §362(a)(3) was "resolved decidedly" by §542, which requires the turnover of estate property to the trustee and carves out certain exceptions to the turnover obligation. The Court reasoned that if §362(a)(3) prohibited the passive retention of property, it would generate two problems within the Bankruptcy Code. That construction would (1) render §542 superfluous because all estate property would be required to be turned over to the debtor immediately upon the filing of the petition under §362(a)(3), and (2) generate conflicting commands because §542 specifically excuses some turnovers of property while §362(a)(3) would require immediate turnover of all of the debtor's property.

The Court expressly declined to address how the turnover obligation in §542 operates or the meaning of other subsections of §362(a). The Supreme Court remanded the case for further proceedings consistent with the opinion.

Although offering a meaningful protection to creditors, the *Fulton* decision is very narrow, limited to a creditor's passive possession of a debtor's property. *Fulton* does not seem to protect creditors who are in the process of acquiring possession of a debtor's property when the petition is filed, as opposed to those who have already taken possession.

For the creditor that has already taken possession of its collateral (whether it be a debtor's car, construction equipment, or some other property), *Fulton* offers some substantial benefits. Most notably, *Fulton* makes clear that this category of creditor does not violate the automatic stay (and risk sanctions) by simply retaining property it acquired before the bankruptcy filing.

No Standardization of the Definition of "Undue Hardship" Yet

In 2021, the U.S. Supreme Court declined to wade into the waters of what, exactly, is an "undue hardship" that would allow a debtor to discharge student loans under 11 U.S.C. § 523(a)(8). By denying a debtor's petition for a writ of certiorari from the U.S. Court of Appeals for the Fifth Circuit, the Court avoided an opportunity to establish uniformity of how to determine an issue that, given the ever-increasing number of individuals who have student loans and who are filing protection under the Bankruptcy Code, is unlikely to fade into obscurity. The petitioner argued in its brief that its case "present[ed] an ideal vehicle to resolve the conflict" between jurisdictions. *McCoy v. United States*, No. 20-886, cert. denied, 2021 WL 2519103 (U.S. June 21, 2021).

The Bankruptcy Code states that a discharge under 11 U.S.C. §§ 727, 1141, 1192, 1228(a), 1228(b), or

1328(b) does not generally discharge a debtor from student loan debt. 11 U.S.C. § 523(a)(8). However, an exception to that exception is that student loans are dischargeable in situations where "excepting such debt from discharge under this paragraph would impose an undue hardship on the debtor and the debtor's dependents." *Id.*

Since set forth by the Second Circuit in *Brunner v. New York State Higher Education Services Corp.*, 831 F.2d 395, 396 (2d Cir. 1987), most courts have adopted a three-part test to determine what amounts to an "undue hardship" under the Bankruptcy Code. Under *Brunner*, to evince an "undue hardship" and obtain a discharge of one's student loans, the debtor must show: "(1) that the debtor cannot maintain, based on current income and expenses, a 'minimal' standard of living for herself and her dependents if forced to repay the loans; (2) that additional circumstances exist indicating that this state of affairs is likely to persist for a significant portion of the repayment period of the student loans; and (3) that the debtor has made good faith efforts to repay the loans." *Brunner, supra*, 831 F.2d at 396. Pursuant to *Brunner*, unless all three elements are satisfied, a Bankruptcy Court jurisdiction has no option but to deny a debtor's request for discharge as to its student loans.

However, not all circuits have taken a uniform approach in applying *Brunner*. In fact, the Eighth Circuit has rejected *Brunner*, and courts in the Eighth Circuit are required to consider the "totality of the circumstances" in each individual debtor's case; not just mechanically applying the three *Brunner* elements. *See Andrews v. South Dakota Student Loan Assistance Corp. (In re Andrews)*, 661 F.2d 702, 704 (8th Cir. 1981). Under this approach, "fairness and equity require each undue hardship case to be examined on the unique facts and circumstances that surround the particular bankruptcy." *Long v. Educ.Credit Mgmt. Corp. (In re Long)*, 322 F.3d 549, 554 (8th Cir. 2003). The Eighth Circuit distilled its analysis of the dischargeability of student loans in *Long* by setting forth the following standard: "if the debtor's reasonable future financial resources will sufficiently cover payment of the student loan debt-while still allowing for a minimal standard of living-then the debt should not be discharged." *Id.* at 554-55.

Predicated on this split of authority between, on one hand, most circuits—including the Fifth Circuit where the petitioner was located—that follow *Brunner* and, on the other, the Eighth Circuit that adheres to the *Andrews* standard, a debtor requested the Supreme Court weigh in on the question.

As explained, *supra*, the *Brunner* and *Andrews* approaches conflict with each other, often resulting in vastly different outcomes regarding dischargeability solely depending on the analysis used against the same set of facts. The totality of the circumstances set forth in *Andrews* and reaffirmed in *Long* allows a court to embrace "a less restrictive approach" to undue hardship than the strict parameters set forth in *Brunner*. *Long, supra*, 322 F.3d at 554. For instance, the *Brunner* test is done based solely on a debtor's "current income and expenses" regardless of whether the debtor's age, disability, or other mental and physical limitations would otherwise make repayment an "undue hardship." With the Eighth Circuit's "totality of the circumstances" in mind, a debtor's age, potential disabilities, and exhaustive job search may be considered to determine if exclusion of student loans from a debtor's discharge presents an "undue hardship." *McCoy, supra*, Brief for Petitioner at 3.

Ultimately, the Supreme Court did not act on the *McCoy* petition, leaving in place, for the time being, the divergent analyses of "undue hardship" in place. However, given the fact that more than 45 million people in the United States have student loans, it is highly likely that another debtor will attempt to have the Supreme Court weigh in on the appropriate standard to use when determining "undue hardship" as set forth in the Bankruptcy Code.

Inaccurate Credit Report Didn't Violate Discharge

A debtor cannot hold a creditor in contempt for violating a discharge injunction based on inaccurate credit report information that later damaged her credit score and prevented her from getting a loan, a Pittsburgh bankruptcy judge has ruled. *In re Minech*, No. 18-21030, 2021 WL 4071875 (Bankr. W.D. Pa. Sept. 7, 2021).

Judge Gregory L. Taddonio of the Western District of Pennsylvania denied Amanda Minech's motion

for contempt, finding that she failed to show that Clearview Federal Credit Union's (Clearview) misreporting of her debt information amounted to coercion.

Minech filed for Chapter 7 relief in March 2018. Four months later, after she failed to reaffirm the two debts she owed to Clearview from her credit card and an auto loan, the court granted her a discharge. Minech applied for a Federal Housing Administration (FHA) loan in July 2020 and discovered that her credit report reflected a debt with Clearview as "charged off." Minech disputed the report and contended that her credit score dropped 26 points because of the adverse report on the unsecured loan. The reinvestigation results revealed that Clearview had verified the accuracy of the information reported, but reduced the past due amount from $1,078 to $634 (as reflected in the credit report). Therefore, failing to resolve the discrepancy on her own, Minech returned to her bankruptcy attorney, who sent a letter demanding that Clearview instruct all credit reporting agencies to remove the adverse report.

When Minech's counsel did not receive a response from Clearview after 20 days, she filed the motion to reopen and the motion for contempt, arguing that Clearview willfully violated the discharge injunction by improperly reporting the unsecured loan as a "charge-off" rather than discharged in bankruptcy under Section 524(a)(2) of the Bankruptcy Code. She further alleged that her credit score dropped below the level needed to qualify for an FHA mortgage loan violated the discharge injunction.

Notably, Section 524(a)(2) says a bankruptcy discharge operates as an injunction against a creditor's act "to collect … any … debt" that has been discharged. Missing from the motion for contempt was any assertion that the adverse report was an act to collect a debt. Also absent was an allegation that Clearview refused to correct the adverse report. In response, Clearview admitted the error and the correction of it, but denied attempting to collect on a debt in violation of the discharge. Clearview also stated that it promptly corrected the report once the demand letter was received from Minech's counsel.

The court acknowledged there is universal agreement that credit reporting can constitute an act to collect a debt. However, to show that a creditor is attempting to collect on a debt through the act of reporting on credit requires evidence to objectively connect the reporting to a collection activity.

The court acknowledged there is universal agreement that credit reporting can constitute an act to collect a debt. However, to show that a creditor is attempting to collect on a debt through the act of reporting on credit requires evidence to objectively connect the reporting to a collection activity. Similarly, a refusal to change a knowingly inaccurate report may suggest that the creditor is seeking to collect a debt.

Here, Judge Taddonio found that the motion for contempt did not draw an "effective connection" between the inaccurate credit report and collecting the underlying debt. The court observed that while it is inaccurate to report discharged debt as "charged off," such a notation literally means that the debt was written off as uncollectable by the creditor. Therefore, it facially signals an end to active collection efforts by that creditor. As such, Minech needed to point to something more substantial to suggest objectively improper coercion. However, Minech conceded that there was nothing else to her claim beyond the credit reporting itself. Accordingly, the court found that Minech did not sustain her burden to state a plausible claim for relief under section 524(a)(2).

CONSUMER CLASS ACTIONS

Watch for Class Actions in States Without Article III Standing Equivalents

In 2021, litigators took heed of the Supreme Court's loud and clear proclamation on Article III standing in *Ramirez*: "No concrete harm, no standing." Litigators bringing and defending class actions in federal courts must carefully assess whether the plaintiffs adequately allege and prove their injuries. But for litigators in state courts, the issue is not so clear.

State courts do not have the same "case or controversy" requirement as federal courts — they are free to set their own standing requirements. *See ASARCO Inc. v. Kadish*, 490 U.S. 605, 617 (1989). Unsurprisingly, states have adopted an array of standing requirements, with only about half imposing a standing limitation equivalent to Article III. Georgia and Massachusetts are two examples. Other states, like California, Pennsylvania, and Virginia, have broader jurisdiction than Article III and allow actions to proceed where federal courts would dismiss for a lack of standing.

In 2022 and beyond, state courts may become safer forums for class actions, particularly those based on statutory violations where plaintiffs have difficulty alleging concrete injuries. Where cases would fail Article III standing challenges in federal courts, plaintiffs will likely pivot to state courts with broader jurisdictional nets. Indeed, as Justice Thomas recognized in his dissent in *Ramirez*, the decision cemented a growing paradox: In some cases, "state courts will exercise exclusive jurisdiction" over class actions based on federal statutes.

Considering plaintiffs' attraction to state courts, defendants must carefully weigh the consequences of winning standing arguments in federal class actions. A dismissal based on Article III standing could end a case, or it could encourage the plaintiffs to re-file the action in state court and prevent the defendants from removing to federal court. After *Ramirez*, every class action litigator must be aware of both federal and state court implications for their cases.

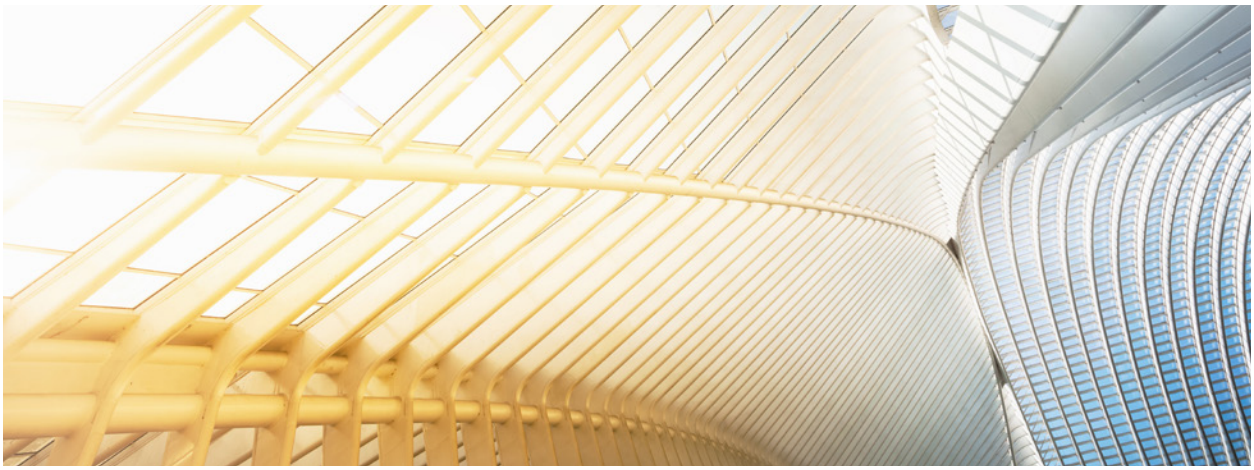
A Closer Look at Administrative Logistics in Class Actions

The Eleventh Circuit Joined the Majority in Holding Administrative Feasibility Is Not a Standalone Requirement for Rule 23 Certification

Over the last nine years, federal circuit courts have cemented a split over how a named plaintiff must demonstrate the ascertainability of class members under Rule 23. In particular, the circuits disagree about whether the plaintiff must provide an "administratively feasible" method of class member identification to have the class certified. Of the 10 circuits weighing in, the First, Third, and Fourth circuits require proof of administratively feasible identification as an element for class certification. The Second, Fifth, Sixth, Seventh, Eighth, and Ninth circuits do not. In 2021, the Eleventh Circuit weighed in and sided with the latter group.

In 2021, in *Cherry v. Dometic Corp.*, an Eleventh Circuit panel held that, when addressing a motion for class certification, courts may consider whether the named plaintiff has demonstrated an administratively feasible method for identifying absent class members, but administrative feasibility is not a standalone requirement for certification. In the district court, the main issue on class certification was whether the proposed class was ascertainable. The class representatives framed ascertainability as an issue of class definition. They argued the proposed class was ascertainable because "the class definition relies exclusively on objective criteria," and identification would be administratively feasible. The defendant argued that the plaintiffs had to prove administrative feasibility to establish ascertainability, which the class representatives failed to do because they provided no evidence of a "workable" identification method. The district court agreed with the defendant and denied class certification.

The Eleventh Circuit vacated that decision. The panel began its analysis by addressing other circuit



holdings on the role of administrative feasibility. The panel noted the Third Circuit applies a heightened standard, which requires, as part of the ascertainability analysis, proof that identification of class members will be "a manageable process that does not require much, if any, individual factual inquiry." The First and Fourth circuits also follow this approach, while the Second, Fifth, Sixth, Seventh, Eighth, and Ninth circuits look at administrative feasibility as part of a greater multifactor analysis, but not an independent requirement.

Given the split in circuit authority, the court turned to the plain text of Rule 23(a) and (b), noting at the outset that "ascertainability" does not appear anywhere in the rule. Nevertheless, following Eleventh Circuit precedent, the panel explained that requiring a class to be "adequately defined and clearly ascertainable" before certification is "implicit" in the rule. As for whether ascertainability is administratively feasible, however, the panel concluded such a requirement follows from neither Rule 23(a) nor Rule 23(b).

The Eleventh Circuit panel concluded "administrative feasibility does not follow from the text of Rule 23(a)" because this quality "does not bear on the ability of a district court to consider the enumerated elements of that subsection." That is, administrative feasibility cannot be required for Rule 23(a) class certification because it is irrelevant to the Rule 23(a) benchmarks: the impracticability of joining all class members, the presence of common questions of law or fact, the typicality of the claims or defenses of the named plaintiffs, and the ability of the named plaintiffs to adequately represent the class. The Eleventh Circuit also held that administrative feasibility did not follow from the text of Rule 23(b). Therefore, it is not a standalone requirement for either type of class certification under Rule 23. Nonetheless, feasibility remains relevant in the Eleventh Circuit because Rule 23(b) includes a balancing test to assess the manageability of the class. Rule 23(b) class plaintiffs must demonstrate that certifying the class as defined will not be thwarted by the "difficulties in managing a class action," like the inability to feasibly identify class members.

Only the Tenth and D.C. circuits have yet to weigh in on the administrative feasibility issue. And unless and until the Supreme Court decides the issue, class-action practitioners should include this issue in strategic decisions about forum transfer and class certification arguments. In courts within circuits with an administrative feasibility requirement, for example, defense counsel should consider emphasizing that administrative difficulties in identifying class members would prohibit ascertainability of the class under Rule 23(a). In other courts, defense counsel should consider arguing that a class cannot be managed and certified under Rule 23(b). And in this latter set of courts — the majority — plaintiffs' counsel may tend to emphasize that administrative feasibility is no bar to Rule 23(a) or Rule 23(b) certification.

While the likelihood of Supreme Court intervention is unclear, administrative feasibility will continue to play a part in class certification battles in 2022 and beyond.

The Eighth Circuit Vacated Certification Because a Technological Means of Conducting Individualized Inquiries Cannot Eliminate the Predominance Requirement

As in *Cherry*, the Eighth Circuit in 2021 examined a logistical issue unique to class actions: If technology can alleviate the burden of conducting individualized inquiries, can a class be certified? The Eighth Circuit answered "no."

The plaintiff in *Ford* sued a brokerage firm for securities violations. In its business, the defendant received stock trade orders from clients and routed those trades to other venues, such as stock exchanges, where the trades occurred. The plaintiff alleged the defendant violated the "duty of best execution" as to the class members' trades, meaning the defendant failed to "use reasonable efforts to maximize the economic benefit to the client in each transaction." The defendant allegedly left stock trade orders unfilled, filled orders at suboptimal prices, or otherwise filled orders in ways that diminished the clients' returns on their requested trades.

At class certification, the defendant argued the proposed class did not satisfy Rule 23(b)(3) because each class member's damages depended heavily on individualized inquiries. Those inquiries included the state of the market at the time of each trade, the value each class member received for his/her trade, and the value the class member could have received had the defendant routed the trade properly. While the magistrate judge recommended denying certification because the damages were individualized, the district judge disagreed and certified the class. The district judge relied on an algorithm proffered by the plaintiff's expert, which could alleviate the burden of individualized inquiries by comparing "hundreds of millions of data points" to calculate each class member's economic loss.

On appeal, the Eighth Circuit panel reversed the district court's certification decision, holding that certifying the class would violate the prohibition on predominantly individualized inquiries, in at least three ways.

First, while the plaintiff's algorithm would compare every trade by every class member to the National Best Bid and Offer (NBBO) price for that trade — the highest acceptable buyer price and lowest acceptable seller price for the given stock at a given time — the trades could have garnered a lower price absent any fault by the defendant. The plaintiff's algorithm thus could not solve the inherent causation proof problem.

Second, certifying the class would require weighing every trade by every class member in light of unusual market conditions at thousands of different times — the quintessential individualized inquiry.

Third, each individual broker's strategy in filling trade orders would also figure into the return every class member made on every trade. Whether a class member's particular trade was executed at a proper price depended on circumstances of the execution of the trade, such as when an NBBO price could not be achieved because fewer shares were available at that price than the number of shares the class member ordered. Compliance with the brokerage firm's duty of best execution thus did not guarantee that the customer would get the best possible deal on a trade; human discretion was involved.

Reviewing these numerous individualized inquiries in light of Rule 23(b)(3) requirements, the Eighth Circuit concluded that the class members' damages were unquantifiable using a common algorithm, and the class could not be certified.

Class action attorneys, especially those seeking to leverage technology in their day-to-day practices, should take note of the Eighth Circuit's message in *Ford*: While a technological solution can "expedite [an individualized] determination, … it cannot change its underlying nature by converting individual evidence into common evidence." Technology may change, but Rule 23's stringent requirements remain.

2021 Developments in Data Breach Class Actions and Multidistrict Litigation

As data breach incidents continue to grow, so does class-action litigation stemming from those incidents. Historically, most data breach class actions settle before the parties litigate class certification. However, in 2021, we saw some key

decisions that litigators should know about when litigating data breach claims in either a class action or multidistrict litigation (MDL).

The Judicial Panel Sets Limitations for Consolidation of Data Breach Cases

For many data breach class actions, a decisive threshold issue is whether to consolidate the cases into a MDL. The MDL process permits centralization of related disputes in front of a single federal court and is designed to promote consistency and efficiency by resolving similar claims and disputes in front of one judge. However, in 2021, the Judicial Panel for Multidistrict Litigation (JPML) appears to have set a size threshold for data breach MDLs when it denied Geico's attempt to consolidate five class-action lawsuits.

In April 2021, Geico suffered a data breach that reportedly impacted over 132,000 individuals. Geico determined that approximately 85% of those individuals lived in New York. In response to the breach, the plaintiffs filed five putative class-action lawsuits in New York (three lawsuits), Maryland (one lawsuit), and California (one lawsuit). In June 2021, Geico attempted to consolidate the class actions into an MDL, arguing that each of the five cases shared the same factual basis and common legal issues.

The JPML denied Geico's motion because "centralization [was] not necessary for the convenience of the parties and witnesses or to further the just and efficient conduct of [the] litigation." While the JPML found that the five cases share common questions of fact, the JPML held that Geico failed to meet its burden that centralization was appropriate because "informal coordination among the small number of parties appear[ed] eminently feasible."

Court Stays Discovery in Data Breach MDL to Allow Issue of Standing to Be Resolved

A district court judge in the Southern District of Florida paused a data breach MDL to allow the court to decide the defendant's motion to dismiss for lack of standing and failure to plead a cognizable claim. In *In Re Mednax Services*, a health care provider defendant suffered a data breach that exposed patient information of approximately 1.3 million individuals. The plaintiffs claim that the defendants' insufficient cybersecurity procedures caused the breach, and the defendant's inadequate response to the breach resulted in additional harm to the plaintiffs.

In August 2021, the plaintiffs combined all claims into one consolidated complaint. The defendants then moved to dismiss all of the plaintiff's claims under Rule 12(b)(1) for lack of standing and Rule

As data breach incidents continue to grow, so does class-action litigation stemming from those incidents.

12(b)(6) for failure to state a claim. The defendants simultaneously moved to stay discovery. The defendants argued that, under Eleventh Circuit law, discovery should be stayed when a defendant makes a facial challenge to the allegations set forth in the complaint to promote judicial efficiency, and such a stay would not prejudice the plaintiffs. In opposition, the plaintiffs argued that stays of discovery are the exception, not the rule, and that class members continue to face increasing risk from the defendant's allegedly deficient cybersecurity procedures.

In granting the stay, the court found that "significant questions exist[ed] regarding Article III's injury-in-fact and traceability requirement." And if the defendants succeeded on the motion to dismiss, "it would substantially impact the viability of claims against one or more [d]efendants and drastically alter the scope of discovery." For these reasons, the court stayed discovery, explaining that the defendants "should not be forced to expend substantial resources responding to discovery given the jurisdictional and facial challenges pending before the [c]ourt."

Individual Issues Concerning Causation and Damages Continue to Present a Hurdle to Class Certification in Data Breach Class Actions

Class certification has only been litigated in a small portion of the filed data breach class actions. However, a common theme in data breach class certification decisions is that the individual issues of causation and damages predominate over the common issues of whether the defendant's cybersecurity procedures or breach notification efforts were deficient. The January 2021 decision in *McGlenn v. Driveline Retail Merchandising, Inc.* was no exception.

There, a district court judge declined to certify a class of employees whose personal information was disclosed when Driveline fell prey to a phishing scam. In January 2017, a scammer — posing as Driveline's CFO — asked a payroll employee to email him 2016 W-2s for all of Driveline's employees. In response, the payroll employee emailed him 15,878 W-2 forms, all of which contained employees' names, addresses, Social Security numbers, and wage information. A former Driveline employee, plaintiff Lynn McGlenn, filed a class action against Driveline, alleging that the breach caused her personal information to be stolen and used to open a fraudulent credit card account. In her class certification motion, McGlenn sought to certify a class of "all current and former Driveline employees" whose personal information was compromised by the scam.

The court denied McGlenn's motion for class certification, finding that establishing the required elements of causation and damages required individualized evidence, and thus, McGlenn failed to satisfy Rule 23's requirements of commonality and predominance. The court explained that McGlenn could not prove causation with common evidence because "several Driveline employees likely had been involved in other data incidents in the two to four years prior to" the phishing scam. Moreover, even employees who could tie their alleged injury to the phishing scam would encounter a significant legal hurdle because the applicable law (Illinois) did not impose a common law duty on Driveline to safeguard information. The court further held that the class members' alleged "risk of harm" was not sufficient to establish Article III standing.

CONSUMER CREDIT REPORTING

COVID-19, the CARES Act, and Post-Accommodation Reporting Guidance

Last year, we wrote about how COVID-19 had permeated all aspects of life and business, including credit reporting. Unfortunately, that did not change in 2021.

The credit reporting rules added to the Fair Credit Reporting Act (FCRA) by the CARES Act remain in full force, as President Biden extended the national emergency declaration until at least February 24, 2022.[4] As a result, accounts that have received an "accommodation" must be reported in accordance with the CARES Act amendments to the FCRA.[5] We wrote about the requirements of the CARES Act amendments in last year's review, as well as the Consumer Data Industry Association's (CDIA) guidance for putting those rules into practice.[6]

While the CARES Act amendments are still in force and the CDIA's guidance for reporting during an accommodation remains in place, post-accommodation reporting has taken center stage as many of the forbearances provided by the CARES Act have ended or will end in 2022. Recognizing the shift, the CDIA has provided guidance for post-accommodation reporting, including guidance for loans that are backed by Fannie Mae and Freddie Mac. As we predicted in last year's review, the amendments to the FCRA have spurred litigation by consumers seeking to enforce the reporting requirements added by the CARES Act. The CDIA's post-accommodation guidance and the new wave of litigation are discussed further below.

CDIA Post-Accommodation Guidance

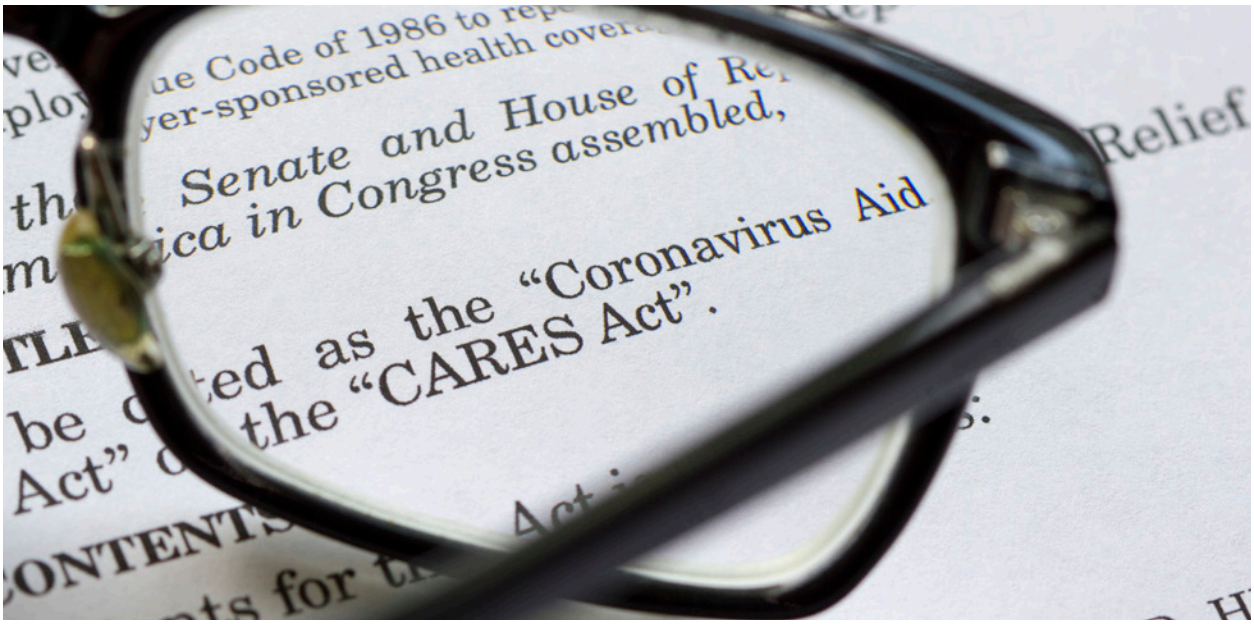
As we noted in last year's review, as is often the case with statutory amendments, the CARES Act did not provide explicit instruction to data furnishers on what Metro II codes to use when reporting accommodations under the FCRA amendments. The same is true for post-accommodation credit reporting – the statute itself provides little practical guidance. That is where the CDIA is intended to fill the gap.

One general principle guides all post-accommodation reporting: the existence of an accommodation cannot result in derogatory reporting after it has ended. For example, accounts that were current when an accommodation began must be reported as current during the accommodation period even after the accommodation ends. Accounts that were delinquent when an accommodation period began must be reported at the same level of delinquency after the accommodation period ends. In other words, furnishers cannot advance the delinquency once the accommodation period is over. Of course, delinquent accounts that were brought current or paid off during an accommodation period should be reported as such. Once an account has been initially reported post-accommodation, normal Metro II standards apply to the reporting.

For mortgages backed by Fannie Mae or Freddie Mac, the CDIA provides additional guidance. In particular, the CDIA's guidance focuses on how to report changes to the loan as a result of the accommodation, such as when the loan enters a short-term repayment plan, payment deferral, or loan modification. Unlike some private institutions, Fannie Mae and Freddie Mac provided defined repayment options for borrowers who took advantage of CARES Act forbearances. Of note, the CDIA advises that the accommodation period payment history profile should never be updated after the accommodation period ends.

Looking Forward

[4] The "covered period" under which the rules apply runs from January 31, 2020 until 120 days after the national emergency regarding COVID-19 is lifted.
[5] See 15 U.S.C. § 1681s-2(a)(1)(F).
[6] See 2020 Consumer Financial Services Year in Review, pp. 27-28.



As we mentioned in last year's review, despite the amendments to Section 1681s-2(a) under the CARES Act, there was no corresponding amendment to Section 1681s-2(b). Despite the affirmative "shall" report language, there is no private right of action under the FCRA for consumers to sue data furnishers for the affirmative act of reporting information that does not comply with the CARES Act amendments to the FCRA. Nonetheless, 2021 has seen an uptick in litigation and regulatory activity that seeks to hold data furnishers (as well as CRAs) accountable for how they report loans that received an accommodation under the CARES Act. With the COVID-19 pandemic still ongoing and many loans just recently coming out of accommodations, it's likely this trend of litigation and regulatory scrutiny will continue.

Litigation Updates

Furnishers

2021 saw a continuation of many of the same claims that were permeating through the courts in 2020. In particular, the plaintiffs' bar continues to pursue three types of cases under the FCRA in high-volume filings, with mixed results: (i) Pay Status cases; (ii) account no longer in dispute cases; and (iii) Scheduled Monthly Payment after account closure cases.

Pay Status Cases

In last year's review, we noted an emerging trend of cases concerning the reporting of a delinquent "pay status" on accounts that were delinquent when they were closed. There was no slowdown on these cases in 2021.

The common fact pattern for these cases involves a delinquent account that is paid off when the account is in a delinquent status. As a result, the data furnisher reports the current status as Account Status 13: Paid or closed account/zero balance. The CDIA's Credit Reporting Resource Guide (CRRG) also advises that the furnisher report a payment rating, which denotes the level of delinquency (if any) immediately before the current status of paid and closed. The purpose behind this is to provide a holistic picture of an account because, while it is now paid off, it was delinquent before that payoff.

Another common factual scenario is where an account has been transferred rather than paid off. In those circumstances, the resulting reporting is similar – the furnisher reports an Account Status 5: Account transferred, and then reports a payment rating reflecting any delinquency on the account that existed before the transfer.

Under both scenarios, consumers claim in the subsequent credit disputes and litigation that the "current account status" shows their account as delinquent when it has been paid in full or transferred (i.e., no money is owed the furnisher of

the information). There have been varying results over the past year in these cases.

For example, the U.S. District Court for the District of New Jersey found that where a payment rating denotes the historical delinquency on a transferred account that otherwise indicates no money is owed, there is no inaccuracy in the reporting as a matter of law. *See Salvador v. Fedloan Servicing*, Civ. No. 20-20568, 2021 U.S. Dist. LEXIS 208554 (D. N.J. Oct. 28, 2021). However, in *Salvador*, the court's reasoning suggests that it is the fact that the account was transferred rather than being paid off that meant the delinquent payment rating was not inaccurate. *See id.* at *17 (finding no factual allegation that plaintiff paid off the overdue loan before it was transferred).

Other courts emphasize a holistic approach when considering the accuracy of the reporting. In *Lacy v. TransUnion, LLC et al.*, Case No. 8:21-cv-519 (M.D. Fla. July 12, 2021), the consumer's mortgage was foreclosed upon and written off. In subsequent reporting, the tradeline denoted the foreclosure and zero balance, but also included a payment rating indicating the account was 120 days delinquent just before it reached zero balance status. In dismissing the consumer's claims, the court noted that no reasonable creditor could be misled into believing that plaintiff was "still late" – emphasizing that the credit report must be viewed in its entirety, and not just with respect to a single data field.

Still, some courts have found that the issue of whether "historical" reporting of a delinquency on an account that has been paid off is a question of fact for a jury to decide. For example, in *Smith v. TransUnion, LLC et al*., Case No. 20-4903 (E.D. Pa. Mar. 19, 2021), the court denied a motion for summary judgment, holding that it could not find as a matter of law that reporting a delinquency through the payment status on an account that had been paid in full was accurate and not misleading.

While many of the decisions affirm the trend of recognizing the reporting of delinquent payment ratings as historically accurate, non-misleading information, adverse decisions have increased the likelihood that similar claims will continue. As demonstrated above, some courts are distinguishing between reporting a delinquent payment rating on loans that have been paid in full versus loans that have been transferred. This trend will be particularly important to follow, because the CRRG does not draw any such distinction when it comes to the reporting of payment ratings.

Accounts No Longer in Dispute

Another continuing trend is lawsuits involving previously disputed accounts that the consumer claims are no longer disputed. In these cases, the consumer previously disputed the account through a CRA and/or furnisher. Following the requirements of Section 1681s-2(a)(3) of the FCRA, the furnisher then reports the account as disputed with an appropriate Compliance Condition Code. Subsequently, the consumer decides (and sometimes) notifies either the CRA and/or the furnisher that they no longer dispute the account/reporting. The consumer then files a lawsuit alleging that the account is inaccurately being reported as being in dispute.

Over the past year, courts have continued to dispose of many of these cases. In particular, courts have continued to reject the argument that a dispute through a CRA notifying it that the consumer no longer disputes an account is not sufficient to require a furnisher to remove a prior dispute notation where there was no direct notice to the furnisher. *See, e.g., Griffin v. Equifax Info Servs., LLC et al.*, No. 1:20-cv-2316 (N.D. Ga. Jan. 25, 2021) ("Simply put, the [furnisher's] investigation [of a dispute from a credit reporting agency under Section 1681s-2(b)] would have to turn up something more than the request from Plaintiff herself [to the credit reporting agency]."). The logic behind these decisions makes sense, because without more, a furnisher's investigation into such a dispute would turn up nothing regarding the consumer's position over the prior dispute other than the present one. This situation also presents a paradoxical situation where the account is being disputed about not being disputed, which raises the question of whether the furnisher should report the account as disputed *again*.

The "no longer in dispute" theory has also failed to gain traction with the federal appellate courts. Just recently, the Eleventh Circuit affirmed the dismissal of a case where the plaintiff failed to inform the data

furnisher that she no longer disputed her account. See *White v. Equifax Information Services, LLC et al.*, Case No. 21-11840 (11th Cir. Dec. 23, 2021). Instead – like many cases – the plaintiff had only sent a dispute to the CRAs, stating that the dispute notification on her credit report was erroneous. The court noted that the furnisher met its obligations under the FCRA when it investigated the dispute and determined that the plaintiff had previously disputed the account, and never informed the furnisher that the dispute was resolved. Notably, the court also rejected plaintiff's arguments that the furnisher was required to reach out to her as part of its investigation. While the court acknowledged that such a step may be a "best practice," that is not what the FCRA requires.

Despite little traction in the courts, the plaintiffs' bar continues to raise the "no longer in dispute" claims, despite continued scrutiny by federal judges over the generic, recycled complaints being filed on this issue. Time will tell whether that scrutiny and the continued losses will stem the tide of the "no longer in dispute" cases, but claims continue to flow for now.

Scheduled Monthly Payment After Account Closure or Charge-Off

Finally, 2021 saw a continued stream of cases involving the reporting of scheduled monthly payments on charged-off or paid and closed accounts.

As alluded to above, two typical fact patterns underly these scheduled monthly payment cases. One set of cases concerns the reporting of scheduled monthly payments on an account that has been charged-off (i.e., the creditor was written off the debt as a loss) while the other concerns accounts that have been paid and closed. In both circumstances, consumers are focused on whether it is inaccurate or misleading for furnishers to report a scheduled monthly payment amount because it suggests an ongoing financial obligation.

Similar to the pay status cases discussed above, many courts have taken a holistic approach when considering the credit reporting that contains a scheduled monthly payment on charged-off or paid and closed accounts. For example, in *Young v. Equifax Info Servs., LLC et al.*, Case No. 20-15283 (D. N.J. Oct. 27, 2021), the court found that the inclusion of a scheduled monthly payment amount in a furnisher's reporting was not inaccurate or misleading when viewed in the context of other information reported. Specifically, in that case the furnisher reported that the consumer's account had a $0 balance, the account was closed, and the last payment occurred more than five years before the dispute at issue was raised. The court concluded that when the account was "viewed as a whole," it was undeniable that there was no ongoing financial obligation. To that end, the court considered the scheduled monthly payment to be historical information that was neither inaccurate nor misleading.

2021 saw a continued stream of cases involving the reporting of scheduled monthly payments on charged-off or paid and closed accounts.

The decisions rejecting the scheduled monthly payment claims almost unanimously rely on a distinction between historical and current information. For example, in *Lawson v. Mich. First Credit Union*, Case No. 20-cv-10460 (E.D. Mich. July 14, 2021), the court found that the reporting of a scheduled monthly payment on a charged-off account was not inaccurate or misleading because the account was also reported as "closed," "paid charge off," and that the balance was "$0." Again, considering the credit reporting holistically, the court found that the information was historical and did not indicate any ongoing payment obligation.

The takeaway from these cases is that the propriety of reporting a scheduled monthly payment on a charged-off or paid and closed account likely turns on whether the other information reported with the scheduled monthly payment. If the reporting, as a whole, demonstrates that the scheduled monthly payment is historical information, rather than an

indication of an ongoing payment obligation, it is not inaccurate or misleading. The importance of clarifying/contextual information cannot be understated when reporting a scheduled monthly payment amount on charged-off or paid and closed accounts.

Consumer Reporting Agencies

Article III Standing

In July, the U.S. Supreme Court decided *TransUnion LLC v. Ramirez*, a landmark FCRA case with vast implications for Article III standing generally.

Ramirez was the rare FCRA case in which a certified class action went to trial, resulting in a $60 million jury verdict. On appeal, a split Ninth Circuit panel reduced the punitive damages award, but otherwise affirmed. The case stemmed from TransUnion reporting the named plaintiff as a "potential match" for a government terrorist watch list, causing him to be denied a car loan. At issue before the Supreme Court was whether class members who were similarly identified as "potential matches" in TransUnion's database, *but whose consumer report was never disseminated to a third party*, had suffered a "concrete injury" sufficient to support Article III standing.

The Supreme Court held they did not. First, the Court emphasized that Congress can grant a statutory right and a cause of action, but the judiciary must still determine whether an alleged injury supports Article III standing. In other words, "under Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court."

Recognizing that "history and tradition" guide its concrete injury assessment, the Court viewed the alleged harm in *Ramirez* as bearing a "close relationship" to defamation actions for reputational harm. Third-party publication is critical—information in TransUnion's database that is never disseminated can only cause "harm [that] is roughly the same, legally speaking, as if someone wrote a defamatory letter and then stored it in her desk drawer. A letter that is not sent does not harm anyone, no matter how insulting the letter is."

The Court rejected the argument that class members whose information was not disseminated had standing due to a risk of *future* harm. Although exposure to future harm can support standing to "pursue forward-looking injunctive relief," these class members lacked standing because they "did not demonstrate that the risk of future harm materialized" or "that they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses."

Ramirez is certain to be front-and-center in standing arguments going forward. Allegations that a defendant violated a plaintiff's statutory right are not enough—"No concrete harm, no standing."

Willfulness Standard

In April, the U.S. Court of Appeals for the Second Circuit weighed in on the willfulness standard articulated in *Safeco Insurance Company of America v. Burr*. Specifically, that a defendant does not act in "reckless disregard" of the FCRA if its "reading of the statute . . . was not objectively unreasonable."

Shimon v. Equifax Information Services LLC involved Equifax's handling of a judgment that was "dismissed after trial." In response to the plaintiff's dispute, Equifax changed the reported "judgment" to "judgment satisfied," while the plaintiff argued the reference should have been removed entirely. Among other allegations, the plaintiff claimed Equifax willfully violated 15 U.S.C. §§ 1681g and 1681i.

The Second Circuit held that *Safeco*'s "reasonable interpretation," defense applies regardless of whether a defendant actually and contemporaneously relies on that interpretation at the time of the allegations. Emphasizing the Supreme Court's instruction that willful FCRA violations must be assessed *objectively*, the court reiterated that "evidence of subjective bad faith" is insufficient. In other words, if a defendant's FCRA interpretation, viewed retrospectively, was not objectively unreasonable, assessing the defendant's actual motivation "would introduce just the sort of subjective inquiry whose relevance the *Safeco* Court rejected."

Class Actions

In September, the U.S. Court of Appeals for the First Circuit affirmed an FCRA class action settlement from the District of Massachusetts. The settlement was challenged by an objecting (attorney) class member, who objected to class counsel's representation, the content of the notice provided to class members, the sufficiency of the recovery for class members, and class counsel's attorneys' fees.

In *Robinson v. National Student Clearinghouse*, the First Circuit agreed with the district court that the class action settlement was "fair, reasonable, and adequate." The court tersely rejected the objecting class member's arguments, noting that its review of the approval is for abuse of discretion. The court concluded that the parties' agreement was the result of arm's length negotiations with a mediator which followed "sufficient"—though informal—discovery, which revealed the number of putative class members and provided factual support for the $1.9 million settlement amount.

Robinson confirms that district courts have extensive discretion to approve or disapprove class action settlements, and that courts of appeals are reluctant to disturb their decisions. An objecting class member's best chance to affect the agreement is, therefore, at the district court's final fairness hearing.

Of course, a district court's discretion is not unlimited. In August, the United States Court of Appeals for the Ninth Circuit reversed and remanded the Central District of California's approval of a pre-certification class. *Kim v. Allison* challenged the dating app Tinder's offer of reduced prices to younger customers. Two of the objecting class members argued that Tinder's payout under the settlement agreement (whether cash or "Super Likes" for class members who reactivate their Tinder account) was inadequate, especially in light of how other recent class claims against Tinder were resolved.

The Ninth Circuit emphasized that pre-certification class settlements demand a "more probing inquiry" by the district court. Although the district court "correctly recited" Rule 23(e)(2)'s fairness factors, it "materially underrated the strength of the plaintiff's claims, substantially overrated the settlement's worth, and failed to take the required hard look at indicia of collusion, including a request for attorneys' fees that dwarfed the anticipated monetary payout to the class."

Industry Group Litigation

Credit Data Industry Association (CDIA)

The CDIA sued the state of Texas after it amended the Texas Fair Credit Reporting Act to limit information credit reporting agencies could include in an individual's credit report. *See* Tex. Bus. & Comm. Code § 20.05(a)(5). Specifically, the law would prohibit CRAs from including information regarding a collection account associated with a medical debt if the consumer was covered by a health benefit plan at the time of the event giving rise to the collection. The CDIA sued seeking declaratory and injunctive relief, arguing that the Texas law was preempted by the FCRA.

After the court dismissed the original complaint, the CDIA filed an amended complaint. Texas filed a subsequent motion to dismiss the CDIA's lawsuit under Rule 12, arguing that the CDIA lacked standing to bring the lawsuit and that the complaint otherwise failed to state a claim upon which relief could be granted. Specifically, Texas argued that the CDIA lacked standing because it had not alleged an injury-in-fact, and that the claim for declaratory judgment was not ripe because any alleged injury was contingent on future events. Texas also argued that the CDIA's claims were barred by the doctrine of sovereign immunity. Finally, the state argued that the complaint failed to state a claim because the Texas law was not preempted by the FCRA.

On September 28, the court denied Texas' motion in its entirety.

With respect to standing, the court found that the CDIA plausibly alleged its members would suffer harm if the law went into effect because they would be required to make substantial changes to their business operations. The court found that the claim for declaratory relief was ripe because the alleged future injury to the CDIA's members need not have occurred for the court to address whether the law was preempted by the FCRA. The court also found that an exception to the doctrine of sovereign immunity allowing a court to enjoin state officials from acting in violation of federal law applied.

Robinson *confirms that district courts have extensive discretion to approve or disapprove class action settlements, and that courts of appeals are reluctant to disturb their decisions.*

The court also rejected Texas' argument that the CDIA had failed to state a claim. Specifically, the court held that the CDIA had sufficiently alleged that the Texas law was preempted by Section 1681t(b)(1) because it concerns the same subject matter as Section 1681c of the FCRA – what medical debt information may be included in a consumer report.

Texas has appealed the court's denial of its motion to dismiss, and the case is now headed to the Fifth Circuit Court of Appeals, at least temporarily.

Association of Credit and Collection Professionals (ACA)

In June, the Association of Credit and Collection Professionals (ACA), along with other stakeholders, sued Sandy O'Laughlin, the commissioner of the Nevada Financial Institutions Division, seeking to prevent a Nevada state law concerning medical debts – S.B. 248 – from taking effect. S.B. 248, among other provisions, prevents collection agencies from reporting any information regarding medical debts during a 60-day notice period created by the law.

The ACA moved for a preliminary injunction, arguing in relevant part that S.B. 248's credit reporting prohibitions were preempted by the Fair Credit Reporting Act. The parties have been waiting for more than six months for a ruling, and are now renewing their request for an emergency injunction after the finalization of Regulation F, a rule implemented by the CFPB concerning medical debts.

Regulatory Updates

Furnishers

CFPB

On July 1, the CFPB issued an enforcement compliance bulletin regarding furnisher and consumer reporting agency requirements during the COVID-19 pandemic for consumer rental information. While the bulletin does not create or change any regulations, it does highlight at least one area that the CFPB is focused on with respect to consumer credit reporting.

The CFPB's bulletin expressed concern over the accuracy of reporting as it relates to renters given the (at the time) winding down of the federal and state moratoriums on evictions that were put in place in response to the COVID-19 pandemic. The federal eviction moratorium has since ended, and many states are without moratoriums of their own. Thus, with evictions resuming, the CFPB anticipates an influx of credit reporting regarding renters and accessing of consumer information as individuals attempt to secure housing.

With respect to data furnishers, the CFPB highlighted four areas that the CFPB "plans to pay particular attention to": (1) Whether furnishers are providing accurate rental information to CRAs; (2) Whether furnishers are providing information about rental arrearages that include amounts that were already paid on behalf of a tenant through government grant or relief programs, such as the Emergency Rental Assistance programs; (3) Whether furnishers are providing information about rental arrearages that include fees or penalties that CARES Act Section 4024(b) or other laws prohibit charging; and (4) Whether furnishers are complying with their obligations to investigate disputed information in a consumer report, including whether they are conducting timely and reasonable investigations.

While the bulletin simply reiterates existing statutory and regulatory obligations for data furnishers, it is a clear message from the CFPB that reporting concerning rental information is on its radar. Data furnishers should also assume that the CFPB is paying equal attention to reporting and dispute investigations related to mortgages. Indeed, just as the federal eviction moratorium has ended, so too

have the CARES Act accommodation requirements for federally backed mortgages. Thus, in addition to the CARES Act amendments to the FCRA which cover the reporting of loans that received an accommodation as a result of the COVID-19 pandemic, the CFPB will undoubtedly be focused on ensuring that post-accommodation reporting and dispute investigations comply with the FCRA.

FTC

While the FTC did not create or modify any substantive regulations concerning data furnishers in 2021, it did increase the penalties for non-compliance with the FCRA. Specifically, the maximum penalty per violation in a lawsuit brought by the FTC was raised to $4,111 under the Federal Civil Penalties Inflation Adjustment Improvements Act of 2015.

Consumer Reporting Agencies

CFPB

On April 6, the CFPB issued a statement that it would rescind its "flexible supervisory and enforcement approach during the COVID-19 pandemic" regarding compliance with the FCRA for CRAs as of April 1. 86 FR 17695-01. It noted that the CFPB believes CRAs had sufficient time to adapt to the business operation changes that resulted due to the pandemic, and they should thus "be able to regularly meet their obligations under the FCRA."

On July 7, the CFPB issued a bulletin stating that it would be "paying particular attention" to CRAs' compliance with their accuracy and dispute obligations under the FCRA with respect to rental information. 86 FR 35595-01. It stated it would pay such special attention as "pandemic-related government interventions aimed at protecting renters" began to expire through the remainder of the year. It advised CRAs to take "immediate steps" to ensure compliance, such as using a sufficient number of identifiers to match consumer report information to the consumer, accurately reporting eviction information that is complete and not

misleading, and properly and timely investigating disputed information. The CFPB warned that failure to take such steps would result in it taking enforcement action to address violations and seeking "all appropriate corrective measures, including remediation of harm to consumers."

On November 4, the CFPB issued an advisory opinion, stating that a CRA that engages in name-only matching violates the FCRA's reasonable procedures requirement, 15 U.S.C. § 1681e(b). Although styled as an advisory opinion, the CFPB made clear that the opinion is considered an "interpretive rule" issued under the CFPB's authority to interpret the FCRA. The opinion focused on the process of name-only matching, defined as "matching information to the particular consumer who is the subject of a consumer report based solely on whether the consumer's first and last names are identical or similar to the first and last names associated with the information, without verifying the match using additional identifying information for the consumer." However, the opinion also expressed particular concern regarding the harm that inaccurate reporting might have on consumers seeking to financially recover in the wake of the COVID-19 pandemic. The opinion concluded that matching on name only (first and last name) will likely lead to inaccuracies in consumer reports, which goes against the purpose of § 1681e(b). The opinion said that "it is not a reasonable procedure to use name-only matching to match information to the consumer who is the subject of the report in preparing a consumer report." It supports that conclusion on "the high risk that name-only matching will result in the inclusion of information that does not pertain to the consumer who is the subject of the report and the relative lack of burden on a consumer reporting agency associated with utilizing additional identifiers or not including name-only matched information in a consumer report."

The opinion further highlights a potential increased risk of inaccuracy when name-only matching is used for Hispanic, Asian, and African American consumers, based on census data showing less last-name diversity in these populations. (The CFPB's reference to this possible demographic disparity is interesting to note, as this opinion was released the same week the CFPB also released a report indicating credit report disputes more commonly occur among consumers residing in majority Hispanic or Black areas.)

Finally, on November 29, the CFPB issued a final rule regarding the amount CRAs can charge consumers for copies of their credit report. Specifically, the final rule increased the ceiling for allowable charges under Section 612(f) of the FCRA to $13.50 effective January 1, 2022.

State Attorneys General

The North Carolina attorney general, the CFPB, and the Federal Trade Commission (FTC) filed an amicus brief in the U.S. Court of Appeals for the Fourth Circuit in support of the consumer plaintiffs' position in *Henderson v. The Source for Public Data, L.P.*, No. 21-1678. Plaintiffs alleged that Public Data, an online public-record provider, is a CRA that violated the FCRA by including false and inaccurate criminal information in background check reports that it produced and offered for sales on its website. Public Data raised Section 230 of the Communications Decency Act (CDA) as a defense, arguing that it was entitled to Section 230 immunity as the publisher of third-party information. Plaintiffs contend Section 230 of the CDA does not bar the application of the FCRA procedural requirements to the consumer reporting agency. The district court agreed with Public Data, finding that the FCRA is not listed in the CDA's list of statutory exemptions from immunity and that Public Data qualified for Section 230 immunity because it did not produce the content of the reports, and instead the information is derived from other content providers. *See generally Henderson v. Source for Public Data, L.P.*, No. 3:20-cv-294, -- F. Supp. 3d – (E.D. Va. 2021). Plaintiffs appealed.

The amicus brief argues, among other things, that Section 230 does not provide immunity to Public Data because plaintiffs' FCRA claims seek to hold Public Data liable on the basis of Public Data's failure to follow the process-oriented requirements that the FCRA imposes on CRAs—not on the basis of the inaccurate data itself. The brief also argues that plaintiff's claims sufficiently alleged Public Data created and developed its reports, including by collecting, sorting, summarizing, and assembling

public-records information, so it was not merely the publisher or speaker of another person's content. The case is still being briefed at the Fourth Circuit.

Legislative Updates

Federal Legislation

Introduced Legislation

H.R. 5714, the CFPB Whistleblower Incentives and Protection Act, was introduced in the House to amend the Consumer Financial Protection Act of 2010 by protecting and incentivizing whistleblowers within the CFPB to anonymously report "conduct within the CFPB that does not serve the American consumer."

The bill offers $50,000 or up to 10% of the total amount of monetary sanctions imposed and collected to whistleblowers who contribute to the "successful enforcement" of an administrative proceeding or court action. If the bill becomes law, the CFPB will determine the amount of the financial award based on the significance of the whistleblower's information and overall contribution to the outcome of the action.

H.R. 3439, the Fair Credit Reporting for Servicemembers Act, was introduced in the House for the third time. The bill aimed to fortify consumer credit protections for active-duty service members by prohibiting derogatory credit information from being reported on an active-duty service member's consumer report while on deployment. The bill also extends these protections to members of the National Oceanic and Atmospheric Administration and Public Health Service.

S. 2790, the Consumer Financial Protection Bureau Accountability Act of 2021, was introduced in the Senate and would require congressional approval for the CFPB annual budget. The current budget is set by the Federal Reserve without congressional approval or oversight.

The Medical Debt Relief Act of 2021, composed of H.R. 773 and S. 214, was introduced in the House and Senate to amend the FCRA and FDCPA. The bills each aim to modify credit reporting requirements regarding medical debt. The bills would prohibit a consumer credit reporting agency from adding medical debt information to a consumer credit report if the debt: 1) was fully paid or settled; or 2) is less than a year old. The bills also would require medical debt collectors to notify consumers before furnishing the medical debt to consumer reporting agencies.

If the bill becomes law, the CFPB will determine the amount of the financial award based on the significance of the whistleblower's information and overall contribution to the outcome of the action.

Similarly, H.R. 1645, the Protecting Consumer Access to Credit Act, was introduced in the House to amend the FCRA requirements for reporting adverse credit information pertaining to financial abuse, unfair or fraudulent mortgage lending, or fraudulent private student lending. The bill would also require CRAs to exclude paid, medically necessary debt from the consumer's credit report if the debt was paid over a year prior. Further, the bill would prohibit credit reporting agencies from using Social Security numbers in credit reports for consumer identity verification purposes. In addition, the bill would require the CFPB to supervise and examine the CRAs' cybersecurity measures, and to conduct a study of the use of nontraditional data in credit reporting.

H.R. 4919, the Deter Obnoxious, Nefarious, and Outrageous Telephone (DO NOT) Call Act was introduced in the House on August 3. The bill would intensify the penalties for violations of the Telephone Consumer Protection Act to curtail the rapidly growing number of predatory robocalls throughout the United States.

The bill is a bipartisan companion bill to S. 1913, which was introduced in the Senate on May 27. Also named the DO NOT Call Act, S. 1913 and H.R. 4919

proposed prison terms of up to one year for willfully and knowingly violating the TCPA, and up to three years for aggravated violations. The two bills also proposed a $20,000 maximum penalty for falsifying caller ID in violation of the TCPA.

Enacted Legislation

The Consider Teachers Act of 2021 (PL 117–49) was passed on October 13, 2021, and amended Section 420N of the Higher Education Act of 1965 (20 U.S.C. 1070g–2) regarding the Teacher Education Assistant for College and Higher Education Grant (TEACH) Program so that the Secretary of Education can request CRAs to remove any negative credit reporting about TEACH recipients under certain circumstances.

The TEACH Program provides funds to students (or "recipients") who are enrolled in a TEACH-eligible study program at a school that participates in the TEACH Program and who agree to teach at a low-income school for at least four years after graduating. Students also must sign the TEACH Grant Agreement to Serve or Repay. If the recipients do not complete their four-year service requirement, their TEACH Grant is converted to a Federal Direct Unsubsidized Stafford loan by the Secretary of Education, but the recipients who do not complete the requirement can ask the Secretary to reconsider.

If (a) the Secretary determines the reason for the conversion was due to: (1) the recipient's failure to timely submit a certification required under the Higher Education Act; (2) an error or processing delay; (3) a change to the fields considered eligible for fulfillment of the service obligation; (4) a recipient's having previously requested to have the TEACH Grant converted to a loan; or (5) another valid reason determined by the Secretary, and (b) the recipient has demonstrated that he/she has met or is in the process of meeting the service requirement, the Secretary can, among other things, request CRAs to remove any negative credit reporting due to the conversion of the TEACH Grant to a loan. But nothing in the Act specifically requires CRAs to remove the information upon the Secretary's request.

State Legislation

In 2021, a few state legislatures implemented and debated changes that affect credit reporting.

The most notable law passed affecting credit reporting was in Maryland. While other states such as Illinois and Nevada have passed similar laws to change how creditworthiness is determined, Maryland's law is one of the most detailed to pass last year. Additionally, California has two bills in consideration in the Senate Appropriations Committee which would also affect how credit reporting agencies interact with consumers and credit financial services organizations.

Maryland

On May 30, Maryland enacted legislation that revises the rules of determining creditworthiness. The law makes changes to Md. Code Ann., Financial Institutions (FI) § 1-212. The law became effective on October 1, and it requires various financial institutions (specifically, Maryland chartered banking institutions, credit unions, savings and loan associations, community development financial institutions, and specified credit grantors) to adhere to the rules concerning evaluations of applications under federal law, 12 C.F.R. § 1002.6. These financial institutions will also be required to consider the following factors as indications of potential creditworthiness:

1. History of rent or mortgage payments;
2. History of utility payments;
3. School attendance; and
4. Work attendance.

Additionally, if an applicant requests, the financial institution must consider other verifiable alternative indications of creditworthiness presented by the applicant not included above.

While there are statutory definitions of what constitutes "school attendance" or "work attendance," these terms likely refer to measuring school or work attendance regarding an otherwise evaluated component. For example, a creditor would need to consider work attendance if the creditor is evaluating the applicant's income for reliability and continuance of income. Likewise, a creditor considering student loans would consider school attendance if the creditor is assessing the

likelihood of graduation.

According to the Maryland Department of Labor, this law requires integration of the above requirements into risk and compliance frameworks by establishing sufficient policies, procedures, and control to ensure compliance with the changes to the rules. However, this law doesn't require a creditor to change its underwriting standards, so the practical impacts of such considerations may be minimal.

This law is similar to other established state laws that require creditors to consider other information submitted by applicants. *See* 815 Ill. Comp. Stat. Ann. 120/4, and Nev. Rev. Stat. Ann. § 604A.5038.

California

In California, Assembly Bill No. 1089, currently held in the Senate appropriations committee, would place licensure requirements on those engaging in credit services and would require those engaging in credit services to comply with oversight requirements as mandated by the Department of Financial Protection and Innovation. The bill would also require consumer credit reporting agencies and creditors that know that a consumer is represented by a credit services organization to communicate with the credit services organization unless otherwise specified.

Additionally, Assembly Bill No. 373, currently awaiting hearing by the Senate appropriations committee, would prohibit a consumer credit reporting agency from including in a consumer credit report accounts about which a consumer has provided the consumer credit reporting agency documentation that the debt, or any portion of the debt, is the result of economic abuse.

CDIA Guide Updates

The CDIA has released the 2021 version of its CRRG. The new version does not include any substantive changes, although it is supplemented by periodic guidance that the CDIA issues in response to particular events, such as the COVID-19 post-accommodation guidance discussed above.

CYBERSECURITY AND PRIVACY

Federal Privacy Developments

While data privacy has remained a major topic of discussion and debate, none of the numerous federal privacy bills introduced in 2021 made material progress toward becoming law. Despite this lack of progress, many believe that a bipartisan consensus is growing regarding the need for comprehensive legislation. The Federal Trade Commission's (FTC) privacy enforcement role was a major focus of 2021's discussion, as leadership changes and proposed funding increases may significantly alter how this agency governs privacy moving forward.

Updates on Federal Privacy Legislation

Over two dozen privacy-related bills were introduced in Congress in 2021. Many of these bills seek to establish a comprehensive privacy regime similar to what is being considered in many state legislatures. One example is the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act, which would create a comprehensive privacy framework that preempts state privacy statutes. In addition to these comprehensive proposals, other bills, such as the Social Media Privacy Protection and Consumer Rights Act and the Filter Bubble Transparency (FBT) Act, took aim at narrower privacy-related concerns.

The Senate Commerce Committee held a series of data privacy-related hearings in the fall. During these hearings, senators from both sides of the aisle expressed their general support for comprehensive privacy legislation. Despite this shared goal, these hearings highlighted the fact that disagreements still exist surrounding some of the key issues (e.g., the merits of a private right of action, and the scope of exceptions for businesses regulated by sector-specific privacy laws). These hearings are particularly noteworthy, as many view the Commerce Committee as the primary legislative gatekeeper on this topic.

Future Role of FTC

The future role of the FTC has also been a major topic of discussion this year. On September 14, the House Committee on Energy and Commerce appropriated $1 billion over 10 years to the FTC to establish and operate a new privacy bureau. Establishing a dedicated bureau in the FTC would likely have a strong symbolic and practical impact. This funding increase exceeds what has been proposed in many privacy bills, and would almost certainly facilitate broader enforcement by this agency. In the absence of a statutory regime, some have speculated the FTC may use "Magnusson-Moss" rulemaking to create more stringent privacy requirements. For further analysis on these potential FTC changes, please visit: https://www.troutman.com/insights/movement-on-all-sides-toward-broader-data-privacy-and-security-oversight-by-ftc.html.

In September, President Biden nominated Alvaro Bedoya to serve as an FTC commissioner. Bedoya has written numerous works related to privacy and is the founding director of Georgetown Law's Center on Privacy and Technology. Collectively, this leadership change and the aforementioned privacy funding could lead to far more enforcement activity and oversight by the FTC.

For further analysis of Bedoya's appointment, please visit: https://www.troutman.com/insights/biden-to-nominate-privacy-advocate-alvaro-bedoya-as-an-ftc-commissioner.html.

On June 15, the Senate approved Lina Khan's nomination as a commissioner of the FTC, and later that day, President Biden swore her in as chair. In a memo to agency staff, Khan emphasized a desire for a "forward-looking" approach that is "especially attentive to next-generation technologies, innovations, and nascent industries across sectors." To achieve this, Khan stressed a "holistic approach to identifying harms, recognizing that antitrust and consumer protection violations harm workers and independent businesses as well as consumers"

The Senate Commerce Committee held a series of data privacy-related hearings in the fall. During these hearings, senators from both sides of the aisle expressed their general support for comprehensive privacy legislation.

and "targeting root causes rather than one-off effects." For further analysis on her selection, please visit: https://www.troutman.com/insights/lina-khan-selected-as-ftc-chair.html.

Federal Outlook-Looking Forward

In 2022, we expect that federal legislators will continue to introduce privacy legislation. The momentum of this legislation may depend in large part on the number of successfully adopted state privacy laws, and the extent to which these state laws conflict with one another. However, preemption will continue to be a major hurdle. Look for discrete pieces of legislation that address single issues rather than an omnibus bill. Outside of Congress, we expect increased enforcement by the FTC, especially if the proposed additional funding is approved. In the years to come, we may look back at 2021 as the "calm before the storm" in the United States.

State Privacy Developments

California

The California Consumer Privacy Act (CCPA) has been in effect for almost two years. The CCPA was California's first stab at an expansive new privacy law that created obligations for many businesses that collect personal information about California residents. The CCPA went into effect on January 1, 2020, and enforcement began July 1, 2020.

The law provides California residents with access and control over their personal information and allows them to say, under certain circumstances, how organizations collect, use, and disseminate this data. More specifically, California provides its residents with certain rights, including the right to access personal information, the right to delete personal information, and the right to opt out of the sale of their personal information.

In March 2021, the California AG finalized a fourth set of modifications to the CCPA regulations. This latest round of modifications focused on clarifying how consumers can opt out of the sale of their personal information, and included provisions: (i) banning so-called "dark patterns" that delay or obscure the process for opting out of the sale of personal information; (ii) permitting businesses to use an opt-out icon in addition to any "Do Not Sell My Personal Information" link; and (iii) requiring businesses that sell personal information collected offline to provide an offline right-to-opt-out notice. For further analysis about these new regulations, please visit: https://www.consumerfinancialserviceslawmonitor.com/2021/03/california-ag-announces-approval-of-fourth-set-of-modifications-to-ccpa-regulations.

Efforts have also been underway to implement the California Privacy Rights Act (CPRA), which takes effect on January 1, 2023. As a reminder, Californians voted the CPRA into law in November 2020. The law amends the CCPA by expanding privacy rights and moving the CCPA closer to the direction of the EU's GDPR. CPRA is not a new law, but rather an expansion of the obligations and disclosures already mandated by the CCPA.

CPRA's implementation efforts are being carried out in large part by the California Privacy Protection Agency (CPPA), the members of which were appointed in March 2021. In October, the CPPA announced that Ashkan Soltani would serve as the agency's inaugural executive director. Soltani will oversee the day-to-day operations of the agency as well as direct enforcement, rulemaking, and public awareness activities. His appointment signals that the CPPA will likely take an aggressive stance when enforcing privacy regulations and policy.

The CPPA also began the CPPA rulemaking process by issuing a call for comments related to any area on which the CCPA has authority to adopt its rules. The final deadline to promulgate regulations is July 1, 2022, which will allow companies time to comply before the effective date of January 1, 2023. To meet this July deadline, the agency needed to publish an initial draft of the regulations no later than December 2021 to account for the time necessary for approval by the California Office of Administrative Law and the required public comment periods. Enforcement of the CPRA will begin July 1, 2023.

For a practical guide on the impact of CPRA on existing CCPA frameworks, please visit: https://www.troutman.com/images/content/2/7/v2/274999/Final_TP_CPRACompendium_Dec2020.pdf.

For further information on the CPPA, please visit: https://www.jdsupra.com/legalnews/california-privacy-protection-agency-6636546.

Virginia Consumer Data Privacy Act

In March, the Virginia Consumer Data Protection Act (CDPA) was signed into law, and Virginia became the second state in the country to adopt comprehensive privacy legislation. It should come as no surprise that Virginia's CDPA is similar to the CCPA and CPRA.

The CDPA will apply to all businesses that control or process data for at least 100,000 Virginians, or those commercial entities that derive at least 50% of their revenues from the sale and processing of consumer data of at least 25,000 Virginians. Under this law, Virginians are empowered with consumer rights, including those found in the CCPA/CPRA. The chart below previews the rights afforded to Virginians and how those rights compared to the rights offered by California under the CCPA and CPRA.

Unlike the CCPA/CPRA, the CDPA includes a broad GLBA exemption that applies to GLBA-regulated entities (rather than just GLBA-regulated data). The CDPA's Privacy Policy requirements are somewhat less stringent than those of its California counterparts, and do not require that businesses provide details on exercising consumer rights, the sources of their data, or the date that the policy was last updated. This law may be amended in the coming year, as the Virginia Consumer Data Protection Working Group (made up of various business and consumer rights stakeholders) continues to review the potential impact of the CDPA.

For more information about the CDPA, please visit Troutman's five-part Virginia Consumer Data Protect Act series, available at https://www.troutman.com/images/content/2/7/279264/VCDPA-Series.pdf.

Colorado Privacy Act

The Colorado Privacy Act (CPA) was adopted in June, making Colorado the third state in the country to adopt a comprehensive data privacy regime. This law will take effect on July 1, 2023, and most closely resembles the CDPA.

The CPA applies to "controllers," which are defined to include any "person that, alone or jointly with others, determines the purposes for and means of processing personal data." A controller is subject to the CPA only if it: (1) conducts business in Colorado or intentionally markets its products or

Rights	CA CCPA	CA CPRA	VA CDPA
Access	✓ Yes	✓ Yes	✓ Yes
Delete	✓ Yes	✓ Yes	✓ Yes
Correct Inaccuracies	✓ Yes	✓ Yes	✓ Yes
Opt Out of Sale or Other Transfers	✗ No	✓ Yes	✓ Yes
Data Portability	✓ Yes	✓ Yes	✓ Yes
No Discrimination	✓ Yes	✓ Yes	✓ Yes

services to Colorado residents; and (2) controls or processes the personal data of 100,000 or more Colorado residents in a calendar year, *or* controls or processes the personal data of 25,000 or more Colorado residents, and derives revenue or cost savings from the sale of personal data.

The exemptions available to businesses under the CPA also align most closely with the CDPA, with the following exceptions: (i) nonprofits are not exempted under the CPA; (ii) the CPA's HIPAA/HiTECH exemption is limited to data regulated under those laws; and (iii) the CPA's GLBA exemption extends to *affiliates* of regulated financial institutions. Like its state-level predecessors, the CPA does not include a private right of action for privacy violations. This law will be enforced by the Colorado attorney general and Colorado's district attorneys. During the first two years of enforcement, businesses will have a right to cure violations within 60 days.

For further analysis about the CPA please visit: https://www.troutman.com/insights/colorado-passes-comprehensive-data-privacy-law.html.

Failed State Efforts

While Virginia and Colorado were the only states in 2021 to pass comprehensive privacy legislation, privacy bills were introduced in about half of the legislatures nationwide. Many of these bills did not advance beyond committee assignment; however, others came quite close to passing. Notably, versions of the Florida Privacy Law (FPL) and Washington Privacy Act passed both houses of each state's legislature. In both instances, the role of a private right of action caused debate that prevented final votes.

Pending State Laws

As of late November, numerous states still had pending data privacy bills. While most if not all of these laws will fail, they are indicative of the continued legislative interest on this topic. We expect that many of these laws may be "carried over" to the second half of the legislative session in states where that process is permissible.

The UPDPA

In July, the Uniform Law Commission (ULC) published a final draft of the long-awaited Uniform Personal Data Protection Act (UPDPA). Similar to the Uniform Commercial Code (UCC), this law is intended to serve as a blueprint for state legislators considering comprehensive privacy legislation. The UPDPA deviates significantly from existing state privacy laws, most critically in its scope (applying to organizations that maintain personal data, regardless of any volume or revenue threshold), and approach to the classification of data processing activities (all activities are deemed compatible, incompatible, or prohibited and the majority of the substantive provisions depend on this designation).

For further analysis of the UPDPA's unique scoping requirements, please visit: https://www.consumerfinancialserviceslawmonitor.com/2021/09/the-uniform-personal-data-protection-act-a-new-approach-to-scoping.

Looking Forward

Data privacy legislation will likely be considered in a majority of state legislatures next year. We can expect the reemergence of bills in states like Florida and Washington (where privacy legislation has already made significant progress), as well as new bills based on the UPDPA, CPRA, CDPA, or CPA. As we experienced with data breach statutes, expect to see states attempt to place their unique mark on privacy.

The growing number of state-level privacy laws taking effect in 2023 will force many businesses to make difficult decisions about their privacy compliance programs, procedures, and documents. To maintain a uniform national approach, unless businesses are able to tag and segregate their data based on consumers' state of residence, they may have no choice but to comply with the most stringent version of each privacy requirement. For instance, businesses processing sensitive personal data may be required to provide opt-in consent to comply with the CDPA, while the CPRA would only have required opt-out consent. Unless such data tagging/segregation is implemented, businesses will likely be required to obtain opt-in consent for the processing of all sensitive data, regardless of a consumer's state of residence.

Businesses should also be mindful of how these state-level privacy laws will be enforced. Currently, California, Virginia, and Colorado all envision

enforcement to be the responsibility of the attorneys general (AGs) or another regulatory body, such as the California Privacy Protection Agency. Enforcement will likely focus on a number of areas, but with a general theme. Specifically, using the California AG's experience with enforcing the CCPA, we can expect that the Virginia and Colorado AGs will want to ensure that organizations are not treating the new laws as check-the-box exercises, but rather are providing consumers with required information and timely engaging with consumer's requests. Indeed, not only will the AGs want organizations to provide the necessary information, but they will also require it be conveyed in a way that can be easily understood by the average consumer, and to provide the fewest number of steps for consumers to access the information and exercise their rights.

For additional information relating to enforcement, please visit our California Consumer Privacy Act Enforcement Series, available here.

Developments in International Law

2021 brought big changes to the international privacy landscape. Although the General Data Protection Regulation (GDPR) has been in effect for over three years now, the European Commission released new standard contractual clauses (SCCs) for businesses to use when transferring personal data outside of the European Union. Further, 2021 broke records for GDPR fines. In addition to Europe's privacy updates, China and South Africa have enacted their own comprehensive privacy legislation.

Europe

Europe has had an impactful year regarding privacy developments, especially in regard to the updated standard contractual clauses and GDPR fines.

Cross-Border Data Transfers

On June 4, the European Commission published its final implementing decision adopting new standard contractual clauses (SCCs) for the transfer of personal data to third countries. SCCs have long been an important tool for European Union (EU) data transfers, as one of only a handful of mechanisms available to legitimize cross-border transfers of data from the EU. The old SCCs were much needed, as they were adopted under the Directive 95/46, which was repealed and replaced by the GDPR. While the old SCCs were limited to two separate templates for controller-to-controller and controller-to-processor transfers, the new SCCs feature interchangeable "modules" to create clauses for the variety of data transfers prevalent today. Such new modules include: from a controller to another controller; from a controller to a processor; from a processor to a processor; and from a processor to its appointing controller.

The new SCCs also include "docking clauses" for multiparty use that allow for change over time. Additionally, the new SCCs contemplate that data exporters may be located outside the EU, an important innovation considering the GDPR's extraterritorial reach.

The new SCCs also address the consequences of the Schrems II decision by requiring parties to affirm they have no reason to believe that the laws of the country of the recipient prevent compliance with the SCCs. To make this affirmation, we are seeing a number of importers of personal data conducting data transfer impact assessments outlining potential risks of non-compliance with SCCs, and discussing supplemental physical, technical and administrative measure to overcome any risks. Companies have some time to update their contracts. Old SCCs executed before September 27, 2021, will be valid for another 15 months, until December 27, 2022.

Importantly, post-Brexit, while the United Kingdom (UK) adopted the GDPR in nearly identical form, the new EU SCCs cannot be used for UK-specific, cross-border data transfers. The UK's Information Commissioner's Office (ICO) has released a draft international data transfer agreement (IDTA), which will replace SCCs. Public consultation on the draft IDTA closed on October 11, 2021.

EU-U.S. Privacy Shield 2.0

Although efforts to develop an EU-U.S. Privacy Shield 2.0 stalled as a result of the pandemic and the 2020 presidential election, 2021 brought hope that diligent efforts are being made between the U.S. government and the European Commission to develop a new framework. In fact, on March 25,

2021, U.S. Secretary of Commerce Gina Raimondo and European Commissioner for Justice Didier Reynders issued a joint statement indicating that intensified negotiations are taking place on an enhanced EU-U.S. Privacy Shield framework to comply with the July 16, 2020 judgment of the Court of Justice of the European Union in the Schrems II case, which invalidated the EU-U.S. Privacy Shield.

The Congressional Research Service reported that the U.S. is seeking to provide the EU with greater assurances through executive orders and administrative action on safeguards to protect the privacy of EU citizens, and to provide some form of redress in U.S. courts for any alleged misuse of their data. It also reported that members of Congress support a Privacy Shield framework and recognize it as vital to U.S.-EU trade investment ties. Optimism remains high that a new framework can be achieved in 2022.

GDPR Fines

2021 broke records for the largest GDPR fines issued. Two large technology companies received the second-highest and highest fines in GDPR history. The highest fine was 746 million euros (approximately $887 million), and the second-highest fine was 225 million euros (approximately $28.3 million). These fines were issued for lack of consent regarding privacy practices and lack of transparency regarding data sharing, respectively. This new record is nearly 15 times larger than the previous record.

China

China enacted two privacy laws in 2021, the Data Security Law of the P.R.C. and the Personal Information Protection Law of the P.R.C.

The Data Security Law of the P.R.C.

China's Data Security Law of the P.R.C. came into effect on September 1. This law applies to data processing within China, as well as data processing outside of China if it could harm national security, the public interest, or the rights and interest of Chinese citizens and organizations.

The Personal Information Protection Law

In August, China passed the Personal Information Protection Law (PIPL), which took effect on November 1. This is China's first full-scale data protection law, and it closely resembles Europe's GDPR. The PIPL has an extraterritorial scope, and as such, businesses across the world should review their data processing activities to determine whether PIPL applies. Generally, PIPL applies to data processing that occurs: (1) to provide products or services to individuals in China; (2) to monitor/evaluate behavior of individuals in China; and (3) under other circumstances described in the laws or administrative regulations.

Some of PIPL's requirements include having a lawful basis for data processing activities and responding to/honoring data subject requests. If a data subject request is rejected, individuals will have a private right of action. Individuals have a right to know and to make decisions regarding to their personal information; restrict use of personal information; consult and copy their personal information from the processors; data portability; correction and deletion; and request explanation of processing rules.

Notably, the PIPL has strict requirements for cross-border transfers. Some of these requirements include meeting a "necessity test," giving notice of the transfer, getting consent to the transfer, and meeting one of the following four conditions:

1. Getting approval from the relevant government authority following a security assessment;
2. Obtaining a personal information protection certification from the relevant government authority;
3. Executing a contract with the recipient organization containing the standard contractual language; or
4. Satisfying "other conditions" provided by laws, regulations, or the Cyberspace Administration of China.

China's Data Security Law and Personal Information Protection Law combined with China's 2017 Cybersecurity Law make up the nation's comprehensive privacy regulatory scheme.

South Africa

Although South Africa's Protection of Personal Information Act (POPIA) was passed in 2013, and although some aspects came into effect July 1, 2020, there was a grace period of 12 months. The grace period ended on July 1, 2021. As such, companies subject to POPIA needed to finalize their compliance programs in 2021. Enforcement includes civil and criminal penalties, as well as fines of up to ZAR 10 million ($580,000 USD).

POPIA was originally modeled off the EU Data Protection Directive 95/46/EC, and shares many similarities with GDPR, such as having conditions for lawful processing, cross-border transfers, and responding to data subject requests. A

Individuals have a right to know and to make decisions regarding to their personal information; restrict use of personal information; consult and copy their personal information from the processors; data portability; correction and deletion; and request explanation of processing rules.

first for South Africa, POPIA institutes a data breach notification obligation. Throughout 2021, the Information Regulator of South Africa has provided guidance regarding the exemptions for the processing of personal data, as well as the processing of special categories of personal data.

Notably, with all aspects of the law now in full effect, the European Commission is likely to make an "adequacy" determination on whether POPIA is adequately protective, which would help enable cross-border transfers of data from the EU to South Africa. If POPIA is not deemed adequately protective, it is likely that amendments to POPIA would follow to facilitate the flow of data between South Africa and Europe.

International trends show that more countries are likely to introduce comprehensive privacy legislation and fines for violations of these laws are on the rise. Practitioners and those interested in the international privacy landscape should watch for changes to existing privacy legislation, such as the GDPR, as well as the introduction of new legislation in other countries.

Information Security

With the continued rise of ransomware and state-sponsored cyberattacks, government agencies, particularly on the enforcement side, were kept busy throughout 2021.

For those unfamiliar with ransomware, it is a type of malicious computer software designed to encrypt data on a victim's device so that the data is rendered unusable, meaning a complete halt to all operations for some businesses. To un-encrypt the data, cyber criminals demand businesses pay a ransom; often, it is only then that some businesses can continue normal operations.

As businesses became better at defending against these types of attacks, namely by creating "data backups" from which data could be recovered without paying the ransom, cyber criminals evolved and turned to a new type of ransomware attack referred to as "double dipping" or "double extortion." This type of attack, which did not begin to surface until late 2019, is aimed at coercing victims to pay by not only encrypting data and then charging a ransom for the decryption key, but also exfiltrating data and then demanding payment in exchange for a promise to permanently destroy or delete the data stolen from the victim. The implied threat is that victims who refuse to pay to recover their data can expect to see the data on the dark web, which may embarrass the victims and tarnish their good reputation and goodwill. This differs from what used to be the standard modus operandi of ransomware attacks, which was to only encrypt data on the victim's system so that it becomes unusable, and then charge a ransom for the decryption key.

With ransomware attacks, including double-dipping attacks, on the rise, several government agencies offered ransomware guidance in 2021 to the general public, as we detail further below.

OFAC Guidance on Paying the Ransom

On October 1, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory warning of the perils of facilitating ransomware payments involving malicious cyber-enabled activities. OFAC has seen an increase in ransomware attacks on various governmental entities, financial institutions, health care institutions, and educational institutions during the COVID-19 pandemic. This advisory warns companies that may unintentionally, inadvertently, or knowingly facilitate victims' ransomware payments — such as financial institutions, cyber insurance firms, and digital forensics and incident response companies — that their facilitation or processing of payments will likely encourage future ransomware payment demands and may also violate OFAC sanctions regulations against designated individuals, entities, or restricted countries. For further analysis, please visit: https://www.consumerfinancialserviceslawmonitor.com/2020/10/ofac-warns-companies-about-facilitating-ransomware-payments.

OFAC Sanctions Compliance Guide

In October, OFAC provided guidance relating to sanctions compliance for the virtual currency industry. OFAC reminded all individuals that as a "general matter, U.S. persons, including members of the virtual currency industry, are responsible for ensuring they do not engage in unauthorized transactions or dealings with sanctioned persons or jurisdictions." Members that are part of the industry should be aware that ransomware actors using virtual currency to facilitate financial transactions may be sanctioned; thus, any U.S. persons transacting with them may be in violation of OFAC's designations. To read OFAC's complete guidance relating to virtual currency, please visit: https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

CISA Guidance

On January 21, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) started a new campaign, called the Reduce the Risk of Ransomware Campaign, which focuses on encouraging the public and private sectors "to implement best practices, tools and resources that can help them mitigate [] cybersecurity risk and threat[s]." Due to the continued effects of the COVID-19 pandemic, CISA will focus the campaign on supporting COVID-19 response organizations and K-12 schools. CISA also reminded the public that it developed a ransomware center (https://www.cisa.gov/stopransomware) containing several resources, such as fact sheets, infographics,

trainings, and webinars. To read more about CISA's campaign, please visit https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware.

FBI Guidance

On July 27, Bryan Vordran, assistant director of the Federal Bureau of Investigation's (FBI) cyber division, told federal lawmakers that if Congress bans ransom payments, it will be "putting U.S. companies in a position of another extortion, which is being blackmailed for paying the ransom and not sharing that [information] with authorities[.]" Vordran said it is the FBI's "opinion that banning ransomware payment is not the road to go down." Vordran stated that "silence benefits ransomware actors the most," and banning ransom payments will likely only result in fewer reported incidents. The FBI argued that lawmakers should instead create a federal standard that would "mandate the reporting of certain cyber incidents, including most ransomware incidents." For further analysis on this guidance, please visit: https://www.consumerfinancialserviceslawmonitor.com/2021/08/the-fbi-warns-lawmakers-that-banning-ransom-payments-may-backfire.

States' Response to Ransomware

Organizations worldwide were busy in early July due to the Kaseya incident. Kaseya, a software provider servicing more than 40,000 organizations, disclosed that it was the victim of a sophisticated cyberattack that is believed to have been orchestrated by REvil, a cybercriminal operation from Russia. This announcement came on the heels of several high-profile ransomware attacks during the COVID-19 pandemic. While federal laws exist to prohibit the payment of ransom to a threat actor, state legislatures also examined this issue in 2021:

New York

In New York, lawmakers proposed two bills. The first bill, SB 6806, prohibits "governmental entities, business entities and health care entities from paying a ransom in the event of a cyber ransom or ransomware attack," while the second, SB 6154, "relates to creating a cybersecurity enhancement fund and restricting the use of taxpayer money in paying ransoms." As of this writing, both bills were still in committee. SB 6806 was referred to committee on May 18 and SB 6154 was referred to committee on April 12.

North Carolina

North Carolina's HB 813 focused on public agencies and governmental entities. HB 813 would prevent these entities from paying threat actors to release information held for ransom. This bill would also clarify to agencies how they must coordinate with the state's Department of Information Technology. As of this writing, this bill had passed a second reading and went to committee on May 13.

Pennsylvania

Pennsylvania's SB 726 would "prohibit [state government agencies] from engaging in ransomware attacks and from extorting payments to resolve or prevent ransomware attacks." SB 726 would also require organizations to notify certain entities of an attack "within one hour of discovery" for managed service providers and "within two hours" for state agencies. As of this writing, the bill had been referred to committee on September 21.

Texas

Texas' HB 3892 would prohibit state agencies from making ransom payments related to a cyberattack. The bill also offers to broadly implement security and response plans for state agencies. For instance, the Department of Information Resources would be tasked with conducting a study "regarding cyber incidents and significant cyber incidents affecting state agencies and critical infrastructure" owned by the state. As of this writing, the bill had been referred to committee on March 24.

The goal of all of this legislation is to eliminate the financial incentive of a ransom payment to threat actors.

State AG Recommendations

State attorneys general also commented on the rise of ransomware attacks. For instance, on June 8, the Massachusetts attorney general's office released a report detailing the rise of ransomware attacks and stressing the importance of protecting data. The report warned that "[a]ll organizations, regardless of sector, size, or location, must recognize that no company is safe from being targeted by ransomware," and Attorney General Maura Healy "strongly encourage[d] all Massachusetts business and government organizations to take the appropriate steps to strengthen data security and ensure [their] computer networks are secure as required by law." For further analysis, please visit: https://www.consumerfinancialserviceslawmonitor.com/page/2/?s=notification.

Several other offices also issued guidance relating to information security, including as it relates to ransomware attacks:

- New Jersey Attorney General Josh Stein issued a column in July recommending that businesses take certain steps to protect their data from the rising threat of ransomware attacks, including installing antivirus and malware protection, only clicking on email links or attachments from people and companies that businesses are familiar with, protecting accounts by using unique and complex passports (as opposed to the same one repeatedly), and conducting regular backups of data. The column is available at https://ncdoj.gov/attorney-general-steins-july-column-protect-yourself-against-ransomware-attacks.
- Washington State Attorney General Bob Ferguson released his sixth annual Data Breach Report on November 5. The report stated that 2021 set the record for number of data breaches and ransomware attacks, with 6.3 million notices sent to residents, 280 data breaches reported, and 150 ransomware attacks reported. The report made several recommendations to lawmakers to enhance the protection of personal information, including expanding the definition of personal information to include Individual Tax Identification Number (ITINS) and redacted Social Security numbers (SSNs) that display the last four digits of an SSN. The report is available at https://agportal-s3bucket.s3.amazonaws.com/2021 Data Breach Report.pdf.
- North Dakota Attorney General Wayne Stenehjem issued a Ransomware Advisory in July urging businesses and government entities to assess data security practices and take steps to better protect operations and consumer data. Borrowing from a June memo issued by Anne Neuberger, deputy assistant to the president and deputy national security advisor for cyber and emerging technology, titled "What We Urge You To Do To Protect Against The Threat of Ransomware," the advisory recommends implementing certain practices such as "multifactor authentication (because passwords alone are routinely compromised), endpoint detection and response (to hunt for malicious activity on a network and block it), encryption (so if data is stolen, it is unusable) and a skilled, empowered security team (to patch rapidly, and share and incorporate threat information in its defenses)."

The report is available at https://attorneygeneral.nd.gov/consumer-resources/scam-prevention/ransomware-advisory.

- Michigan Attorney General Dana Nessel issued a consumer alert providing background and advice relating to ransomware, including her perspective as to why it may be a bad idea to pay a ransom demand. The alert also indicates that when it comes to protecting against ransomware, prevention is better than the cure. To this end, the alert includes several tips for businesses to protect against ransomware, including: (i) making sure all devices are protected with comprehensive security software; (ii) updating software often; (iii) installing reliable ransomware protection software; (iv) practicing safe surfing, i.e., being careful where you click; and (v) backing up data onto an external hard drive or cloud regularly. The alert is available at https://www.michigan.gov/ag/0,4534,7-359-81903_20942-324685--,00.html.
- California Attorney General Rob Bonta issued a Ransomware Bulletin in August to health care facilities and providers to remind them of their obligation to comply with state and federal health data privacy frameworks (like the California Confidentiality of Medical Information Act and the Health Insurance Portability and Accountability Act of 1996), which mandate appropriate procedures to ensure the confidentiality of health-related information, including security measures that can help prevent the introduction of malware, including ransomware, to protect consumers' health care-related information from unauthorized use and disclosure. This bulletin was issued after multiple ransomware attacks against California health care facilities went unreported. Bonta recommended several steps that entities can take to protect data, including keeping all operating systems and software housing health data up to date with the latest security patches; installing and maintaining virus protection software; providing regular data security training; restricting users from downloading, installing, or running unapproved software; maintaining regular data backups; and having a recovery plan in the event of a data security incident. The bulletin is available at https://oag.ca.gov/news/press-releases/attorney-general-rob-bonta-calls-full-compliance-state-health-data-privacy-laws.

U.S. Department of Labor

In a first for the department, the U.S. Department of Labor issued guidance for plan sponsors, plan fiduciaries, record-keepers, and plan participants on best practices for maintaining cybersecurity, including tips on how to protect the retirement benefits of America's workers. The guidance is directed at plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act, and at plan participants and beneficiaries. These tips include providing questions to help business owners hire a service provider with strong cybersecurity practices, advising recordkeepers to create a well-documented cybersecurity program, and reducing the risk of fraud and loss to retirement accounts by using multi-factor authentication for logins and routinely monitoring one's account. This guidance, available at https://www.dol.gov/newsroom/releases/ebsa/ebsa20210414, seeks to help protect an estimated $9.3 trillion in assets.

New York Department of Financial Services

In February 2021, the New York Department of Financial Services (NYDFS) issued guidance aimed at all authorized property/casualty insurers. The guidance provides best practices to manage cyber insurance risk sustainably and effectively. These best practices include establishing a formal cyber insurance risk strategy, managing, and eliminating exposure to silent cyber insurance risk, evaluating systemic risk, rigorously measuring insured risk, educating insured and insurance producers, obtaining cybersecurity expertise, and requiring notice to law enforcement. NYDFS emphasizes the recent growth in cybercrime — especially considering the COVID-19 pandemic — and the important role insurers play in mitigating and reducing the risks of cybercrime. NYDFS also recommends against paying ransom payments, which it contends "fuels the vicious cycle of ransomware" and does not guarantee that an organization will get its data back or that criminals will not use that stolen data in the future. Notably, NYDFS is the first U.S. regulator to issue specific guidance for property/casualty insurers writing cyber insurance. The guidance is available at https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02#_edn23.

Department of Justice

On October 6, the Department of Justice (DOJ) announced two new initiatives: the Civil Cyber-Fraud Initiative (the Initiative) and the National Cryptocurrency Enforcement Team (NCET). These programs focus on monitoring contractor cybersecurity, and combating cryptocurrency used for illicit purposes. The Initiative will use the existing False Claims Act against government contractors and grant recipients that fail to implement sufficient cybersecurity protection. This tool has been used by the government to redress fraudulent claims for federal funds in the past and includes provisions that allow whistleblowers to share in any recovery. The Initiative seeks to hold accountable entities when they: (1) knowingly provide deficient cybersecurity products or services; (2) knowingly misrepresent their cybersecurity practices or protocols; or (3) knowingly violate obligations to monitor and report cybersecurity incidents and breaches. For more information, visit https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

NCET will tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors. NCET will also work with other divisions, such as the Department of Justice Criminal Division's Money Laundering and Asset Recovery Section, Computer Crime, and Intellectual Property Sections among other sections. The head of the NCET will report to the assistant attorney general in the Criminal Division. The team will also assist in tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups.

Infrastructure Information Security

In the United States, high-profile infrastructure-related data security incidents have led to increased federal scrutiny. These incidents include attempted attacks on water treatment facilities in California and Nevada. President Biden signed an executive order aimed at enhancing U.S. cybersecurity practices and protecting federal government systems. The order calls for collaboration between the federal government and the private sector to confront "persistent and increasingly sophisticated malicious cyber campaigns" that threaten U.S. security. Some specific steps the executive order highlights include: (i) creating a standardized playbook for federal responses to cyber incidents; (ii) establishing a "Cybersecurity Safety Review Board" of public and private-sector officials, which should convene after major cyber-attacks to provide analysis and recommendations; and (iii) improving the security of software sold to the government, including by requiring developers to share certain security data with the public. The order is available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity. In October, President

Biden met with representatives from 30 countries to discuss the risks associated with increased ransomware attacks, and nearly $2 billion of Biden's infrastructure bill is aimed at improving data security.

Multiple bills in Congress are aimed at creating additional reporting obligations for infrastructure-related data security incidents. One such bill is the bipartisan Cyber Incident Notification Act of 2021, which would require some businesses (such as those involved in the provision of financial services, health care, and utilities) to report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours. A similar measure was incorporated into the House annual defense policy package. Of course, these federal obligations would likely be imposed in addition to existing state-level breach notification requirements.

Changes to Breach Notification Statutes

Without a national security breach notification law, all 50 states have enacted legislation requiring businesses, and sometimes government entities, to notify certain individuals/regulators of a "breach" compromising personal information. Several amendments to state and federal notification rules during the past year are noteworthy.

HIPAA

On September 15, the FTC issued a statement affirming that mobile applications dealing with health information or other connected devices that collect health information "must comply with the [Health Insurance Portability and Accountability Act's (HIPAA)] Health Breach Notification Rule[.]" HIPAA's Health Breach Notification Rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information. Much of the information now collected by health-focused mobile applications includes glucose levels, heart health, and sleep cycles. The FTC's statement is of particular importance for developers thinking about collecting vaccine status information for verification purposes; for further analysis on these privacy issues, please visit Troutman Pepper's *Law360* article: https://www.law360.com/articles/1352956.

Arkansas (Ark. Code Ann. § 10-4-429)

Under this amendment, data breach notification obligations now apply to state entities, including subdivisions and schools. The amendment follows the same definition of personal information as to its general data breach notification law. The update to the law also requires public entities to report data security incidents to an auditor within five (business) days after confirmation of an incident.

Connecticut (Conn. Gen. Stat. § 36a-701b)

Connecticut amended its breach notification statute to broaden the definition of personal information to include medical information, passport data, and other government-issued cards. Importantly, the notice deadline has been shortened from 90 days to 60 days. The amendment also requires businesses to provide 24 months of complimentary credit identity theft prevention to individuals with an impacted Social Security number or tax identification number.

Mississippi (Miss. Code § 75-24-29)

Mississippi amended its notification law to expand the definition of "personal information" to include valid and current tribal identification cards issued by a federally recognized Indian tribe. The amendment did not modify the notice deadline.

Oregon (H.B. 2128)

Oregon expanded its breach notification requirement to include tax professionals. Tax professionals are now required to report an event of a breach of security if the breach is associated with tax return preparation. Notification of a confirmed breach is due within five days to the Oregon Department of Revenue.

Texas (Tex. Bus. & Com. Code § 521.053)

Texas amended its breach notification law to require the Texas attorney general's office to post a list of notifications it receives when a breach affects at least 250 Texans on its website. These entities must include the number of impacted residents notified. The Texas attorney general can remove a notification after a year if no additional breaches have been reported by the entity.

Non-regulatory governmental bodies and industries across sectors are attempting to better inform business leaders of proper security.

Insurance-Specific Breach Notification Updates

The National Association of Insurance Commissioners (NAIC) adopted the Insurance Data Security Model Law (#668) in 2017 in response to high-profile data breach of insurers and other institutions. The model requires insurers and other entities licensed by state departments of insurance to develop implement and maintain an information security program, investigate any cybersecurity events, and notify the state insurance commission of such events.

By 2019, the NAIC Insurance Data Security Model law had been adopted in 11 states: Michigan; Indiana; Ohio; Virginia; Louisiana; Mississippi; Alabama; South Carolina; New Hampshire; Delaware; and Connecticut. In 2020, Hawaii, Maine, Tennessee, and Wisconsin also followed suit. For further analysis on the NAIC model law and how its requirements compare to New York's Cybersecurity Regulations, which also apply to insurance entities, please visit: https://www.consumerfinancialserviceslawmonitor.com/2021/11/wisconsin-enacts-insurance-data-security-law-requiring-notification-of-cybersecurity-incidents-to-insurance-commissioner-within-three-business-days.

Industry Guidance on Information Security

It is not just regulatory agencies and legislatures that are attempting to find solutions and provide guidance relating to information security. Non-regulatory governmental bodies and industries across sectors are attempting to better inform business leaders of proper security. We discuss guidance updates made by such entities in 2021:

NIST Guidance Updates

The National Institute of Standards and Technology (NIST) offered examples for implementing the Framework for Improving Critical Infrastructure Cybersecurity (known as the Cybersecurity Framework) in a manner that complements the use of other NIST security and privacy management standards and practices. For those interested in reading the full highlights, please visit https://www.nist.gov/publications/approaches-federal-agencies-use-cybersecurity-framework-0. Earlier in 2021, NIST also offered organizations methods for improving their phishing detection. The "Phish Scale" is a method for rating the difficulty of human phishing detection, which NIST described as the understanding variability in phishing click rates. To read more about the method, please visit https://www.nist.gov/publications/nist-phish-scale-method-rating-human-phishing-detection-difficulty.

CIS Top 18

The Center for Internet Security (CIS) had previously released a set of prioritized actions aimed at protecting organizations and data from known cyber-attack vectors, called the CIS Critical Security Controls (CIS Controls). The CIS Controls previously contained 20 critical structure controls, but in 2021, CIS released version 8 of the CIS Controls, which made significant updates to the controls' organization and priorities. For instance, version 8 consolidated and combined the prioritized actions by the activities themselves, rather than by who manages devices for information security-related activities. Further, CIS consolidated activities relating to physical devices and fixed boundaries, while it added cloud and mobile technologies. The updated controls now contain 18 rather than 20 prioritized actions. For those interested in learning more about the 18 CIS controls, please visit https://www.cisecurity.org/controls. This change is relevant for businesses (especially those doing business in California) seeking to adopt "reasonable security procedures" since the California attorney general's office provided its view that the Top 20 CIS Controls represent the "minimum level of information security that all organizations that collect or maintain personal information should meet." This suggests that such controls represent the baseline for "reasonable security procedures and practices," at least in California.

Notable Litigation/Settlements in 2021

2021 set the record for number of data breaches in a year. These data breaches have affected many types of industries, from large corporations to video conferencing platforms and grocery chains. In turn, this has spawned class action litigation and settlements. Here are notable ones from the past year.

On June 3, in *Shiyang Huang v. Equifax Inc.* (*In re Equifax Customer Data Sec. Breach Litig.*), 999 F.3d 1247 (11th Cir. 2021), a $425 million settlement over the 2017 Equifax data breach was upheld in the Eleventh Circuit. The Equifax data breach had compromised the private records of 147.9 million Americans, along with 15.2 million British citizens, and about 19,000 Canadian citizens. In January 2020, a Georgia federal judge approved the settlement, that included $380.5 million in class members' benefits, compensation for class members who already had credit monitoring, and $1 billion on data security over five years. Out of the estimated 147 million class members, 388 objected to the settlement. The Eleventh Circuit approved the settlement despite these objections.

On October 21, in *In Re: Zoom Video Communications Inc. Privacy Litigation*, No. 5:20-cv-02155, a California federal judge preliminarily approved an $85 million deal in a putative class action alleging Zoom of unlawfully sharing personal data with unauthorized third parties. The action also accused Zoom of misrepresenting the strength of its encryption protocols and failing to stop malicious meeting disruptions, which came to be known as "Zoombombings." Under this deal, users with paid subscriptions will be eligible to receive the greater between 15% of their subscription costs during the class period or $25. Zoom also agreed to improve security, privacy disclosures, and consumer data protection through over a dozen major changes to its practices. These changes will include specialized employee training, alerting users when hosts or other participants use third-party applications during a meeting, and ensuring its privacy statement discloses users' ability to record or transcribe meetings or share data with third parties.

In the summer of 2021, a settlement arose out of a breach suffered by Accellion, a technology company that provides secure file-sharing services. The hack, which arose out of an outdated file transfer product, affected institutions around the world, including the Bank of New Zealand, Harvard Business School, Washington's state auditor, and two large U.S. law firms.

One potential settlement involves a bank's agreement to pay a $5.9 million settlement after it was accused of putting 1.48 million customers' data at risk by using Accellion. As a result of the breach suffered by Accellion, bank account information, Social Security numbers, and passport details, among other information, were exposed.

One proposed settlement is *Ricky Cochran et al. v. The Kroger Co. et al.*, No. 5:21-cv-01887 (N.D. Cal. 2021). On June 30, a California federal court announced preliminary approval of a $5 million settlement, which would end a putative class action suit on behalf of Kroger customers. If approved, the grocery store chain will pay a cash payment on average of about $91 for non-California resident class members, and $181 for California resident class members. Instead of cash payments, claimants could elect to receive two years of credit monitoring and insurance services, or a payment for reimbursement of documented losses of up to $5,000. Kroger must also confirm it has migrated to a new file transfer system. Lastly, Kroger must monitor the dark web for indications of fraudulent activity with respect to data of Kroger customers and current and former employees in connection with the data breach, for five years.

On May 17, 2021, the New York attorney general reported a settlement agreement with Filters Fast LLC, over a data breach that compromised the personal information of 324,000 consumers nationwide. Filters Fast is an online air and water filter retailer. The breach allowed the attacker to collect the names, billing addresses, and primary account numbers of customers who purchased products with their credit cards, and associated expiration dates. Under the settlement, Filters Fast is required to pay the state of New York $200,000; execute and enforce systems and security measures to prevent future data breaches; create a security program to ensure regular updates and reports to Filters Fast's CEO; execute

an incident response and data breach notification plan to identify, contain, eradicate, and recover from breaches; and ensure that third-party security assessments take place over the next five years.

On January 15, the Department of Health and Human Services (HHS) announced a settlement with Excellus Health Plan, Inc., over a data breach that affected 9.3 million people. Excellus Health Plan provides health insurance coverage to over 1.5 million people in Upstate and Western New York. The Office of Civil Rights investigation found that there were potential violations of HIPAA, including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, information system activity review, and access controls. Per the HHS, this incident involved "hackers installing malware and conducting reconnaissance activities that ultimately resulted in the impermissible disclosure of the protected health information . . . including names, addresses, dates of birth, email addresses, Social Security numbers, bank account information, health plan claims, and clinical treatment information." Excellus has agreed to pay $5.1 million and will implement a corrective action plan that includes two years of monitoring.

Developments in Data Breach Class Actions and Multidistrict Litigation

As data breach incidents continue to grow, so does class-action litigation stemming from those incidents. Historically, most data breach class actions settle before the parties litigate class certification. However, in 2021, we saw some key decisions that litigators should know about when litigating data breach claims in either a class action or multidistrict litigation (MDL).

The Judicial Panel Sets Limitations for Consolidation of Data Breach Cases

In many data breach class actions, a decisive threshold issue is whether to consolidate the cases into a MDL. The MDL process permits centralization of related disputes in front of a single federal court and is designed to promote consistency and efficiency by resolving similar claims and disputes in front of one judge. However, in 2021, the Judicial Panel for Multidistrict Litigation (JPML) appears to have set a size threshold for data breach MDLs when it denied Geico's attempt to consolidate five class-action lawsuits.

In April 2021, Geico suffered a data breach that reportedly impacted over 132,000 individuals. Geico determined that approximately 85% of those individuals lived in New York. In response to the breach, the plaintiffs filed five putative class-action lawsuits: three in New York, one in Maryland, and one in California. In June, Geico attempted to consolidate the class actions into an MDL, arguing that each of the five cases shared the same factual basis and common legal issues.

The JPML denied Geico's motion because "centralization [was] not necessary for the convenience of the parties and witnesses or to further the just and efficient conduct of [the] litigation." While the JPML found that the five cases share common questions of fact, the JPML held that Geico failed to meet its burden that centralization was appropriate because "informal coordination among the small number of parties appear[ed] eminently feasible."

Court Stays Discovery in Data Breach MDL to Resolve Standing Issue

A district court judge in the Southern District of Florida paused a data breach MDL to allow the court to decide the defendant's motion to dismiss for lack of standing and failure to plead a cognizable claim. In *In Re Mednax Services*, a health care provider defendant suffered a data breach that exposed patient information of approximately 1.3 million individuals. The plaintiffs claim that the defendants' insufficient cybersecurity procedures caused the breach, and the defendant's inadequate response to the breach resulted in additional harm to the plaintiffs.

In August 2021, the plaintiffs combined all claims into one consolidated complaint. The defendants then moved to dismiss all of the plaintiff's claims under Rule 12(b)(1) for lack of standing and Rule 12(b)(6) for failure to state a claim. The defendants simultaneously moved to stay discovery. The defendants argued that, under Eleventh Circuit law, discovery should be stayed when a defendant makes a facial challenge to the allegations set forth in the complaint to promote judicial efficiency,

and such a stay would not prejudice the plaintiffs. In opposition, the plaintiffs argued that stays of discovery are the exception, not the rule, and that class members continue to face increasing risk from the defendant's allegedly deficient cybersecurity procedures.

In granting the stay, the court found that "significant questions exist[ed] regarding Article III's injury-in-fact and traceability requirement." And if the defendants succeeded on the motion to dismiss, "it would substantially impact the viability of claims against one or more [d]efendants and drastically alter the scope of discovery." For these reasons, the court stayed discovery, explaining that the defendants "should not be forced to expend substantial resources responding to discovery given the jurisdictional and facial challenges pending before the [c]ourt."

Individual Issues Concerning Causation and Damages Continue to Present a Hurdle to Class Certification in Data Breach Class Actions

Class certification has only been litigated in a small portion of the filed data breach class actions. However, a common theme in data breach class certification decisions is that the individual issues of causation and damages predominate over the common issues of whether the defendant's cybersecurity procedures or breach notification efforts were deficient. The January 2021 decision in *McGlenn v. Driveline Retail Merchandising, Inc.* was no exception.

There, a district court judge declined to certify a class of employees whose personal information was disclosed when Driveline fell prey to a phishing scam. In January 2017, a scammer — posing as Driveline's CFO — asked a payroll employee to email him 2016 W-2s for all of Driveline's employees. In response, the payroll employee emailed him 15,878 W-2 forms, all of which contained employees' names, addresses, Social Security numbers, and wage information. A former Driveline employee, plaintiff Lynn McGlenn, filed a class action against Driveline, alleging that the breach caused her personal information to be stolen and used to open a fraudulent credit card account. In her class certification motion, McGlenn sought to certify a class of "all current and former Driveline employees" whose personal information was compromised by the scam.

The court denied McGlenn's motion for class certification, finding that establishing the required elements of causation and damages required individualized evidence, and thus, McGlenn failed to satisfy Rule 23's requirements of commonality and predominance. The court explained that McGlenn

could not prove causation with common evidence because "several Driveline employees likely had been involved in other data incidents in the two to four years prior to" the phishing scam. Moreover, even employees who could tie their alleged injury to the phishing scam would encounter a significant legal hurdle because the applicable law (Illinois) did not impose a common law duty on Driveline to safeguard information. The court further held that the class members' alleged "risk of harm" was not sufficient to establish Article III standing.

CCPA Litigation

On August 6, 2021, in *Burns v. Mammoth Media, Inc.*, No. 2:20-cv-04855-DDP (C.D. Cal.), a court in the Central District of California dismissed a data breach putative class action for lack of standing, notwithstanding evidence that the stolen data of 40 million consumers had allegedly been offered for sale on the dark web. The court determined that the data breach could not possibly have caused a risk of identity theft, fraud, and attendant harms given the "essentially useless" nature of the data. For further analysis on this case, please visit: https://www.consumerfinancialserviceslawmonitor.com/2021/08/no-standing-in-data-breach-case-involving-essentially-useless-stolen-data.

A California magistrate judge refused to dismiss a class action against a popular stock trading platform. Plaintiffs allege the platform failed to maintain industry standard security, leading to 2,000 customers' funds and personal information being accessed without authorization. The judge held plaintiffs had adequately pled a claim for violations of the CCPA, which allows consumers to seek statutory damages for data breaches that result from a company's alleged failure to implement reasonable security procedures.

On October 4, a group of retailers pushed to dismiss a putative class action lawsuit alleging violations of the CCPA. The case, which was initially filed in 2020 against multiple retailers and their service provider, is *Shadi Hayden vs. The Retail Equation et al.* No. 8:20-cv-01203. On a motion to dismiss, the retailers argued, among other things, that (i) the alleged violations took place before the CCPA took effect, and the CCPA does not apply to conduct before that date; and (ii) the alleged violations do not amount to a "data breach" under California's breach notification law, and therefore the CCPA's private right of action provision does not apply.

In *Gardiner v. Walmart, Inc.*, No. 4:20-cv-04618, a court dismissed a putative class action in a purported "data breach." This action contained key holdings on multiple issues of first impression that have been raised in recent data breach actions. These key holdings include a dismissal based on plaintiff's attempt to base his CCPA claim on an alleged breach that occurred before January 1, 2020, the date the CCPA became effective, and dismissal of a UCL claim that was predicated on the CCPA. For further analysis, please see: https://www.troutman.com/insights/california-court-tosses-alleged-data-breach-suit-holding-ccpa-does-not-apply-retroactively.html.

BIPA Litigation

Since the enactment of the Illinois Biometric Privacy Act (BIPA) in 2008, it has been a steady source of litigation. Last year was no exception, with caselaw around statute of limitations and standing. Several BIPA cases also settled, including the second-highest settlement in BIPA history.

On September 17, a three-judge panel of the Illinois Appellate Court for the First Judicial District issued a highly anticipated decision regarding the statute of limitations for claims under BIPA. In *Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st) 200563, the court considered which limitation period should apply to BIPA claims: a five-year "catch all" limitation period set forth in Illinois' Code of Civil Procedure, 735 ILCS 5/13-205 or the one-year limitation set forth in 735 ILCS 5/13-201. The court ultimately decided that claims under BIPA Sections 15(e) and (d) are subject to the one-year limitation period, while BIPA sections 15(a), (b), and (e) enjoy the longer five-year limitation period. BIPA, itself, did not specify a limitations period. For further analysis on the impacts of this case, please visit: https://www.troutman.com/insights/hoping-for-a-one-year-statute-of-limitations-under-illinois-bipa.html.

The U.S. Court of Appeals for the Seventh Circuit issued a decision in *Fox v. Dakkota Integrated Sys., LLC*, 2020 WL 6738112 (7th Cir. Nov. 17, 2020),

which clarified an unanswered question regarding standing: Does an alleged failure to comply with a retention schedule for biometric data, as required by Section 15(a) of BIPA, without more, suffice to plead an injury in fact for purposes of Article III? The court answered that it does, bolstering standing for litigants alleging BIPA violations. In *Fox*, plaintiff alleged that her former employer, Dakkota, required its employees to scan their hands when clocking in and out of work. She alleged the company failed to maintain a retention schedule for the biometric data and failed to destroy her biometric data when she left the company, in violation of Section 15(a) of BIPA.

In *Kowalski v. American Airlines, Inc.*, No. 1:17-cv-09080, putative class members (who are customers of American Airlines) allege American Airlines violated Section 15(a) of BIPA by failing to create publicly available biometric retention and destruction schedules and are seeking to sever and remand their claim back to state court. On July 27, the court heard arguments on this point. The action was first filed in state court in 2017, but American Airlines removed the case to federal court in December of that year. Currently, standing under Section 15(a) remains murky at the federal level. While Illinois state courts have unequivocally allowed for standing under BIPA without evidence of actual harm following *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, 432 Ill. Dec. 654, 129 N.E.3d 1197, federal courts are less keen to allow cases where a plaintiff did not suffer a "concrete" harm.

On September 14, the Seventh Circuit heard oral arguments in a highly watched case, *Cothron v. White Castle*, No. 20-3202 (7th Cir.). In *Cothron*, the plaintiff alleged her employer, White Castle, violated BIPA by failing to obtain employee consent when collecting biometric information through a system that allowed employees to sign documents and access paystubs with their fingerprints. The system was implemented in 2007 – before BIPA was enacted – and the plaintiff claims she only gave consent to the collection of her data in 2018. The plaintiff alleges the ongoing collection of her information – over 11 years – violates Section 15(b) and 15(d) of BIPA. The court will consider whether a BIPA violation occurs only upon the initial unlawful collection of biometric information, or each time the information is collected (e.g., whether a violation occurs solely the first time one's fingerprints are scanned, or whether there is a separate BIPA violation for each subsequent scan).

Clearview AI argued that BIPA violates the First Amendment by inhibiting the company's ability to use public information in its search engine. The court dismissed this argument.

On August 27, in *American Civil Liberties Union et al. v. Clearview AI Inc.*, No. 2020-CH-04353, a Cook County circuit judge ruled that Clearview AI cannot use the First Amendment to avoid suit under BIPA. Clearview AI is a facial recognition company that collects billions of images from public platforms, such as Facebook, and puts them into a database that allows users to identify someone based on an uploaded photograph. Clearview AI argued that BIPA violates the First Amendment by inhibiting the company's ability to use public information in its search engine. The court dismissed this argument. This case is expected to have wide-reaching impact on the protections granted to information amassed from publicly accessible sources.

On June 25, Mary Kay Cosmetics, Inc., was hit with a proposed class action alleging illegal scans and use of plaintiff's facial geometry without their informed consent in *Marvalace Garrett v. Mary Kay Cosmetics, Inc.*, No. 2021-CH-03124. On June 24, in *Fiza Javid v. Ulta Beauty Inc.*, No. 2021-Ch-03109, cosmetic store Ulta Beauty was also hit with a proposed class action regarding its facial scans, which allow a consumer to virtually try on makeup. Both lawsuits, filed by separate plaintiffs, allege that the companies fail to inform consumers about the purposes or length of time biometric facial data is collected, and fail to have a publicly available policy governing data collection, storage, and destruction practices. In the past, Sephora was sued for its

virtual make-up kiosks in 2018 in *Salkauskaite, et al. v. Sephora USA, Inc.*, No. 2018-CH-14379 (Cir. Ct. Cook Cnty., Illinois). In this class action, plaintiff alleged Sephora disseminated her biometric information to sell her products without informing her that her biometrics were being collected, stored, used, or disseminated. Sephora later settled, and final approval for the settlement, including a $1.25 million settlement fund, was granted on June 23, 2021. These lawsuits represent a growing trend in "face print" lawsuits under BIPA.

On January 26, in *Campana v. Nuance Communications, Inc.*, No. 2021-CH-00374, defendant Nuance Communications, was sued for alleged violations of BIPA. The proposed class action alleges that Nuance's interactive voice recognition, used by companies to handle extremely large call volumes, "collects and analyzes callers' actual voiceprints" to understand the caller's request and automatically responds with a personalized response instead of a menu list. The complaint alleges that this collection violates BIPA. Notably, BIPA requires entities collecting biometric information to: (i) inform the owner of the information in writing; and (ii) obtain written consent. 740 ILCS 14/15(b). Compliance with these sections would be extremely difficult in a telephone context. Since a number of companies use Nuance's software, such as FedEx, such companies may face exposure for such use in the future.

On May 28, in *Carpenter v. McDonald's Corporation*, No. 1:21-cv-02906, a class action was brought against McDonald's alleging the fast-food restaurant had stored customers' voiceprints without their permission. McDonald's employs an AI voice assistant, which consumers interact with when placing an order. The complaint alleges this technology "extracts" information on the consumer such as age, gender, national origin, and accent, from their voiceprint.

BIPA Settlements

On September 30, in *In Re: TikTok Inc. Consumer Privacy Litigation*, No. 1:20-cv-04699, an Illinois federal judge approved a $92 million settlement resolving biometric and other data privacy related claims against TikTok. Several members of the class objected over its value; however, the judge found the deal to be fair. The settlement ends more than 20 proposed class actions alleging TikTok failed to inform users that its facial recognition technology collects and stores biometric identifiers. The purported class actions also allege that TikTok failed to obtain written permission before this collection, as required by BIPA and other state and federal privacy laws. In addition to funding the $92 million settlement fund, TikTok agreed not to use its app to collect users' biometric data, geolocation or GPS data; transmit U.S. user data outside the U.S.; or store user data in databases outside the U.S. The parties settled after two mediation sessions as President Trump ordered ByteDance – the parent company of TikTok – to sell TikTok's U.S. operations. This is the second-largest settlement in the history of BIPA.

On September 2, an Illinois state judge approved a $5.85 million settlement between owners of almost 40 Wendy's restaurants and their employees in *O'Sullivan v. WAM Holdings, Inc.*, No. 19-CH-11575. The employees had alleged the company collected fingerprint data to track their work, in violation of BIPA, because their fingerprints were collected when clocking in and out. Under the settlement, each class member will receive a net amount of $384, and each lead plaintiff will receive $7,500.

Shutterfly, the photo-sharing company, will pay $6.5 million to end claims that it stored Illinois residents' biometric data from its facial-recognition technology without obtaining consumers' consent. In *Miracle-Pond et al. v. Shutterfly Inc.*, No. 1:19-cv-04722, plaintiffs allege that facial recognition was used to collect their biometric data without their consent, and that the company did not make its biometric policies readily available to users, as required by law. An estimated 950,000 Illinois residents are included in the class. The settlement was filed on February 18.

Topgolf, the popular entertainment venue and sports bar, will pay $2.6 million to settle a BIPA lawsuit. In *Burlinski v. Top Golf USA Inc.*, No. 1:19-cv-06700, former employees alleged the company violated BIPA when it collected employees' fingerprint data and distributed this data to its timekeeping vendor without receiving informed consent. The named plaintiffs filed a motion for preliminary approval of the settlement on June 4.

The proposed 2,660-member class will lead to an estimated net recovery of $630 per person.

On June 14, in *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186, Six Flags agreed to a $36 million settlement in a proposed class action, which alleged it collected the biometric information of its passholders' without obtaining prior consent. In 2019, the Illinois Supreme Court unanimously ruled that plaintiffs could bring claims for BIPA violations without alleging a separate real-world harm. The proposed class consists of individuals who visited Six Flags Great Adventure in Gurnee, Illinois, between October 1, 2013, and December 13, 2018.

On April 16, Heartland Employment Services LLC, a nursing and rehabilitation care company, agreed to pay $5.4 million to former employees who claimed the company's fingerprint collection violated BIPA. In their complaint, originally filed in 2018 in Illinois state court and later removed to federal court, the employees alleged that Heartland collected their fingerprints without first receiving written consent and explicitly disclosing the collection. Under the agreement, Heartland is not required to admit fault or liability.

Additional Developments in Case Law

The case law around cybersecurity and data privacy continues to evolve, especially as it concerns Article III standing, privilege, and contract interpretation. Here are a couple noteworthy cases from last year.

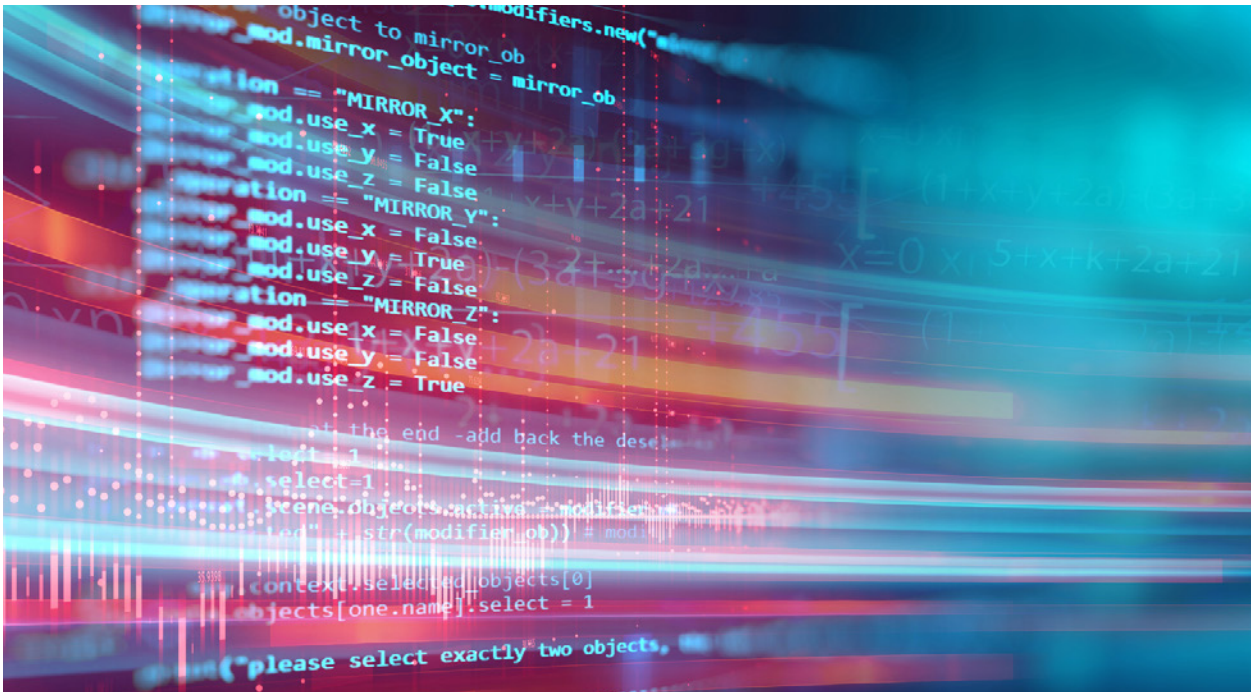
On January 12, in *Rahman v. Marriott International, Inc.*, No. 8:20-cv-00654, the U.S. District Court for the Central District of California dismissed data breach claims against Marriott for lack of subject matter jurisdiction, finding that the data compromised was not sensitive information as required by the Ninth Circuit to establish injury-in-fact for Article III purposes. The complaint alleged that class members were victims of a cybersecurity breach when two members of a Marriott franchise in Russia accessed class members' names, addresses, phone numbers, email addresses, genders, birth dates, and loyalty account numbers without authorization. Marriott confirmed that while names, addresses, and other publicly available information were obtained in the breach, no sensitive information (such as Social Security numbers, passport numbers, or credit card information) was accessed. In dismissing the complaint, the court reaffirmed that absent disclosure of sensitive information, there was no credible risk of identity theft creating risk of real and immediate injury. As a result, the plaintiff had not established standing under Article III.

In *Landry's Inc. v. Ins. Co. of the Pa.*, No. 19-20430, 2021 U.S. App. LEXIS 21668 (5th Cir. July 21, 2021), the U.S. Court of Appeals for the Fifth Circuit held that the meaning of "publication" in the context of a privacy-related commercial general liability policy included dissemination of information to a single person. The court determined that an insurance carrier had a duty to defend its insured against data breach liability when the policy included coverage for injury arising out of "[o]ral or written publication, in any matter, of material that violates a person's right of privacy." The Fifth Circuit ruled that because the liability policy included "oral or written publication, in any manner," the term "publication" must include dissemination of information to a single person.

Privilege in Incident Response

The attorney-client privilege and the work product doctrine are two related but distinct doctrines to protect information that is shared with legal counsel from future disclosure. The attorney-client privilege protects communications to and from one's attorney(s) (and their delegates) for the purpose of seeking legal advice, while the work product doctrine protects materials prepared by an attorney—or the agents of an attorney—in anticipation of litigation. In the context of cybersecurity investigations, these two protections often overlap. Some people tend to group these two protections together and treat them interchangeably, but the distinct purposes, origins, and tests for these two protections inform the unique methods that must be employed to assert them during the life of cyber investigations and any subsequent litigation.

2021 provided several updates in the evolving legal landscape regarding the attorney-client privilege and work product doctrine in the context of incident response. Two notable cases are described below.



In *Guo Wengul v. Clark Hill, PLC*, 338 F.R.D. 7 (D.D.C. 2021), the plaintiff moved to compel production of incident response related documents, including a report produced by an external security-consulting firm, Duff & Phelps. Clark Hill claimed to have used a dual-track response system, modeled after the one used after the Target Corporation data breach, where one task force (eSentire) works to investigate the incident and preserve business continuity and another task force (Duff & Phelps) is engaged to assist in counsel providing legal advice. Clark Hill produced the eSentire report but held onto the Duff & Phelps report.

On January 12, the court held that the work product doctrine was inapplicable here because, unlike in the Target Corporation data breach response, there was nothing in the record supporting the claim that the two separate reports were dual-track or that eSentire produced a similarly comprehensive report such as the Duff & Phelps report. Furthermore, Clark Hill shared the Duff & Phelps report with leadership, the IT department, and used it in connection with managing various issues not limited to potential litigation. As such, the court found the report to be prepared in the ordinary course of business, irrespective of litigation, and not protected under the work product doctrine.

The court further held that attorney-client privilege was not applicable because Clark Hill sought Duff & Phelps' cybersecurity advice with this report, not their outside counsel's. The court found the fact that the Duff & Phelps report was the only full-scale report produced, that the report contained recommendations on how to improve cybersecurity practices, and that the report was shared with the IT department and FBI to support the conclusion that the report was not intended to obtain legal advice.

A judge compelled disclosure of a report prepared by a cybersecurity vendor that had been hired by a law firm. This law firm was hired by their client on the day of a suspected incident. There was an understanding between the vendor and outside counsel that the investigation would be privileged. However, the judge compelled disclosure after determining the behavior between the vendor, law firm, and client, did not support this belief.

Regulatory Enforcement

State and federal actors focused on cybersecurity and new technologies in 2021, from issuing guidance to enforcement actions. This focus will likely continue into 2022.

FTC Consent Agreements

On February 5, the FTC finalized a settlement with a Nevada-based company that provides travel emergency services. In 2019, SkyMed experienced a data breach that exposed consumer data. After an investigation, in December 2020, the FTC had alleged SkyMed failed to take reasonable steps to secure sensitive customer information including certain health records. The complaint alleged that this unsecured information was stored in a database, and contained members' information such as names, dates of birth, home addresses, health information, and membership account numbers. Moreover, the FTC also alleged that SkyMed deceived customers by displaying a "HIPAA Compliance" seal on every page of its website, implying that its privacy policies met the security and privacy requirements under HIPAA. Under the settlement, SkyMed must provide notice to every customer affected by the 2019 data breach, implement a comprehensive information security program, and obtain biennial assessments of this program by a third party. The settlement also prohibits the company from misrepresenting how it secures personal data, the circumstances of and response to any future data breach, and whether SkyMed has been endorsed by or participates in any government-sponsored privacy or security program.

On June 22, the FTC announced it had settled a case with Flo Health, Inc., an app that allows users to track their period and ovulation cycle. In January 2021, the FTC alleged that the company had shared sensitive health data from millions of users with marketing and analytics firms, including Facebook and Google, despite promising to keep users' health data private. Under the settlement, Flo Health must notify all affected users about the disclosure of their health information and instruct any third party that received users' health information, to destroy that data. The company is also prohibited from misrepresenting the purposes for which it collects, maintains, uses, or discloses the data, how much consumers can control the data, its compliance with privacy, security, or compliance programs, and how it collects, maintains, uses, or discloses users' personal information.

On May 7, the FTC finalized a settlement with California-based photo app Everalbum over allegations that it was building a facial recognition technology using users' photos and videos, without their express consent. The FTC also alleged that Everalbum failed to destroy the photos and videos of users who deactivated their accounts, despite promising to do so. Under the settlement, the FTC will require Everalbum to clearly and conspicuously disclose to all its users all the purposes for which Everalbum will use and share biometric information, obtain the affirmative consent of users who upload biometric data, destroy all photos and videos from users who deactivated their Ever accounts, destroy all facial mappings derived from users who did not provide their express affirmative consent; and destroy any methods or algorithms developed in whole or in part using the biometric information collected from users of the Ever application. For further analysis on this FTC claim, please visit: https://www.consumerfinancialserviceslawmonitor.com/2021/01/photo-storage-app-agrees-to-erase-biometric-data-to-resolve-ftc-claims.

FTC Guidance on AI Technology

On April 19, the FTC released guidance on the use of artificial intelligence (AI) technology, and specifically its use in health care delivery and its potential to exasperate existing racial biases. The guidance begins with reminding developers and users of AI that the FTC has traditionally enforced three laws in relation to AI: (1) Section 5 of the FTC, which prohibits unfair or deceptive practices; (2) the Fair Credit Reporting Act when an algorithm is used to deny people employment, housing, credit, insurance, or other benefits; and (3) the Equal Credit Opportunity Act when a biased algorithm that results in credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or because a person receives public assistance. To avoid discrimination, the FTC recommends using a comprehensive data set when building algorithms, which includes designing your model to account for data gaps and limiting where or how you use the model. The other recommendations include looking for discriminatory outcomes, embracing transparency and independence, being truthful on whether your algorithm can deliver fair or unbiased results, and truthful in how you use data.

This year, many of the FTC's efforts have been focused on privacy concerns and addressing technologies that exacerbate existing racial inequalities.

FTC Bans

On September 1, the FTC announced a permanent ban on the surveillance app SpyFone for secretly harvesting and sharing real-time data on people's physical movements, phone usage, and other online activities. The app is operated by Support King LLC, and is designed to intercept phone activities like texts, calls, emails, web histories, and location information. The FTC ordered the company to delete all illegally harvested information. This is the second case by the FTC against "stalkerware" apps, and the first time the agency is banning a company. The FTC alleges the app failed to ensure people were using the app for legitimate purposes and didn't protect information it collected. This failure allowed stalkers or domestic abusers to surreptitiously download the app on an individual's phone and stealthily track their potential targets. This also exposed device owners to hackers, identity thieves, and other threats online.

FTC's Future Enforcement Efforts

Last year, many of the FTC's efforts have been focused on privacy concerns and addressing technologies that exacerbate existing racial inequalities. The agency has focused on the increased use of health apps, videoconferencing, education technology, and the accuracy of data used for housing, employment, and credit. In this pursuit, the FTC has implemented the Every Community Initiative, which examines consumer protection issues and the impact of unlawful privacy practices on distinct groups, and marginalized populations, such as Black Americans, military service members, and older adults, among other groups. In September, the agency published a report to Congress highlighting key efforts that the FTC will continue to focus on: (1) integrating competition concern; (2) advancing remedies; (3) focusing on digital platforms; and (4) expanding understanding of algorithms.

Securities and Exchange Commission

In 2021, the SEC increased its focus on cyber disclosure. The SEC filed two administrative actions in 2021, one involving a cyberattack on an educational services company, and the other involving a cyber vulnerability at a financial services firm.

On June 14, the SEC settled charges against real estate company First American Financial Corporation for "disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed sensitive customer information." According to the SEC's order, a cybersecurity journalist notified First American on May 24, 2019, of a vulnerability with its application for sharing document images that exposed over 800 million images dating back to 2003, including images containing data such as Social Security numbers and financial information. The SEC further stated that in response to the incident, First American issued a press statement on the evening of May 24, 2019 and furnished a Form 8-K to the Commission on May 28, 2019. The SEC stated, however, that First America's senior executives responsible for these public statements "were not apprised of certain information that was relevant to their assessment of the company's disclosure response to the vulnerability and the magnitude of the resulting risk. In particular, the order finds that First American's senior executives were not informed that the company's information security personnel had identified the vulnerability several months earlier but had failed to remediate it in accordance with the company's policies. The order finds that First American failed to maintain disclosure controls and procedures designed to ensure that all available, relevant information concerning the vulnerability was analyzed for disclosure in the company's public reports filed with the Commission."

Per the SEC's press release, the SEC charged First American with violating Rule 13a-15(a) of the Exchange Act. Without admitting or denying the SEC's findings, First American agreed to a cease-and-desist order and to pay a $487,616 penalty.

On August 16, the SEC settled charges against Pearson plc, a U.K. educational publisher, for inadequate disclosure of a cyber intrusion. The company agreed to pay $1 million to settle charges that it allegedly misled investors about a 2018 cyber intrusion. Per the SEC, this intrusion involved the theft of millions of student records, including dates of birth and email addresses. The SEC alleged, among other things, that in its July 2019 semi-annual report, Pearson referred to a data privacy incident as a hypothetical while knowing that such an incident had occurred in 2018. The SEC claimed that a media statement issued in July 2019 "understated the nature and scope of the incident, and overstated the company's data protections."

The SEC order stated that Pearson violated Section 17(a)(2) and (a)(3) of the Securities Act, which prohibits misleading statement or omissions in the context of a securities offering. The order also stated the company violated Section 13(a) of the Exchange Act, which governs mandatory disclosures a publicly traded company must make. Without admitting or denying the SEC's findings, Pearson agreed to cease and desist from committing violations of these provisions and to pay a $1 million civil penalty.

DEBT COLLECTION

There were three significant developments in the debt collection industry in 2021, with the Court of Appeals for the Eleventh Circuit disrupting the industry by calling into question the use of third-party vendors, the Consumer Financial Protection Bureau (CFPB or the Bureau) releasing its long-awaited final debt collection rule, Regulation F, and the Supreme Court clarifying its Article III standing analysis in the context of alleged statutory violations in *TransUnion LLC v. Ramirez*.

Hunstein **Calls Into Question the Use of Vendors in Debt Collection**

The most significant case affecting the industry this year, *Hunstein v. Preferred Collection & Management Services*, came as a shock. For context, Section 1692c(b) of the FDCPA prohibits a debt collector from communicating with most third parties "in connection with the collection of any debt" unless it has the consumer's consent. Communications with the consumer's attorney, a creditor or its attorney, the debt collector's attorney, or a consumer reporting agency are permissible, as are certain communications with third parties to locate a consumer or those required by a court or court judgment. A debt collector is subject to liability for all other third-party communications "in connection with the collection of any debt."

In a panel decision on April 21, the Eleventh Circuit held that: (1) a consumer had standing to bring a claim under the Fair Debt Collection Practices Act (FDCPA) because he alleged an invasion of privacy based on the spread of his debt-related information; and (2) a debt collector's outsourcing of its letter process to a third-party letter vendor violates the FDCPA because sending the data to create and mail letters to consumers violates the prohibition on third-party disclosure set forth in Section 1692c(b) of the FDCPA.

Further complicating the matter, the Eleventh Circuit then vacated its original opinion and issued a substitute opinion. *Hunstein vs. Preferred Collection & Management Services, Inc.*, --- F. 4th ----, No. 19-14434, 2021 WL 4998980 (11th Cir. Oct. 28, 2021).

Unfortunately for the industry, the substitute opinion did not reverse the panel's original opinion. Instead, the majority of the panel doubled down on its original opinion and found that Hunstein had standing to sue, even after the Supreme Court's *Ramirez* decision. Despite the Supreme Court's clarification of standing for statutory violations, the *Hunstein* panel majority nonetheless found the alleged statutory violation sufficiently analogous to the common law tort of public disclosure of private facts to convey standing under the FDCPA. *Id.* at *10. In so holding, the majority reasoned that a statutory harm need only be similar in *kind* to a common law tort, not necessarily similar in *degree*. *Id.* at *5-10.

All was not lost, however; in a sharp dissent, Judge Tjoflat claimed the majority opinion "goes off the rails" and ignored the requirement set by *Ramirez* that a plaintiff must allege a statutory violation sufficiently analogous to a common law tort. *Id.* at *17. He viewed Preferred's communication to its vendor as insufficiently "public" to constitute a public disclosure of private facts. *Id.*

On November 17, the Eleventh Circuit vacated the substitute opinion and agreed *sua sponte* to reconsider *en banc* whether Preferred's transmission of private debtor information to its mail vendor violated the FDCPA. *See* 2021 WL 5353154 (11th Cir. Nov. 17, 2021).

The Eleventh Circuit's decision to rehear the case *en banc* may reflect the substantial industry implications of its prior ruling (as reflected in the large number of amicus briefs that have been submitted in the appeal). If debtors have standing to sue when collections agencies outsource private information to any vendor, the opinion in *Hunstein* could have a dramatic impact on the litigation exposure of debt collectors and require those collectors to conduct ministerial functions "in-house."

The *en banc* hearing is scheduled to take place in February 2022.

Regulation F Takes Effect November 30, 2021

On October 30, 2020, the CFPB released its long-awaited final debt collection rule—also known as Regulation F. The Bureau supplemented the rule on December 18, 2020 and both parts were adopted pursuant to the Bureau's authority under the FDCPA.

On April 7, 2021, the CFPB issued a Notice of Proposed Rule Making (NPRM), which proposed delaying the effective date of the rule for 60 days. However, on July 30, the CFPB issued a press release indicating the effective date would not be delayed.

The CFPB determined that an extension of the effective date was unnecessary since most public comments did not support it, and most industry commenters stated that they would be prepared to comply with the rules by the original November 30, 2021 deadline. However, the CFPB expressly stated that its current decision would not prohibit it from reconsidering the rule later. Thus, the rule, in its entirety, became effective 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 communication by voicemail, email, and texts. Specifically, the rule directly addresses the following topics:

Definitions

The rule significantly revises several definitions that will dictate how debt collectors comply with the FDCPA. The more material revised definitions include:

- **Communicate** or **Communication:** The rule defines these terms to mean "the conveying of information regarding a debt directly or indirectly to any person through any medium." *See* § 1006.2(d). According to the Bureau, general advertising that includes no information about a specific debt likely would not meet the definition of a communication. Further, a "limited-content message" is not a communication. The FDCPA imposes restrictions not only on a debt collector's communications with a consumer, but also on a debt collector's attempts to communicate with a consumer even where such attempts are not

successful (e.g., where a consumer does not answer a debt collector's call).

- **Consumer:** A consumer is defined as "any natural person obligated or allegedly obligated to pay any debt," and for purposes of a debt collector's communications, may include a spouse, parent of a minor, legal guardian, estate executor, or confirmed successor in interest. *See* §§ 1006.2(e), 1006.6(a). The Bureau left open whether it will further define this term to clarify its application when the consumer is deceased, which may be useful in the context of debt validation notices.
- **Limited-content message:** The rule allows a debt collector to leave a voicemail message for a consumer that is not a communication under the FDCPA provided it is a "limited-content message." To be a "limited content message," the voicemail must include:

  1. a business name for the debt collector (that does not indicate that the debt collector is in the debt collection business);
  2. a request that the consumer reply to the message;
  3. the name (or names) of one or more person(s) whom the consumer can contact to reply to the debt collector; and
  4. a phone number (or numbers) that the consumer can use to reply to the debt collector.

See § 1006.2(j)(1). The voicemail may also include certain optional content, including:

  1. a salutation;
  2. a request that the consumer reply to the message;
  3. suggested dates and time for the consumer to reply to the message; and
  4. a statement that if the consumer replies, the consumer may speak to any of the company's representatives or associates.

Id. Nothing else can be included in the limited content message for it to retain its status as a non-collection communication.

Unlike the first proposed rule, released in 2019, the Bureau ultimately confined limited content messages to voicemail only. *See* § 1006.2(j). Further, the rule instructs that if a collector places a call to a consumer that results in a live connection with an unauthorized third-party, the collector should not leave any message (limited content or otherwise) and instead, simply state that they will call back another time.

The call frequency limits are not technically a bright-line rule, but rather establish a rebuttable presumption of violation if they are exceeded.

Telephone Call Frequency Limits – Section 1006.14

The rule bars a debt collector from making more than seven telephone calls to a consumer within seven consecutive days in connection with the collection of a debt, or within a period of seven consecutive days after having had a telephone conversation with the person in connection with the collection of such debt. *See* § 1006.14(b)(1). Further, voicemails left for the consumer, including ringless voicemails, count as "calls" for purposes of calculating the call attempt limitation, as do limited content messages left for consumers (see above). Calls excluded from the call attempt calculation include calls directly to the debt collector and that are returned by the collector with prior consumer consent within a period no longer than seven consecutive days after receiving that consent; calls that do not connect to the dialed number; and calls placed to certain professional persons (such as an attorney representing the consumer). *See* § 1006.14(b)(3).

The call frequency limits are not technically a bright-line rule, but rather establish a rebuttable presumption of violation if they are exceeded. Further, the rule added commentary stating that even if the frequency limits are not exceeded, a debt collector could still violate the FDCPA if the

natural consequence of another aspect of the debt collector's communications is to harass, oppress, or abuse any person in connection with the collection of a debt. Specifically, Comment 14(b)(2)(i)–2 discusses how the presumption of compliance can be rebutted and includes a non-exhaustive list of factors that may rebut the presumption of compliance.

Electronic Communications – Section 1006.6(b)

The rule does not prohibit electronic debt collection communications, including emails and text messages, nor does it establish explicit rules for such communications. Instead, it outlines guidelines for email and text communications in its discussion of third-party communications. Section 1006.6(d)(3) establishes a safe harbor from civil liability for third-party disclosures resulting from email or text communications if the debt collector establishes procedures to reasonably confirm and document that the debt collector emailed or texted the consumer in accordance with certain established procedures.

Electronic Communications – Email

The debt collector can use the safe harbor for email communications in three methods. The applicable method is contingent on how the debt collector received the consumer's email address and include the following:

1. The "direct communication with the consumer" method allows email communications where the consumer either used the email address to communicate with the debt collector about the debt (and has not since opted out) or the debt collector received prior consent to use that email address (which the consumer has not withdrawn). *See* § 1006.6(d)(4)(i). Consumer consent can be provided orally, in writing, or electronically, *see comment* 6(d)(4)(i)(B)–1 to § 1006.6, and provision of the email address via website or online portal is considered consent. *See comment* 6(d)(4)(i)(B)–2 to § 1006.6.2.

2. The "creditor communication with the consumer" method allows the debt collector to send an email to an email address that the creditor used to communicate with the consumer if five specific criteria are met:

3.
    a. the creditor obtained the email address from the consumer;
    b. the creditor used the email address to communicate with the consumer about the account and the consumer did not ask the creditor to stop using it;
    c. before the debt collector used the email address to communicate with the consumer about the debt, the creditor sent the consumer a written or electronic notice that clearly and conspicuously disclosed the information required under the rule (including the right to opt out of email communications);
    d. the opt-out period has expired and the consumer has not opted out; and
    e. the email address has a domain name that is available for use by the general public (e.g., @gmail.com), unless the debt collector knows the address is provided by the consumer's employer; in which case, the debt collector may not send communications to the address.

See § 1006.6(d)(4)(ii).

4. The "prior debt collector communication with the consumer" method allows the debt collector to use an email address that a prior debt collector used to communicate with the consumer if it was obtained in accordance with the consumer-use or prior creditor-use methods, the immediately prior debt collector used that email address for communications with the consumer about the debt, and the consumer did not opt out of such communications.

See § 1006.6(d)(4)(iii).

Electronic Communications – Text Message

The rule provides a safe harbor for text messages under two circumstances: 1) where consumers have used the telephone number to communicate with the debt collector, via text message, about the debt; or 2) where the debt collector has received direct prior consent to use that number for text messages.

The "consumer-use" method allows debt collectors to text a phone number where:

1. the consumer used that number to communicate with the debt collector about the debt by text message;
2. the consumer has not since opted out of text communications to that number; and
3. within the past 60 days, either:
    a. the consumer sent a text message to the debt collector from that phone number; or
    b. the debt collector confirmed, using a complete and accurate database, that the phone number has not been reassigned since the date of the consumer's most recent text message to the debt collector from that phone number.

See § 1006.6(d)(5)(i). However, the consumer-use text message safe harbor does not apply where the consumer only used the phone number to communicate with the debt collector via telephone call. *See comment* 6(d)(5)(i)–1 to § 1006.6.

Alternatively, there is a safe harbor to use the phone number for texts if the debt collector received directly from the consumer prior consent to use the telephone number to communicate by text message, the consumer has not since withdrawn that consent, and within the past 60 days the debt collector either:

1. obtained the prior consent or renewed consent from the consumer; or
2. confirmed, using a complete and accurate database, that the telephone number has not been reassigned from the consumer to another user since the date of the consumer's most recent consent to use that telephone number to communicate about the debt by text message.

See § 1006.6(d)(5)(i)(ii).

Opt-Out Notice

The rule requires any electronic communications to include a clear and conspicuous opt-out notice describing a "reasonable and simple method" for opting out. *See* § 1006.6(e). Debt collectors may not require consumers to pay any fees or provide any information other than the consumer's opt-out preferences in order to opt out. *Id.* The opt-out notice provisions apply to all electronic communications, including emails, text messages, direct messaging communications on social media, and even communications in an application on a website, mobile telephone, or computer.

Time and Place Restrictions – Section 1006.6(b)

The rule clarifies restrictions on the times and places at which a debt collector may communicate or attempt to communicate with a consumer, including by clarifying that a consumer need not use specific words to assert that a time or place is inconvenient for debt collection communications.

The CFPB has interpreted the language in FDCPA Section 805(a)(1) that a debt collector should assume that the convenient time for communicating with a consumer is after 8 a.m. and before 9 p.m. local time at the consumer's location, unless the debt collector has knowledge of circumstances to the contrary.

The rule adopts a safe harbor to facilitate compliance with the time and place restriction when the debt collector has conflicting or ambiguous information regarding a consumer's location. The safe harbor would apply in circumstances in which the debt collector does not have knowledge of the consumer's actual location. Generally speaking:

- a debt collector is not required to determine where the consumer is located when communicating or attempting to communicate with the consumer; and
- knowledge that a telephone number is associated with a mobile telephone does not, without more information, create conflicting or ambiguous information about time and place restrictions.

However, a debt collector may know or should know that it is inconvenient to communicate or attempt to communicate with a consumer at a time outside of the presumptively convenient times (8 a.m. to 9 p.m.) in any of the time zones in which the consumer might be located.

Consumer's Ability to Set Restrictions – Section 1006.14(h)(1)

The rule restricts the times and places during which a debt collector may communicate with a consumer and a consumer does not need to use specific words or assert a time or place that is inconvenient for debt collection communications. Rather, these restrictions apply to any time or place that the debt collector *knows or should know* is inconvenient. Additionally, a consumer may designate certain means of communications as off-limits for debt collection communications. The respect for the consumer's preferences is a common thread throughout the rule.

Records Retention Requirements – Section 1006.100

The rule clarifies a debt collector's obligation to retain records evidencing compliance or noncompliance with the FDCPA and Regulation F. A debt collector must retain records beginning on the date it begins collection activity and for a period of three years after the debt collector's last collection activity on the debt. If the debt collector retains recordings of phone calls, they must be archived for three years after the date of the call. *See* § 1006.100.

Time-Barred Debt – Section 1006.26

The rule prohibits debt collectors from suing or threatening to sue consumers to collect a time-barred debt, which is defined as a debt for which the applicable statute of limitations has passed. The Bureau declined to finalize certain time-barred debt disclosures included in the proposed rule and did not provide suggested discourses, or a related safe harbor provision, for notifying consumers that their debt is time-barred.

Model Validation Notice

In the proposed rule, the CFPB provided a model validation notice form which, if used, would create a safe harbor for debt collectors. The proposed validation notice was designed to protect debt collectors from the high volume of FDCPA lawsuits alleging that the validation letter violated the FDCPA in one way or another. The final rule ultimately ended up largely the same as the proposal—if a debt collector wants to take advantage of the safe harbor, its collection notice must mirror the model notice, subject to state law requirements.

The model validation notice form now requires an "itemization date." The collector may choose one of five dates as the itemization date:

1. the last statement date,
2. the charge-off date,
3. the last payment date,
4. the judgment date, or the transaction date.

The itemization date must be chosen on or before the date on which the validation notice is sent to the consumer and cannot be changed once chosen. The itemization date(s) need not be provided in subsequent communications.

The CFPB's recent validation information FAQs can be found here.

Debt Parking/Delayed Credit Reporting – Section 1006.30

The Bureau finalized its proposal against debt parking, or the process of credit reporting the debt before communicating with the consumer. The rule requires that debt collectors send a communication about the debt to the consumer before reporting the debt to any credit reporting agency. If that communication is in writing, the debt collector must wait a reasonable time (to ensure there are no deliverability issues) before they can report the account. For traditional mail, the Bureau defined "reasonable time" as 14 days, regardless of delivery method.

Conclusion

The rule serves as the most expansive and dramatic revision to the FDCPA in its history. Luckily for creditors, the Bureau also noted that it "declines to expand the rule to apply to first-party debt collectors who are not FDCPA debt collectors," and noted that "the Bureau did not solicit feedback on whether or how such provisions should apply to first-party debt collectors." Thus, creditors are, for now at least, unaffected by the revisions.

We also recommend the CFPB's Debt Collection Rule FAQs which are slowly being built out by the Bureau. The current topics include:

- Limited-Content Messages
- Telephone Call Frequency
- Telephone Call Frequency: Presumptions
- Telephone Call Frequency: Excluded Calls
- Telephone Call Frequency: Rebutting the Presumptions
- Validation Information
- Validation Information: Residential Mortgage Debt

We expect more to come from the Bureau soon.

TransUnion v. Ramirez – Article III Standing Under the Federal Consumer Law Statutes

In June, the Supreme Court issued its opinion in *TransUnion LLC v. Ramirez*, holding that a concrete injury under the Fair Credit Reporting Act (FCRA) requires more than the existence of a risk of harm that never materializes. 141 S. Ct. 2190 (2021). The Court tackled two questions: first, whether a plaintiff can establish Article III standing without suffering a concrete harm aside from simply alleging a violation of a federal statute, which provides for the recovery of statutory damages. Second, the Court decided whether each putative class member must establish Article III standing to assert a claim for statutory damages. In a 5-4 decision, the Court held that on the first issue, plaintiff suffered "no concrete harm, [and thus had] no standing." On the second issue, the Court held that "[e]very class member must have Article III standing in order to recover individual damages."

While the Court's decision specifically addressed questions of Article III standing as applied to the FCRA, this decision is proving to be a far-reaching and a highly debated opinion that spans numerous substantive areas of law, including consumer protection claims, data breach cases, and privacy matters. In the months following the decision, the implications of this case continue to be debated in lower courts.

Background of *TransUnion v. Ramirez*

This case arose from a product offered by TransUnion that attached a "potential match" alert to the credit files of individuals with names matching a name designated by the Department of the Treasury's Office of Assets Control (OFAC) as individuals restricted from certain transactions for national security reasons (e.g., terrorists, drug traffickers, etc.). The named plaintiff, Sergio Ramirez, alleged TransUnion transmitted his consumer report with the OFAC alert attached to a car dealership when Ramirez attempted to finance a car purchase. He alleged he suffered an actual injury in the form of denied credit, embarrassment in front of his family, and a resulting vacation cancellation.

Ramirez contacted TransUnion and requested a copy of his credit file. In response, TransUnion mailed him a file disclosure that did not contain the OFAC alert. TransUnion also mailed Ramirez a separate letter referencing the file disclosure letter and explaining that his name was a "potential match" to a name on the OFAC list.

Ramirez filed a class action suit under the FCRA and alleged two types of claims: First, Ramirez alleged TransUnion failed to maintain reasonable procedures to assure the maximum possible accuracy of the information in its consumer reports (the "reasonable procedures" claim). Second, Ramirez alleged TransUnion violated the FCRA's requirement to provide consumers, upon request, with all information in its files by providing the OFAC potential match information in a separate mailing, and that TransUnion violated the FCRA's requirement to provide consumers with a summary of their rights with each file disclosure by not including a summary of rights in the OFAC-alert mailing (the "disclosure" and "summary-of-rights" claims).

Ramirez sought to represent a class of over 8,000 individuals to whom TransUnion sent a similar OFAC-alert letter. Although the "potential match" alert was attached to the credit files of all class members and stored in TransUnion's internal files, only the files of 1,853 of the class members were disseminated to third parties. The remaining 6,332 could not prove a consumer report with the OFAC alert was disseminated. Further, even among the 1,853 class members for whom a consumer report with an OFAC alert was disseminated, only Ramirez alleged he was denied credit as a result. The suit also alleged each class member was injured by receiving the nonconforming file disclosure mailings, but only Ramirez alleged he even read the letters, let alone was confused by them.

The district court certified a national class for the FCRA claims, and after trial, a jury awarded the class $8 million in statutory damages and $52 million in punitive damages. On appeal, the Ninth Circuit affirmed certification and the statutory damages award but reduced the punitive damages award to $32 million. Regarding the reasonable procedures claim, even though most of the class members could not allege their credit file with an OFAC alert was ever transmitted to a third party, a divided Ninth Circuit panel held a "material risk of harm" existed sufficient to establish Article III standing simply because TransUnion had compiled the allegedly false information in its database and could have disseminated it upon request. The Ninth Circuit further held every class member suffered an injury by receiving the nonconforming mailings since the separate credit file and OFAC-alert mailings were "inherently shocking and confusing."

[Ramirez] alleged he suffered an actual injury in the form of denied credit, embarrassment in front of his family, and a resulting vacation cancellation.

The Supreme Court granted TransUnion's petition for certiorari and heard oral arguments on March 30. The Court's 5-4 decision resulted in a reversal and remand of the Ninth Circuit's opinion, finding that, contrary to the Ninth Circuit's position, all class members needed to suffer a materialized harm to have standing.

The Court began with the plaintiffs' main claim: that TransUnion failed to follow reasonable procedures by including allegedly inaccurate or misleading OFAC alerts in the plaintiffs' credit files, in violation of 15 U.S.C. § 1681e(b). The Court immediately drew a distinction between the 1,853 class members whose consumer reports with the OFAC alert were disseminated to third parties and the 6,332 class members whose reports were not disseminated. Even if they were only labeled as a "potential terrorist," the Court held that the former category of consumers had asserted a concrete injury sufficient to confer standing; the latter had not.

Regarding the 1,853 class members, the Court held they had suffered a "reputational harm" through the publication of false or misleading information that bore a close relationship to a harm associated with a traditionally recognized cause of action: the tort of defamation. TransUnion argued that even these individuals had not suffered an injury, because the information included in the OFAC alert was not technically false; it merely identified a consumer as a potential match on the OFAC list, not a guaranteed match. The Court rejected this

argument: although the common law analogue must be close, the harm asserted need not be an "exact duplicate" of the traditional cause of action. Thus, even though defamation requires falsity, the publication of misleading information was, to the Court, close enough.

For the remaining 6,332 class members, the Court held that the mere existence of the OFAC alert in their credit files, without proof of dissemination, did not constitute a concrete injury. The Court analogized this to a defamatory letter stashed away in a desk drawer. Defamation requires publication; otherwise, the reputational harm does not materialize.

The Court also rejected the plaintiffs' argument that a material risk that TransUnion could have disseminated the information upon the request of a third party constituted a concrete injury. Instead, the Court held that a mere risk of future harm that never materializes, standing alone, does not constitute a concrete injury. These plaintiffs had also failed to factually establish a sufficient risk of harm to begin with: their allegations that their consumer reports with an OFAC alert could have been disseminated if requested by a third party were too speculative.

Finally, since there was no evidence that these plaintiffs even knew the OFAC alerts were in their internal credit files, the Court noted it was "difficult to see how a risk of future harm could supply standing when the plaintiff did not even know that there was a risk of future harm."

The Court lastly turned its attention to the disclosure and summary-of-rights claims, noting these dual claims involving the format of TransUnion's mailings were "intertwined." On these claims, the Court held that none of the plaintiffs other than Ramirez had suffered a concrete injury. The Court held that the allegedly noncompliant format of the mailings had not caused the class members an injury with a close relationship to a traditionally recognized harm. In fact, the plaintiffs had demonstrated no harm at all, as there was no evidence that any class member other than Ramirez had opened the mailings, suffered confusion or distress, or that they would have tried to correct their files if they had received the mailings in the proper format. As such, the Court held that these claims asserted nothing more than "bare procedural violation[s], divorced from any concrete harm," insufficient to confer standing.

Cases Following *TransUnion v. Ramirez*

In the months following *Ramirez*, many circuit and state courts have addressed the Article III standing questions posed in *Ramirez*. In the dissenting opinion in *Ramirez*, Justice Thomas opined that *Ramirez* may be a "pyrrhic victory" for TransUnion because it did not prohibit Congress from creating statutory rights, but only held the federal court lacked jurisdiction to enforce them absent a concrete harm. However, based on recent decisions since *Ramirez*, it seems that both circuit and district courts align with heavily scrutinizing whether plaintiffs can establish standing.

Other than *Ramirez*, circuit and district courts across the country have released various opinions of note as it relates to Article III standing in consumer protection law cases. Of these decisions, only one Tenth Circuit opinion found that a plaintiff met the heightened standing requirement post *Ramirez*. Additionally, many of the subsequent decisions have been applied to the FDCPA, which shows the far-reaching effect of *Ramirez* beyond FCRA cases.

In *Lupia v. Medicredit, Incorporated*, the Tenth Circuit found that a plaintiff had standing to bring an FDCPA action against a debt collector based on receipt of a single phone call. No. 20-1294, 2021 U.S. App. LEXIS 24547 (10th Cir. Aug. 17, 2021). In *Lupia*, a defendant sent correspondences to a plaintiff to collect an unpaid debt. After receiving the initial correspondence, the plaintiff notified the defendant to both dispute the debt and request that the defendant cease communications. Despite the plaintiff's request, the defendant placed an additional call. Plaintiff then asserted a claim under the FDCPA.

The Tenth Circuit noted that *Ramirez* instructs courts to look at the history and judgment of Congress in determining whether there was an injury. The court found that the plaintiff suffered a concrete injury because the plaintiff's claims were similar to the tort of "intrusion upon seclusion" and rejected the defendant's argument that one call did not cause injury noting that "though a single phone call may not intrude to the degree required at common law, that phone call poses the same kind of harm

recognized at common law – an unwanted intrusion into a plaintiff's peace and quiet." Additionally, the Tenth Circuit noted that unlike in *Ramirez*, the plaintiff in this case was not merely relying on a procedural violation and the plaintiff's claim had "roots in long- standing common- law tradition."

In *Friend v. CACH LLC*, a district court in the Seventh Circuit dismissed an FDCPA case for lack of Article III standing. No. 4:19 CV 6, 2021 U.S. Dist. LEXIS 177359 (N.D. Ind. Sep. 17, 2021). In its holding, the court emphasized that to establish Article III standing, a plaintiff must establish concrete harm that plaintiff would not have incurred had the debt collector complied with the FDCPA. The plaintiff must allege more than mere contact between the plaintiff and the defendant when the defendant allegedly knew the plaintiff was represented by counsel.

In *Friend*, the plaintiff sued the defendant for violations of Section 1692g(b) (failing to cease communications and/or validate debt), Section 1692e(8) (reporting an inaccurate balance to the credit bureaus), Section 1692f(1) (attempting to collect amounts not authorized by the agreement creating the debt), and Section 1692c(a)(2) (communicating directly with the plaintiff, despite notice of counsel) of the FDCPA. The court found that the plaintiff's failure to address standing as to three of his four FDCPA claims in supplemental briefings resulted in waiver and that plaintiff failing to respond to the defendant's summary judgment motion and the court's order to address Article III standing constituted dismissal. The court emphasized that the plaintiff's mere recitations that the "[d]efendant['s] conduct damaged [the] [p]laintiff financially" were insufficient at the present state of the litigation, and there was otherwise no clear evidence of concrete harm sufficient to establish injury in fact for Article III standing on these claims. This aligns with *Ramirez* and older Seventh Circuit opinions such as *O'Toole v. Bob Roache Law* and *Smith v. GC Services Limited Partnership*, that found plaintiffs lacked standing to bring an FDCPA claim.

In two New York district court opinions, the court applied *Ramirez* in the context of the FDCPA and the "mailing vendor" cause of action theory commonly alleged by plaintiffs. In *In re FDCPA Mailing Vendor Cases*, the court dismissed six FDCPA complaints finding that plaintiffs in each of the respective cases failed to demonstrate injury-in-fact sufficient for Article III standing in response to show cause orders and that a defendant using an outside firm to print and mail dunning letters to consumers did not give rise to a concrete injury. No. 21-2312, 2021 U.S. Dist. LEXIS 139848 (E.D. N.Y. July 23, 2021). Similarly, in *Bush v. Optio Solutions LLC*, the court held that, in the wake of *Ramirez*, a debt collector disclosing that a consumer owes a debt to a third party does not rise to the level of a concrete, particularized injury for Article III purposes. No. CV 21-1880 (GRB)(ARL), 2021 U.S. Dist. LEXIS 140835 (E.D.N.Y. July 28, 2021).

Lastly, two district court opinions that predate *Ramirez* seem to show a tradition of courts being hesitant to find Article III standing in cases where plaintiffs are bringing claims under the FDCPA.

In *Shepherd v. Debt Recovery Sols. of Ohio, Inc.*, the court dismissed a putative class action alleging violations of the FDCPA, finding that the named plaintiff had not suffered a concrete injury, and therefore, he lacked standing to assert a claim. *No. 3:20-cv-520* (*N.D. Ohio Apr. 22, 2021*). The plaintiff alleged that a debt collection letter he received from the defendant was misleading and attempted to collect an amount that was not authorized by the agreement creating his debt. The defendant moved to dismiss plaintiff's claim, asserting that he failed to plead the existence of an actual injury. The court agreed, finding that plaintiff's allegations did not show "a material risk of real harm to a concrete interest." Because plaintiff was not required to take an action that would cause him to incur a transaction fee, the court concluded that he had not suffered an actual injury. Additionally, in *In Giannini v. Fin. Recovery Servs.*, the Northern District of Illinois dismissed a case for lack of standing where a plaintiff alleged a defendant violated the FDCPA by "fail[ing] to include safe harbor language" in its collection letter. No. 20 C 4212, 2021 U.S. Dist. LEXIS 9504 (N.D. Ill. Jan. 19, 2021). In its ruling, the court emphasized that to establish standing under the FDCPA, a plaintiff must show that plaintiff suffered concrete harm based on detrimental action taken in light of a defendant's omission in a collection letter. The court also clarified that a plaintiff's experience

of stress, anxiety, worry, confusion, and annoyance is not enough in and of itself to establish standing.

Conclusion

Ramirez established that plaintiffs need more than a statutorily created right (public or private) cause of action to make their way into federal court. Additionally, *Ramirez* clarifies that it is the judiciary, not Congress, that is charged with determining whether a concrete harm exists, based on a historical inquiry. Though *Ramirez* helped to clarify issues surrounding what constitutes an injury for Article III standing purposes, the decisions that have followed illustrate that the principles established in *Ramirez* can be applied to other consumer protection laws and that while such lawsuits may continue to be filed, they will have a much harder time progressing in federal court, which could result in more of these types of cases being filed in state court.

FAIR LENDING

The past few years have seen considerable ebbs and flows in the fair lending space. Though a major initiative of the Obama administration, fair lending was a less significant portion of Trump-era regulators' agenda. With the Biden administration, however, fair lending issues have come roaring back to the forefront, with an increased emphasis on disparate impact and redlining. Meanwhile, some states — particularly New York — have been active.

Within 2021, the most notable highlights within this landscape include the Department of Justice's (DOJ) initiative to combat redlining, the CFPB's and New York Department of Financial Services' (NYDFS) focus on reducing discrimination within mortgage lending, the Consumer Financial Protection Bureau's (CFPB) proposed changes to the Small Business Data Collection Rule, and the Federal Trade Commission's (FTC) report analyzing consumer fraud trends affecting communities of color.

DOJ Redlining Initiative

In October 2021, the DOJ announced the launch of the department's new Combatting Redlining Initiative (Redlining Initiative). The Redlining Initiative represents the department's most aggressive and coordinated enforcement effort to date, addressing redlining that is prohibited by the Fair Housing Act and the Equal Credit Opportunity Act. In speaking about the new initiative, Attorney General Merrick Garland emphasized that "lending discrimination runs counter to fundamental promises of our economic system," and that "[w]hen people are denied credit simply because of their race or national origin, their ability to share in our nation's prosperity is all but eliminated."

The Redlining Initiative, led by the Civil Rights Division's Housing and Civil Enforcement, will further the department's efforts to ensure mortgage credit and homeownership are accessible to all Americans, regardless of race, national origin, or neighborhood location. The Redlining Initiative will:

- Utilize the U.S. attorneys' offices as force multipliers to ensure that fair lending enforcement is informed by local expertise on housing markets and the credit needs of local communities of color.
- Expand the department's analyses of potential redlining to both depository and non-depository institutions.
- Strengthen partnerships with financial regulatory agencies to ensure the identification and referrals of fair lending violations to the DOJ.
- Increase coordination with state attorneys general on potential fair lending violations.

In addition to the Redlining Initiative, the DOJ, the CFPB, and the Office of the Comptroller of the Currency (OCC) announced agreements with various U.S. national banks to resolve allegations of lending discrimination using redlining tactics.

Mortgage Lending

In 2021, both federal and state regulations provided guidance on ways to combat racial and sexual orientation discrimination within mortgage lending. On August 31, 2021, the New York Department of Financial Services (DFS) issued an industry letter to all supervised mortgage lending institutions and their affiliates on preventing sexual orientation discrimination in mortgage lending. New York's fair lending law prohibits discrimination in, among other things, the granting; withholding; extending; renewing; or fixing of rates, terms, or conditions of any form of credit on the basis of sexual orientation.

After analyzing mortgage loan applications and terms from four non-depository lenders and one bank from 2016-2018, NYDFS found notable disparities in approvals, denials, and terms of credit between same-sex and opposite-sex pairs in mortgage lending. While NYDFS could not determine whether these disparities resulted from discrimination, it notes that the findings raise sufficient concern of possible discrimination based on sexual orientation. As a result, NYDFS issued its industry letter.

After analyzing mortgage loan applications and terms from four non-depository lenders and one bank from 2016-2018, NYDFS found notable disparities in approvals, denials, and terms of credit between same-sex and opposite-sex pairs in mortgage lending.

The letter recommended that all mortgage lenders take the following actions to reduce risks of discrimination based on sexual orientation:

- Vest the board of directors and senior management of institutions with responsibility for developing a fair lending plan and ensure that the lender's practices comply with the plan.
- Monitor implementation of the fair lending plan and adherence to the plan's policies and procedures, continually addressing application and underwriting processes, as well as pricing policies.
- Implement a training program for new hires, current employees, and management at least semi-annually that provides lending personnel updates on fair lending issues and requires participants to certify an understanding of and a commitment to uphold the principles of fair lending laws and the policies and procedures contained in the fair lending plan.
- Ensure automatic and timely review by a higher-level supervisor of all rejected or withdrawn applications for loans from same-sex pairs who indicated that they would live together in a mortgaged property.
- Extend, in writing, the principles of the fair lending plan to the lender's refinancing and collection practices.
- Periodically review and update the fair lending plan and compliance program, including periodic review by senior management, to ensure that they remain current.

NYDFS also recommended that all mortgage lenders take the following compliance actions:

- Update policies and procedures to address sexual orientation anti-discrimination efforts.
- Utilize rate sheets and exception logs to document applications from same-sex pairs who indicated that they would live together in the mortgaged property that are either (1) denied for any reason other than a failure to meet the institution's written underwriting standards; or (2) granted, but with credit terms less favorable than the applicable rate sheets would otherwise determine.
- Monitor loan portfolio for compliance with fair lending policies and procedures, which may include identifying those loan applications from, and loans made to, same-sex pairs who indicated that they would live together in the mortgaged property and distinguishing such applications and loans from those applications from, and loans made to, same-sex pairs who do not consist of two individuals who indicated that they would live together in the mortgaged property.
- Regularly assess marketing and advertising strategies to ensure compliance with the principles and provisions of fair lending laws and the fair lending plan.
- Investigate and attempt to identify the causes of any unexplained disparities in underwriting and pricing between same-sex and opposite-sex pairs who indicated that they would live together in the mortgaged property.

Additionally, the CFPB issued a request for information (RFI) to seek input on rules governing the Home Mortgage Disclosure Act (HMDA) to ensure data collected is accurate and can be used by the CFPB to further the goals of the 2015 amendments to the HMDA. The CFPB foresees this evaluation will help strengthen its ability to maintain a fair, competitive, and nondiscriminatory mortgage market. The RFI follows an August 2021 HMDA report, which identified a trend of mortgage lenders

denying credit and charging higher interest rates to Black and Hispanic applicants as compared to white applicants.

In 2015, changes to the HMDA regulations expanded the types of data reported by lenders to improve overall market information and help with monitoring for fair lending compliance. The 2015 rule also improved the reporting process by aligning requirements with industry data standards, significantly enhancing the technological interface, and easing requirements for some small banks and credit unions.

The CFPB currently seeks comment from the public to ensure the agency can use the data collected under the HMDA Rule to meet the rule's goals and to assess overall effectiveness of the HMDA Rule. Specifically, the CFPB will focus on collecting data related to institutional coverage and transactional coverage, data points, benefits of the new data and disclosure requirements, and operational and compliance costs.

CFPB Fall 2021 Supervisory Highlights

Lastly, in December of 2021, the CFPB issued its *Fall 2021 Supervisory Highlights*, which covers examinations undertaken between January 2021 and June 2021.

In the report, CFPB examiners found that mortgage lenders discriminated against African American and female borrowers in granting pricing exceptions as compared to non-Hispanic white and male borrowers. Specifically, examiners found lenders lacked oversight and control over how mortgage loan officers granted pricing exceptions to customers. Examiners did not identify evidence that explained the disparities observed in the statistical analysis. Instead, examiners identified instances where lenders provided pricing exceptions for a competitive offer to non-Hispanic white and male borrowers with no evidence of customer initiation. Furthermore, examiners noted that lenders failed to retain documentation to support pricing exception decisions.

Additionally, CFPB examiners found that lenders improperly considered small business applicants' religion in their credit decisions. For religious institutions applying for small business loans, some lenders improperly utilized a questionnaire that contained explicit inquiries about an applicant's religion.

Small Business Data Collection Rule

In September 2021, the CFPB issued, for public comment, a proposed rule amending Regulation B to implement changes to the Equal Credit Opportunity Act (ECOA) created by Section 1071 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). Congress enacted Section 1071 for the purpose of facilitating enforcement of fair lending laws enabling communities, governmental entities, and creditors to identify business and community development needs and opportunities for women-owned, minority-owned, and small businesses. Under Section 1071, financial institutions are required to collect and maintain certain data for small business applicants, while also restricting access to certain information. As part of the data collection, financial institutions must limit or "firewall" access to the race, ethnicity, and sex data from employees in a position to make credit decisions about those applications. Financial institutions must submit this data to the CFPB annually, and thereafter, the CFPB must make the data available to the public.

Consistent with Section 1071, the proposed rule would require covered financial institutions to disclose application data from small businesses and demographic information about credit applicants, including those that are owned by women or minorities. The CFPB's proposal also addresses its approach to privacy interests and the publication of Section 1071 data, shielding certain demographic data from underwriters and other persons, recordkeeping requirements, enforcement provisions, and the proposed rule's effective and compliance dates.

The CFPB's anticipated change is likely to elevate fair lending issues with respect to small business lending, which may become subject to the levels of regulatory and public scrutiny observed with home mortgage lending. Changes are expected to go into effect in 2022 as the comment period ended on January 6, 2022.

FTC Consumer Fraud Minority Report

The FTC recently released a "Serving Communities of Color Report" that details fraud and consumer issues having a disproportionately negative impact on communities of color. This report is the latest installment released by the FTC on the topic and follows prior initiatives, such as the 2014 "Every Community Initiative" that helped the FTC develop a strategic plan for addressing disparities in communities of color, and the June 2016 "Combating Fraud in African-American and Latino Communities Report," which focused on reducing fraud in Black and Latino communities.

The report focuses its findings on Black and Latino communities and summarizes the FTC's efforts over the last five years to address and understand consumer issues that have disproportionately impacted these communities. The report explains that the FTC filed more than 25 actions involving alleged conduct that either targeted or disproportionately impacted communities of color. The report includes main law enforcement areas affecting communities of color: automobile buying; for-profit school advertising; marketing prepaid cards; government impersonators; marketing for inmate services; jobs and money-making opportunities; credit, background checks, and access to housing; and payday loans and debt collection.

Some of the most relevant insights from the 2021 report data include:

- Majority white and Latino communities were more susceptible to impersonator scams, while majority Black communities faced issues with credit bureaus at higher rates.
- When compared against majority white communities, majority Latino communities filed more reports related to credit bureaus, banks and lenders, debt collection, auto issues, and business opportunities.
- The FTC analyzed 23 cases that revealed typical cases for consumers in majority Black communities involving issues with, among other things, payday loan applications, student debt relief programs, and money-making schemes, such as false "work-at-home-business opportunities" and "employment scams" where scammers promise large profits for selling certain products.
- Reports from majority Black and Latino communities show that these groups are more likely to pay scammers in ways that have few, if any, fraud protections by paying with the following: cash, cryptocurrency, money orders, and debit cards. In contrast, reports from majority white communities show that this group is more likely to pay scammers with credit cards.

Additionally, the report emphasizes that outreach programs are an integral part of the FTC's work to protect and educate consumers in all communities. The FTC notes that it has grown its outreach efforts to reach communities of color by listening to and working with trusted sources in those communities to deliver consumer protection messages in an effective way. Additionally, the FTC has furthered its community outreach efforts by working with national and local minority organizations to educate consumers, create consumer education materials in multiple formats and languages, and create educational materials to alert people to scams and offer helpful information to those affected financially by COVID-19.

Looking Forward

2021 saw the initiatives of the Biden administration gathering steam, and with that, significant updates within fair lending. It is expected that federal and state regulators will continue to focus on fair lending issues in 2022. Practitioners, companies, and business owners operating in this landscape should pay close attention to policy changes released by the CFPB, the FTC, and local jurisdictions related to mortgage lending and consumer fraud affecting minority communities.

KEY TRENDS AND LEGISLATION IN HEALTH CARE

Legislation

Congress Passes Bipartisan "No Surprises Act"

In the final days of 2020, Congress included the bipartisan "No Surprises Act" in the omnibus spending bill. The legislation addresses practices known as surprise billing and balance billing. Surprise billing happens when patients unknowingly receive care from providers that are outside of their health plan's network, and can occur with both emergency and non-emergency care. Balance billing, where a provider charges a patient the remainder of what his or her insurance does not cover, is currently prohibited in Medicare and Medicaid.

Beginning January 1, 2022, out-of-network providers are prohibited from billing for emergency services at a rate higher than applicable in-network cost-sharing. Health plans also are required to treat out-of-network services as if they were in-network for purposes of calculating patient cost-sharing. Most importantly, the legislation included arbitration procedures to address disagreements between providers and payors. Under the Act, if providers and payors cannot reach agreement on payment after a 30-day open negotiation period, then either party may invoke the federally regulated independent dispute resolution (IDR) process.

On September 30, the Biden administration released an interim final rule dramatically affecting the contours of this IDR process. According to the rule, the IDR entity "must begin with the presumption that the QPA is the appropriate . . . amount." Any deviation from "the offer closest to the QPA" must be clearly demonstrated by supporting information that the value of the item or service is "materially different from the QPA." This interim final rule is a promising step towards consumer affordability that also balances transparency and predictability for insurers.

The Growth and Future of Telehealth: COVID-19 and Beyond

Since the onset of the COVID-19 pandemic, the United States has experienced an unprecedented growth in telehealth utilization. Following an initial spike in the early stages of the pandemic, overall telehealth utilization represents roughly 17% of all outpatient/office visits. The results widely differ according to medical specialty with the highest rates of utilization in the mental health field.

With this explosive growth in such a short time, regulators have scrambled to keep up with this shift toward telehealth. In response to the pandemic, most states added a range of temporary authorizations for telehealth services. Additionally, many states temporarily introduced payment parity rules to reimburse providers for telehealth services at the same amount as in-person visits. Indeed, several states, including California, have passed legislation to permanently establish payment parity for telehealth services. As the country emerges from the pandemic, it remains to be seen how various states and the federal government will address temporary telehealth measures. However, given the operational efficiency arguments and recent legislative changes, it appears telehealth is here to stay.

New Regulatory Mandate on Health Care Price Transparency

In October 2020, the Department of Health and Human Services, Department of Labor, and Department of Treasury issued final rules to enhance price transparency in the health care field. The Transparency in Coverage final rule requires most private health care plans to not only make cost-sharing estimates readily available to enrollees, but also to publicly disclose the negotiated rates between providers and plans. While designed to combat purported informational asymmetries between the insurers and insured, the law will likely have negative countervailing effects. For instance, this price transparency may reduce incentives for

providers to offer lower rates in order to become a preferred provider. Moreover, factoring in compliance costs to insurers may eventually lead to higher costs on premiums. In effect, the final rule may lead to the very outcome it sought to avoid from the outset: higher health care costs for consumers.

California Law Expands Mental Health Coverage

On January 1, 2021, California Senate Bill 855 (SB 855) went into effect, dramatically expanding mental health coverage requirements for health plans and insurers that are subject to California insurance laws. Among the many revisions to the 1999 mental health parity law, SB 855 expanded the scope of coverage of mental health/substance use disorders (MH/SUD) beyond the prior specified list to include all such disorders "as defined by preeminent national and international bodies." More importantly, SB 855 declares extensive standards for evaluating what constitutes medically necessary treatment. If the medically necessary treatment is not available in network, plans and insurers are required to "arrange coverage" for out-of-network services. Moreover, the bill prohibits discretionary authority on behalf of the plan to determine eligibility for benefits or coverage. The stringent statutory definition for medical necessity, coupled with the bill's other internal compliance requirements, may lead to increased mental health parity litigation. Given these notable changes to prior law, insurers should be wary of this potential litigation risk and tailor their policies to ensure compliance under SB 855.

The Individual Mandate Survives Another Round at the Supreme Court

The Affordable Care Act (ACA) survived the third challenge to the law's constitutionality since its passage just over a decade ago. In *California v. Texas*, a group of states and two individuals challenged the ACA's minimum essential coverage provision, known as the individual mandate. The case comes on the heels of *National Federation of Independent Businesses v. Sebelius*, which upheld the individual mandate on the basis of Congress' taxing power. However, since the holding in *Sebelius*, Congress revised the individual mandate to reduce the penalty for noncompliance to zero dollars. The challengers argued that the individual mandate was no longer constitutional because it does not generate revenue, and thus the entire ACA must fall.

In a 7-2 opinion, the Court held that none of the states nor the individual petitioners had standing to sue. The Court dismissed the claims asserted by individual citizens as (despite having to purchase health insurance) they were not harmed by the zeroed-out penalty provision. Moreover, the states failed to show "injury fairly traceable to the defendants allegedly *unlawful* conduct" since they could not point to the connection between the mandate and greater enrollment in state-financed health care. Although the constitutionality of the ACA remains intact, we will likely see another installment in the ACA constitutional saga in the coming years.

MORTGAGE

New York Court of Appeals Settles Statute of Limitations Issues Related to Mortgage Foreclosures

The New York Court of Appeals issued a consolidated order in four separate mortgage foreclosure appeals addressing issues related to the timeliness of mortgage foreclosure actions, which the court noted involves the "intersection of two areas of law where the need for clarity and consistency are at their zenith: contracts affecting real property ownership and the application of the statute of limitations." The individual cases are: (1) *Freedom Mortgage Corporation v. Engel*; (2) *Ditech Financial, LLC v. Naidu*; (3) *Wells Fargo Bank v. Ferrato*; and (4) *Vargas v. Deutsche Bank Nat'l Trust Co.*

Engel and *Naidu* questioned whether a voluntary discontinuance of a prior foreclosure action revoked the lender's acceleration of the mortgage debt. Under New York law, a foreclosure action commenced more than six years after acceleration is time-barred.

The plaintiffs in both cases argued that their subsequent foreclosure actions were timely commenced because they had affirmatively revoked prior elections to accelerate the mortgage debt by voluntarily withdrawing those complaints. Despite the trial court holding that the respective accelerations were revoked by a voluntary discontinuance of the preceding foreclosure action, the Appellate Division reversed in each case, dismissing the actions as time-barred.

The Court of Appeals rejected the Appellate Division's approach, noting that it is both "analytically unsound as a matter of contract law" and "unworkable from a practical standpoint." The Court of Appeals reasoned that the Appellate Division's decision suggested that the "revocation inquiry turns on an exploration into the bank's intent, accomplished through an exhaustive examination of post-discontinuance acts." The Court of Appeals found this approach inconsistent with the policy underlying the statute of limitations because under this rejected interpretation, timeliness "cannot be ascertained with any degree of certainty," an outcome repeatedly disfavored by the court.

Instead, the Court of Appeals adopted a "clear rule" that when acceleration occurs by the filing of a foreclosure complaint, the lender's voluntary discontinuance of that action constitutes an affirmative act of revocation as a matter of law, absent an express, contemporaneous statement to the contrary by the lender. This decision adheres to precedent favoring consistent, straightforward application of the statute of limitations, which serves the objectives of "finality, certainty, and predictability," to the benefit of borrowers and lenders.

In *Ferrato* and *Vargas*, the Court of Appeals addressed whether specific actions on behalf of a lender constitute acceleration of mortgage debt, thereby commencing the six-year statute of limitations period.

In *Vargas*, the borrower commenced an action under Real Property Actions and Proceeding Law § 1501(4) seeking to discharge a mortgage on real property based upon the expiration of the statute of limitations. The borrower alleged that the lender's default letter sent in August 2008 accelerated the debt. The trial court found that the default letter was insufficient to accelerate the loan, but upon the borrower's motion to renew, denied the lender's motion to dismiss and granted summary judgment in favor of the borrower to discharge the mortgage. The Appellate Division affirmed. The Court of Appeals reversed, holding that the default letter did not accelerate the mortgage debt because it did not seek immediate payment of the entire balance, but rather "referred to acceleration only as a future event, indicating the debt was not accelerated at the time the letter was written."

In *Ferrato*, the Court of Appeals held that the lender's prior foreclosure action did not serve to accelerate the borrower's modified loan because

the lender did not reference the loan modification or attach the modified loan agreements, which had materially distinct terms, stating that "the deficiencies in the complaints were not merely technical or de minimis and rendered it unclear what debt was being accelerated — the commencement of these actions did not validly accelerate the modified loan."

These decisions represent a clear win for lenders and servicers operating in New York. For several years, New York courts have grappled with statute of limitations issues in foreclosure actions and what constitutes a revocation of the acceleration of mortgage debt. These decisions create a clear rule in New York regarding the statute of limitations in foreclosure actions.

Florida Supreme Court Settles Question of Conflicting "Borrower" Definition in Note and Mortgage

In *WVMF Funding v. Palmero*, 320 So. 3d 689, 2021 Fla. LEXIS 1054, 46 Fla. L. Weekly S 195 (June 24, 2021), the Florida Supreme Court accepted jurisdiction to provide guidance to courts in resolving conflicts created by inconsistently used terms in notes and mortgages, in particular the definition of a "borrower." In so doing, the court reiterated previous decisions holding that the "mortgage must be read alongside the note it secures" and "the note prevails in the event of the conflict."

Robert Palmero and his wife Luisa Palmero obtained a reverse mortgage on their residence. Among the documents they signed were the promissory note and the mortgage instrument. The note was signed by Mr. Palmero only, which identified him as the "borrower." In addition to Mr. Palmero, the mortgage was signed by Mrs. Palmero, below a sentence that read, "BY SIGNING BELOW, Borrower accepts and agrees to the terms contained in this Security Instrument and in any rider(s) executed by Borrower and recorded with it."

Following Mr. Palmero's death, his estate did not repay the accelerated loan balance, prompting a judicial foreclosure action in the Circuit Court for Miami-Dade County. Mrs. Palmero opposed foreclosure, arguing that she was a "co-borrower" under the mortgage based on the following language in the mortgage creating an exception to enforcement of the foreclosure provision: "A Borrower dies and the [mortgaged] Property is not the principal residence of at least one surviving Borrower."

The Circuit Court found that Mrs. Palmero was not a "co-borrower," but denied foreclosure based on a federal statute governing the insurability of reverse mortgages by the secretary of the Department of Housing and Urban Development. On appeal, the Third District Court of Appeal held that the Circuit Court had erred in determining that Mrs. Palmero was not a "co-borrower" because, as a matter of law, the mortgage defined her as a "borrower."

The Florida Supreme Court accepted jurisdiction to resolve "the express and direct conflict between the Third District's decision" and the Supreme Court's previous decisions in *Graham v. Fitts*, 53 Fla. 1046, 43 So. 512, 513-14 (Fla. 1907) (requiring joint construction of note and mortgage in foreclosure actions), and *Hotel Mgmt. Co. v. Krickl*, 117 Fla. 626, 158 So. 118, 119 (Fla. 1934) (setting forth the "general rule" for foreclosure actions that "if there is a conflict between the terms of a note and mortgage, the note should prevail").

The Florida Supreme Court quashed the Third District Court of Appeals' holding that Mrs. Palmero was a "borrower" under the mortgage "as a matter of law." Explaining that courts should read the mortgage and the note together and should "look to the note to resolve any conflict," the court said that the note's definition of the "borrower" as only Mr. Palmero was dispositive, regardless of any references to Mrs. Palmero as a "borrower" in the mortgage.

CFPB Issued Rule Delaying the Mandatory Compliance Date of the New General Qualified Mortgage Final Rule

On April 27, 2021 the Consumer Financial Protection Bureau (CFPB) issued a final rule to delay the mandatory compliance date for the General QM Final Rule until October 1, 2022. The CFPB stated that it issued the rule "to help ensure access to responsible, affordable mortgage credit and to preserve flexibility for consumers affected by the COVID-19 pandemic and its economic effects." The mandatory compliance was originally set for July 1, 2021.

Becoming effective on March 1, 2021, the General QM Final Rule was created to address the expiration of the GSE patch, which permits certain mortgage loans eligible for purchase or guarantee by Fannie Mae and Freddie Mac (GSEs) to qualify as QM loans despite not meeting all requirements of the general QM loan definition. The General QM Final Rule, among other changes, replaced the 43% debt-to-income (DTI) limit in the General QM loan definition with a price-based threshold that compares a loan's annual percentage rate to the average prime offer rate for a comparable loan.

As a result of the new rule, lenders can continue to originate QM loans using the old general QM loan definition for loans with an application received before October 1, 2022. Additionally, the GSE patch will continue to exist until October 1, 2022.

Blunting some of the effectiveness of this new rule, Fannie Mae in Lender Letter LL-2021-09 and Freddie Mac in Bulletin 2021-13 communicated that they would nevertheless move forward with generally only purchasing loans originated on or after July 1, 2021 if they conformed to the requirements of the General QM Final Rule. This effectively ended, as of July 1, 2021, the GSE patch as an alternative means for lenders to originate a QM loan.

Considering the CFPB's announcement in February 2021 that it intended to review the General QM Final Rule, there was speculation that the CFPB issued this rule to buy time to amend or repeal the General QM Final Rule, which was issued under the Trump administration. As of the date of this publication, neither has occurred. Regardless, lenders should continue to monitor the actions of the GSEs and the CFPB for future developments regarding the General QM Final Rule.

CFPB Issued the 2021 Mortgage Servicing COVID-19 Rule

On June 28, 2021, the CFPB issued a final rule to amend Regulation Z's mortgage servicing requirements to "establish temporary special safeguards to help ensure that borrowers have time before foreclosure to explore their options, including loan modifications and selling their homes."

The rule, which applies to federally regulated mortgage loans secured by a principal residence, accomplished four things:

1. It created "temporary special COVID-19 procedural safeguards," which limited the situations where a servicer could "mak[e] the first notice or filing required by applicable law for any judicial or non-judicial foreclosure process until after December 31, 2021."

2. It allowed servicers to offer borrowers experiencing COVID-19-related hardships

streamlined loan modification options based on an incomplete application, so long as the modification options met certain criteria.

3. It amended Regulation Z's "early intervention requirements" by requiring servicers until October 1, 2022 to discuss with certain delinquent borrowers COVID-19-related information at specific points of live contact.

4. It clarified "more precisely when the servicer must renew reasonable diligence efforts" when a borrower is in a short-term payment forbearance program for a COVID-19 hardship based on an incomplete application.

While the rule's "procedural safeguards" are narrower than the original foreclosure prohibition discussed in the proposed rule issued in April of 2021, it still limited servicers' ability to initiate foreclosures.

Although this rule did not go into effect until August 31, 2021, both Fannie Mae and Freddie Mac (GSEs) issued policies that prohibited servicers between July 31, 2021 and August 31, 2021 from initiating any foreclosure activities that would violate the rule, essentially moving up the effective date of this rule for GSE loans to July 31, 2021.

Desktop Appraisals Are Here to Stay

Desktop appraisals, a once temporary and largely popular method of conducting mortgage loan appraisals, will become permanent according to an announcement by the Federal Housing Finance Agency (FHFA). The quicker and less cumbersome method of conducting appraisals was initially implemented as one of several temporary fixes by the FHFA in March 2020 to ease the burden on the mortgage industry among the lockdowns and social distancing necessitated by COVID-19. While these flexibilities largely expired in 2021, Sandra Thompson, acting director of the FHFA, announced that both Fannie Mae and Freddie Mac will allow appraisals to be conducted remotely beginning in early 2022.

The announcement, made at the Mortgage Bankers Association's Annual Convention and Expo in October 2021, was largely well-received. According to Thompson, the change will especially benefit

Desktop appraisals, a once temporary and largely popular method of conducting mortgage loan appraisals, will become permanent according to an announcement by the Federal Housing Finance Agency (FHFA).

those appraisers in rural communities that often have to travel large distances between properties.

"This can help each appraiser complete more loans in a day and can also help rural communities more readily obtain a necessary appraisal when the borrower is purchasing a property," Thompson said. "This certainly should allow lenders, borrowers, and appraisers alike to take advantage of the efficiency gains that desktop appraisals can provide."

Desktop appraisals are often conducted using public records such as listings and tax appraisals and generally obviate the need for appraisers to physically inspect the property. While faster and more convenient, an appraiser could incur additional risks if an appraisal is made on inaccurate data. Nevertheless, given its successful use in 2020 and 2021, the benefits appear to outweigh the risks.

Loan Origination Complaints Spike

According to a September 2021 report published by the CFPB, consumer complaints related to loan origination issues have significantly increased during the COVID-19 pandemic.

In its research brief, the CFPB compiled data from 2018 to 2020 and determined that the number of loan origination complaints, spearheaded by mortgage complaints, rose 50%. According to the CFPB, the spike in complaints related to the financing of existing mortgages is likely attributed to

consumers trying to take advantage of historically low interest rates.

In contrast, the CFPB found that the number of delinquent mortgage servicing complaints fell in 2018 and remained low throughout 2020. The CFPB attributes this statistic to the effectiveness of the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which provided relief for struggling homeowners with federally backed mortgages.

The data compiled by the CFPB also showed a racial and socioeconomic link to the types of complaints that were received. Complaints pertaining to financial struggles and identity theft were more predominant among consumers with lower incomes and higher shares of Black and Hispanic borrowers, while those with higher incomes from predominately white communities submitted more complaints about the actions or inactions of their lender and servicer.

According to the CFPB, this data is "especially concerning" and reflective of a growing wealth gap between communities where "new credit, especially mortgages and mortgage refinances, may be disproportionately available to consumers from communities with higher AMIs and a greater share of white, non-Hispanic residents. Past barriers limiting access to mainstream credit for racial minorities, the long-term impact of the 2008 mortgage crisis, and continued inequality in access continue to determine the types of opportunities consumers have—and these contexts shape consumer interactions with the CFPB," the report added. The CFPB concluded that these differences "serve as one more reminder of the starkness of the racial wealth divide in the United States and its relationship to credit access, especially housing finance."

PAYMENT PROCESSING AND CARDS

Regulatory Developments

Throughout the year, Congress has confirmed President Biden's nominations for various positions. Notably for payment processors, President Biden chose Lina Khan as the new Federal Trade Commission (FTC) chair and Rohit Chopra as the new Consumer Financial Protection Bureau (CFPB) acting director. While Khan has historically focused on Big Tech and privacy concerns, all businesses should prepare for a more active commission than they have seen in prior years. Chopra served as the CFPB assistant director between 2010 and June 2015 and thereafter became an FTC commissioner. During his stint at the FTC, lawsuits and administrative actions were brought in the payment processing and debt collection industries. Businesses should be on high alert and ensure compliance with applicable laws and regulations as these two agencies ramp up enforcement actions.

The Payday Lending Rule continues as an area of heated debate. Originally passed in 2017, the rule has faced persistent challenges. In October 2021, the Fifth Circuit issued a one-paragraph order to extend a stay on CFPB payday lending regulations currently challenged by the Community Financial Services Association of America Ltd. and the Consumer Service Alliance of Texas. The stay will allow small dollar lenders to postpone the June 2022 compliance date.

In October 2021, the CFPB ordered Amazon, Apple, Facebook, Google, PayPal, and Square to provide information regarding consumer payment products and their underlying business practices. The orders request information on how the companies collect, use, and share information, any restrictive access policies that may limit merchants' abilities to use other payment services, and practices related to consumer privacy protection, customer service, and compliance with consumer protection laws.

Money transmission also has been the focus of regulators. In particular, in September, the Conference of State Bank Supervisors (CSBS) released the Model Transmission Modernization Act (model law) to replace the 50 state-specific money transmitter laws with a nationwide standard. Unless the states adopt the model law, no change will affect any existing state money transmission laws. If enacted by the states, the law will create a common regulatory regime for money transmission, including stored value, sale of payment instruments, and transmission of fiat and virtual currency.

California passed a bill requiring money transmitters to display a toll-free telephone number on their websites for customers to receive live assistance. The telephone number must operate at least 10 hours per day, Monday through Friday, excluding federal holidays. Receipts issued to customers also must contain the customer service phone number. The law will take effect on July 1, 2022.

Litigation and Enforcement Actions

In a Form 10-K filed in February, PayPal Holdings, Inc. (PayPal) announced that it had received a civil investigative demand (CID) from the CFPB on January 21 "related to Venmo's unauthorized funds transfers and collections processes, and related matters." PayPal owns and operates Venmo as part of its digital wallet portfolio.

As reported by *The Wall Street Journal* in March 2019, "In a bid to curb losses on its platform, Venmo is threatening to sic debt collectors on some users who carry negative balances in their accounts, according to customer-service emails reviewed by *The Wall Street Journal*. Venmo also recently amended its user agreement to give itself the power to recover money its customers owe by seizing it from their other accounts at PayPal."

Though collection practices may have been the primary subject of the CFPB's CID, the investigation is representative of increased scrutiny that payment and other financial companies have experienced and will likely continue to experience under the Biden administration.

FTC Bureau of Consumer Protection Acting Director Daniel Kaufman said, "The message here is simple for mobile banking apps and similar services: Don't lie about your customers' ability to get their money when they need it."

In March, the FTC announced a settlement with Beam Financial, Inc. (Beam), a mobile banking app, whereby Beam was banned from offering any service that may be used to deposit, store, or withdraw funds, and must give a full refund to users. Beam also is prohibited from misrepresenting the interest rates, restrictions, and other aspects of any financial product or service.

The FTC alleged that Beam falsely promised users 24/7 access to their funds and high interest rates on their accounts. Beam promised its users they could make transfers out of their accounts and would receive their requested funds within three to five business days. However, some users waited weeks or months to receive the funds. Beam also claimed users would receive at least 0.2% or 1.0% on their accounts, but many users received an interest rate of 0.04%. Consumers also stopped earning interest after requesting to withdraw their money even though Beam did not return their funds until weeks or months later.

As part of the settlement, full refunds — including interest — were required to be provided to all of Beam's customers, which consisted of at least $2.6 million in November 2020. Further, Beam must periodically update the FTC on its refund efforts, including identifying any consumer complaints.

FTC Bureau of Consumer Protection Acting Director Daniel Kaufman said, "The message here is simple for mobile banking apps and similar services: Don't lie about your customers' ability to get their money when they need it."

The commission vote approving the stipulated final order was 3-1, with then-FTC Commissioner and current CFPB Director Rohit Chopra voting "no."

In July, the FTC voted to approve seven omnibus resolutions authorizing staff attorneys to use compulsory process to investigate key enforcement targets. The vote fell along party lines, with Democratic Commissioners Lina Khan, Rohit Chopra, and Kelly Slaughter voting in favor of the resolutions, and Republican Commissioners Christine Wilson and Noah Phillips voting against them. The vote — along with several others made at the same public hearing — signaled that Khan intends to remake the FTC into a much more aggressive, and potentially much more partisan, consumer protection agency.

As explained in the FTC's press release, the omnibus resolutions authorize compulsory process for key enforcement priorities:

"Priority targets include repeat offenders; technology companies and digital platforms; and healthcare businesses such as pharmaceutical companies, pharmacy benefits managers, and hospitals. The agency is also prioritizing investigations into harms against workers and small businesses, along with harms related to the COVID-19 pandemic. Finally, at a time when merger filings are surging, the agency is ramping up enforcement against illegal mergers, both proposed and consummated."

FTC staff attorneys must still seek commission approval before issuing compulsory process demands, which are generally issued as civil investigative demands or subpoenas. But with these resolutions, any single FTC commissioner can authorize compulsory process without seeking the input of any other commissioner or a vote of the entire commission.

"The reforms are designed to ensure that our staff can comprehensively investigate unlawful business practices across the economy," said Khan. "They will help relieve unnecessary burdens on staff and cut back delays and 'red tape' bureaucracy when it comes to advancing our Commission's law enforcement priorities."

PREDATORY LENDING

The term "predatory lending" generally encompasses both private lawsuits and official governmental enforcement actions against lenders — including local and national banks, online lenders, nonbank entities, or nontraditional lending entities — asserting that such entities impose unfair, deceptive, or abusive loan terms on borrowers. In many instances, these actions seek to impose state interest rate caps on entities that claim to be exempt from these caps based on various legal theories. Predatory lending actions also can include claims of discriminatory lending (*e.g.*, placing more onerous loan conditions on minority borrowers), violations of the Truth in Lending Act or Fair Debt Collection Practices Act, and related state UDAAP claims.

2021 brought several notable developments in this area of consumer financial law at both state and federal levels and across executive, legislative, and judicial branches. One executive branch development that will undoubtedly have an impact throughout 2022 and beyond was the confirmation of Rohit Chopra as the new director of the Consumer Finance Protection Bureau (CFPB). Chopra's track record, while serving as the CFPB assistant director from 2010 to 2015 and as a Federal Trade Commission commissioner from 2018 to 2021, suggests that under his leadership, the CFPB will take on more aggressive rulemaking and enforcement efforts against purported predatory lending practices. On the legislative side, Congress took action this year to overturn the "True Lender Rule" that the Office of the Comptroller of the Currency (OCC) finalized in 2020.

State legislatures have been active in this space too, as demonstrated by the passage of the Illinois Predatory Loan Prevention Act in March 2021. And, on the judicial front, the Court of Appeals for the Ninth Circuit issued a September 2021 decision in *City of Oakland v. Wells Fargo*, which examined proximate cause principles under the Fair Housing Act (FHA) where a municipality claimed injuries allegedly caused by a bank's lending practices.

Congress Overturns OCC's True Lender Rule Under Congressional Review Act

In October 2020, the OCC settled on the bright-line "True Lender Rule" to clarify whether a national bank or federal savings association (collectively, "national bank") was the "true lender" in a partnership between the national bank and a third party — primarily fintech companies. These relationships between national banks and fintech companies began to surface as fintech companies entered the loan marketplace, looking to create affordable lending options for borrowers. Opponents claimed that this type of partnership can be used to avoid state interest rate limits by using the national bank as an artifice for the "true lender," the fintech company, to avoid interest rate caps in the state where the loan is issued. In creating the True Lender Rule, the OCC announced its intention to provide clarity for banks, borrowers, and partnering financial companies through a bright-line test to identify the lender in a transaction. The rule established simply that when a national bank makes a loan, it is the true lender if, as of the date of origination, it is: (1) named as the lender in the loan agreement or (2) funds the loan.

That rule and the clarity it provided, however, did not last long. Acting under the Congressional Review Act (CRA), the Senate voted in May 2021 to overturn the True Lender Rule, and the House followed suit on June 24, 2021. President Biden, whose administration had expressly supported overturning the True Lender Rule, signed the joint resolution on June 30, 2021.

The decision by Congress to overturn the OCC's action stems from criticism by consumer advocates as to the construction of the True Lender Rule and its potential loopholes for supposedly usurious lending tactics. On January 5, 2021, New York Attorney General Letitia James led several attorneys general in filing suit against the OCC and Acting Comptroller Brian Brooks, alleging that the True Lender Rule was in direct conflict with the National Bank Act (NBA). Under the NBA, national banks are

capped at charging a maximum interest rate set by the state where the bank's headquarters are located. Yet, third parties and nonbank lenders can only charge the maximum rate allowed in the state where the loan is issued. The complaint alleged that, under the True Lender Rule, the national bank and third-party partnership allows third parties to take advantage by charging consumers the national bank's maximum interest rate. The complaint also alleged that the OCC rushed to issue the True Lender Rule, citing the unprecedented 4,000 comments received on the proposed rule in September 2020, of which a majority were in opposition.

By using the CRA, Congress can expedite procedures by which it may disapprove regulatory rules issued by federal agencies via a joint resolution. Generally, either house may submit a disapproval resolution within 60 days after Congress receives the proposed agency rule. The CRA also allows for a new Congress to review regulations issued in the last 60 legislative days under a previous session of Congress. Once a resolution is passed in both houses, it goes to the president for signature. If so enacted, the agency rule may not take effect, and the agency is prevented from issuing a "substantially similar" rule. Thus, Congress returned the issue to the status quo that existed before the True Lender Rule was adopted by the OCC and has prevented the OCC from adopting a "substantially similar" rule in the future.

In the absence of the True Lender Rule, the question of whether a bank or fintech company is the true lender will return to being determined on a case-by-case basis, with standards varying by state, court, and the circumstances of each case. The absence of a bright-line rule creates an environment of uncertainty for banks and lenders regarding the legality of and ability to collect loans based on the agreed upon interest rates.

Illinois Passes Predatory Loan Prevention Act

On March 23, 2021, Illinois Governor J.B. Pritzker signed the Illinois Predatory Loan Prevention Act (PLPA) into law. The PLPA imposes sweeping changes to lending laws in Illinois and contains broad language that creates substantial uncertainty for the state's lenders and borrowers.

By using the CRA, Congress can expedite procedures by which it may disapprove regulatory rules issued by federal agencies via a joint resolution.

The drafters of the PLPA relied heavily on the federal Military Lending Act (MLA), which instituted an annual percentage rate cap for interest charged on loans to military service members and their dependents. The MLA contains an inclusive definition for calculating the APR, typically referred as the MAPR. In addition to the interest rate, the MAPR includes fees, charges imposed for credit insurance, debt cancellation and suspension, and other credit-related ancillary products sold in connection with the transaction. If voluntary, these are excluded from the calculation of the normal APR.

Lenders cannot charge interest and fees that, when added together, would exceed a 36% MAPR. This requirement was intended to provide extra protection to service members from lending practices that "could pose risks for service members and their families," while also promoting military readiness and service member retention. In other words, Congress attempted to set the MAPR to meet the needs of a particular group.

By contrast, the PLPA applies the MLA's lending rules to *all* Illinois consumers, and drastically increases the scope of the law beyond the MLA. The PLPA's stated purpose is "to protect consumers from predatory loans consistent with federal law and the Military Lending Act which protects active duty members of the military," and it "shall be liberally construed to effectuate its purpose." Unlike the federal MLA, which limits its application to a particular group with specific gaps in its coverage, the Illinois law grants the MARP limit to all consumers and applies the MLA to all transaction types.

The PLPA applies to all parties that offer or make loans in the state of Illinois, and it attempts to make banks and other regulated financial service providers involved in partnership arrangements with nonbanks the "true lender" under Illinois law. While "[b]anks, savings banks, saving and loan associations, credit unions, and insurance companies … are exempt from the provisions of this Act," the PLPA is drafted to make it very difficult for nonbank lenders to partner with these institutions by including "true lender" concepts to these arrangements. The PLPA does this by stating that it applies to nonbank partners if:

"1. the person or entity holds, acquires, or maintains, directly or indirectly, the predominant economic interest in the loan; or

2. the person or entity 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

3. the totality of the circumstances indicate that the person or entity is the lender and the transaction is structured to evade the requirements of this Act. Circumstances that weigh in favor of a person or entity being a lender include, without limitation, where the person or entity:

    i. indemnifies, insures, or protects an exempt person or entity for any costs or risks related to the loan;

    ii. predominantly designs, controls, or operates the loan program; or

    iii. 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 Tale of Two Cities: Ninth Circuit's *City of Oakland* Follows Supreme Court's *City of Miami* to Define Proximate Cause Under the FHA

In September 2021, the Ninth Circuit sitting *en banc* issued its decision in *City of Oakland v. Wells Fargo*. The decision is notable as the only federal circuit court opinion analyzing proximate cause under the Fair Housing Act (FHA), following the U.S. Supreme Court's instruction in *City of Miami* that "foreseeability alone is not sufficient to establish proximate cause under the FHA." *See Bank of America Corp. v. City of Miami, Florida*, 137 S. Ct. 1296, 1305 (2017). Like *City of Miami*, and many other similar suits that have arisen around the country, *City of Oakland* involved claims by a municipality that banks engaging in alleged discriminatory lending practices had caused an increase in foreclosures, which in turn decreased property values and the municipalities' tax revenue and increased public service expenses.

Understanding the Ninth Circuit's *City of Oakland* decision requires looking back to the U.S. Supreme Court's 2017 decision in *City of Miami*. There, the city of Miami, FL claimed that, by engaging in discriminatory lending practices through allegedly placing more onerous conditions on loans made to minority borrowers, the defendant banks had caused higher foreclosure rates and resulting vacancies in minority neighborhoods, which in turn caused the city to lose property tax revenue and spend more on various municipal services. Prior to reaching the Supreme Court, the Eleventh Circuit concluded that the city's injury fell within the "zone of interests" protected by the FHA, and that the city had "plausibly alleged that its financial injuries were foreseeable results of the Banks' misconduct."

The Supreme Court reversed. Due to the interconnected nature of the housing market with economic and social life, the Court acknowledged that a violation of the FHA may cause "ripples of harm" to flow beyond a defendant's conduct, but nothing in the FHA indicates that Congress intended to provide a remedy for that distant harm. The Court concluded that, in the context of the FHA, "foreseeability alone does not ensure the close connection that proximate cause requires." The Court declined, however, to "draw the precise boundaries of proximate cause under the FHA," holding instead that "lower courts should define, in the first instance, the contours of proximate cause under the FHA and decide how that standard applies to the City's claims for lost property-tax revenue and increased municipal expenses."

The first circuit court to take a pass at "drawing the boundaries" of proximate cause was the Eleventh

Circuit after *City of Miami* was remanded. The Eleventh Circuit adopted a broad view of proximate cause that once again allowed the city's claim to proceed. *See City of Miami v. Wells Fargo & Co.*, 923 F.3d 1260 (11th Cir. 2020). That decision, however, was vacated when the city voluntarily dismissed its suit, while the defendants' second petition for certiorari to the Supreme Court was pending, thereby mooting the issue. *See Wells Fargo & Co. v. City of Miami, Florida*, 140 S. Ct. 1259 (2020) (Mem.) (citing *United States v. Munsingwear, Inc.*, 340 U.S. 36 (1950)).

The Ninth Circuit then weighed in with *City of Oakland v. Wells Fargo & Co.* The initial panel decision, much like the Eleventh Circuit's vacated decision, held in early 2020 that the text and legislative history of the FHA indicated that Congress intended the statute to have a broad scope that would include less direct injuries, such as those asserted by the city. But that opinion, too, was destined for precedential defrocking, as it was vacated when the Ninth Circuit granted rehearing *en banc*.

After rehearing, in September 2021, the Ninth Circuit *en banc* concluded that the city had failed to sufficiently plead proximate cause for its reduced tax revenue claim and increased municipal spending claims. The court looked to the legislative history of the FHA, as well as multiple U.S. Supreme Court decisions on proximate cause, and concluded that the city's alleged harm was multiple steps removed from the alleged FHA violations. Moreover, the alleged increase in foreclosures was not "surely attributable" to discriminatory lending: A borrower's default may be attributable to many independent factors, including "job loss, a medical hardship, a death in the family, a divorce, a fire or other catastrophe, Covid-19, broader economic trends, or any number of unpredictable causes not present when the loan was made." The number of variables and independent decisions not attributable to the defendant that are involved in causing a foreclosure and other variables affecting property values made the chain of causation too attenuated to support liability under the FHA.

Similar suits under the FHA brought by municipalities for injuries claimed to be caused by predatory lending have arisen in multiple jurisdictions around the country. Standing as the only precedential circuit court decision defining the scope of proximate cause under the FHA, *City of Oakland* will be a guiding beacon for courts navigating similar FHA claims in years to come.

In 2021, the two dominant forces that impacted the student lending sphere were the continuing COVID-19 pandemic and the change in presidential administrations. The pandemic resulted in a continuation of many student loan forbearance programs and likely minimized certain types of student loan litigation. The new administration led to an increase in federal regulation and enforcement actions, and likely emboldened state actors to increase their supervision activities in the student lending space.

STUDENT LENDING

Continuing Effects of the COVID-19 Pandemic

Federal Loans

This year also brought significant developments in the area of federal student loan repayment programs, with the pandemic serving as a backdrop for many of these actions.

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 pause on student lending payments was initially set to expire on September 30, 2020, on August 6, 2021, the Department of Education announced the final extension of these protections, which would go through January 31, 2022 due to the ongoing COVID-19 pandemic. The Department of Education hoped that additional time and a definitive end date would allow borrowers to plan for the resumption of payments and reduce the risk of delinquency and defaults after restart. While CARES Act relief was extended in the past, the department signaled that this extension would be the final time federal student loan borrowers would see a pause on their loan payments.

In addition to the continued pause on federally held student loans payments through the beginning of 2022, the Department of Education also announced that federally held student loan borrowers with a total permanent disability (TPD) will receive more than $5.8 billion in automatic student loan discharges. Borrowers who qualify for the loan relief will be identified through an existing data match with the Social Security Administration. The Department of Education first started matching receipts of relief in September 2021.

The Department of Education additionally announced two other policy items related to TPD borrowers. First, the department will indefinitely extend the policy it had previously announced in March of 2021 to stop asking these borrowers to provide information on their earnings. Previously, this process would result in the reinstatement of loans if and when borrowers did not respond. Second, the department began the elimination of the three-year monitoring period required under current regulations during the negotiated rulemaking that will begin in October. Both of these measures, the department noted, were aimed at short- and long-term steps to address TPD borrower's prior reinstatement concerns.

Private Litigation

Given the federal government's nearly two-year pause in much of its student loan enforcement activities, this year also saw a decrease in the litigation concerning private student loans. There were still, however, some interesting litigation decisions involving student loans and student loan servicers.

For example, on October 30, 2021, in *Porter v. Experian Info. Servs.*, the U.S.D.C. for the Northern District of Georgia granted the student loan servicer's motion to dismiss the plaintiff's claims under the FCRA for inaccurately reporting that the borrower's student loan payments were delinquent for the months that his account was in forbearance status. The court's decision relied on the fact that the borrower's delinquency began before he was granted forbearance status. As a result, the borrower could not make the threshold showing that the student loan servicer inaccurately reported the loan.

Similarly, the U.S.D.C. for the District of New Jersey determined that a report with a "past due" pay status is not inaccurate or misleading, despite information indicating that the consumer owes $0.00, and the account was transferred and closed out. This matter was just one of the many "pay status" cases that the federal courts addressed in 2021. Although courts initially differed on how they addressed these cases, the trend was gradually moving in defendants' favor, with many courts

concluding that it is not misleading to show a "past due" payment rating on an account that has a $0.00 balance because the payment rating is a field that looks at the history of the account, rather than its current status.

In *Koeut v. Navient Corp.*, the U.S.D.C. for the Southern District of California granted Navient's motion to dismiss the plaintiff's claims for violations of the FCRA and California Consumer Credit Reporting Agencies Act (CCCRAA). The plaintiff's claims arose from credit reports that included debt on his loan with Navient, which was previously discharged when the plaintiff filed for Chapter 7 bankruptcy. Ultimately, the court's reasoning was the plaintiff's failure to demonstrate that Navient knew or should have known of the plaintiff's bankruptcy discharge at the time of the investigation into the plaintiff's dispute.

In March 2021, the Sixth Circuit in *Willison v. Nelnet, Inc.*, affirmed summary judgment for a student loan servicer on two claims arising under the FDCPA. The servicer's immunity was derived from the "debt collection exception" of the FDCPA. Under the exception, a servicer is not a "debt collector" for purposes of the FDCPA if the loan obtained by the servicer "was not in default at the time it was obtained." 15 U.S.C. § 1692a(6)(F)(iii). In *Willison*, the Sixth Circuit concluded that the loan servicer qualified for the "debt collection exception" because the servicer obtained the loans when they were in "repayment" rather than default "status". The servicer in *Willison* was the beneficiary of the Federal Family Education Loan Program (FFELP),[7] which allows new lenders to purchase loans and "remove [them] from default." 34 C.F.R. § 682.405(a)(1).

Private Loans

Although privately held student loan borrowers did not have the same level of federal protection as borrowers paying to the federal government during the pandemic, on March 31, 2021, the Department of Education announced that it would grant a waiver on interest and payments through the end of September 2021 to anyone with a Federal Family Education Loan (FFEL), extending back to March 13, 2020. The department announced that penalties and interest would be removed and anyone who made payments could ask for a refund retroactively. Further, under this relief, defaulted loans would also be restored to a more positive status, credit bureaus would be notified to remove any black marks, and any wages or tax refunds garnished would be returned.

Some states have also taken it upon themselves to enact additional protections for private borrowers. For example, in California, private student loan borrowers will receive benefits from the Private Student Loan Collection Reform Act signed into law by Governor Gavin Newsom on October 6, 2021. The law, which takes effect July 1, 2022, among other provisions, places new documentation requirements on the collection activity for student loans from private lenders. The act prohibits a private education lender or a private education loan collector, from making any written statement to a debtor in an attempt to collect a private education loan unless the private education lender or private education loan collector possesses certain information regarding the loan and provides this information to the debtor.

Student Loans in Bankruptcy

While the CARES Act continued to alleviate the need of some borrowers to seek a discharge of their student loans through bankruptcy in 2021, significant developments have still occurred in the application of the Bankruptcy Code to student loan debt in both Congress and federal courts.

Two Senate bills would make it easier to discharge federal student loan debt through bankruptcy. The first is the FRESH START through Bankruptcy Act of 2021. Through this bill, federal student loan borrowers could seek discharge of their federal student loans after a waiting period of 10 years from the date the first loan period is due. Among other provisions, the FRESH START ACT of 2021 would retain the existing "undue hardship" standard under *Brunner v. New York State Higher Educ. Serv. Corp.*

[7] FFELP allows private lenders to make federal student loans to students that are insured by guaranty agencies. These guarantee agencies are then reinsured by the federal government. FFELP loans were paused on July 1, 2010 as a result of the Health Care and Education Reconciliation Act of 2010.

(*In re Brunner*), 831 F.2d 395 (2d. Cir. 1987) to allow relief of student loan debt outside the period of 10 years.

The second bill is the Medical Bankruptcy Fairness Act of 2021. While the primary focus of the act would be to allow for the discharge of medical debt, it also aims to make it easier for student loan borrowers to discharge their student loans in bankruptcy by modifying the current "undue burden" test employed in Federal Courts.

While Congress has been working on legislation to modify the discharge of student debt through bankruptcy, various federal courts have called the three-prong "undue burden" standard from *Brunner* into question. Under this test, a debtor must show: (1) that the debtor cannot maintain a "minimal" standard of living for herself and her dependents if she were to repay the loans; (2) other circumstances would prevent the same problems with repayment for a significant portion of the repayment period of the student loans; and (3) that the debtor has made good faith efforts to repay the loans. *Brunner*, 831 F.2d at 396.

Most recently, the U.S. Court of Appeals for the Second Circuit ruled that some privately issued student loans can be discharged in bankruptcy if certain conditions are met. The court's decision in *Homaidan v. Sallie Mae, Inc.*, 3 F.4th 595 (2d Cir. 2021), marked a win for borrowers attempting to lessen the load of student loan debt. In *Homaidan*, a unanimous panel held that the privately held student loan that Homaidan had after graduating from Emerson College was not the type of "educational benefit" that is exempt from discharge under Title 11 U.S.C. § 523(a)(8)(A)(ii). Homaidan argued that the holder of his private loan had engaged in a "scheme" of issuing dischargeable loans to unsophisticated student borrowers and then demanding repayment even after the loans were discharged in bankruptcy. The Second Circuit joined both the Fifth and the Tenth Circuits that have also previously narrowly interpreted the meaning of "educational benefit" under Title 11 U.S.C. § 523(a)(8)(A)(ii). *See McDaniel v. Navient Solutions, LLC* (*In re McDaniel*), 973 F.3d 1083, 1086 (10th Cir. 2020), and *Crocker v. Navient Solutions, LLC* (*In re Crocker*), 941 F.3d 206, 209 (5th Cir. 2019), *as revised* (Oct. 22, 2019).

Although the circuits remain divided on the dischargeability of some student loan debt, in June 2021 the Supreme Court declined to grant certiorari in *McCoy v. United States*, 810 F. App'x 315 (5th Cir. 2020), *cert. denied sub nom. McCoy v. United*

States, 141 S. Ct. 2794 (2021). This was a case that would have called into question the "undue burden" standard. In *McCoy*, Thelma McCoy had amassed more than $345,000 in student loan debt. She consolidated her debt into a monthly payment plan, but due to her low income and disabilities, her monthly payment was set at $0. The Fifth Circuit in *McCoy* affirmed the district court's judgment of the bankruptcy case. The judgment denied McCoy the benefit of discharge of the debt because she could not show that additional circumstances existed indicating that she was likely to not be able to repay her loans for a significant portion of the repayment period of her loans (the second prong of the "undue burden" test).

While it remains a question how long the "undue burden" standard of *Brunner* will persist within the courts or whether Congress will legislatively modify this standard, student loan borrowers today have increasing avenues within the federal courts to seek discharge of their student loan debt through bankruptcy proceedings.

Federal Regulation

In addition to pandemic-related relief programs, we also saw an uptick in federal government regulation and policymaking in the student lending space in 2021. The involvement revolved around debt forgiveness, Department of Education regulation, and CFPB action.

Debt Forgiveness

Federal student loan debt forgiveness dominated many headlines in 2021, although large-scale debt forgiveness for the majority of borrowers did not come to pass (and may never come to pass given the heated debate on both sides).

In February, attorneys general from 17 states wrote to Congress, supporting proposed legislation that would result in cancellation of up to $50,000 in loan debt per borrower.

In April, the U.S. Department of Education forgave nearly $1 billion in debt to students who were allegedly defrauded by their schools into taking out loans. The relief was granted under the Borrower Defense to Repayment program and affected approximately 72,000 individual borrowers.

In August, the department also automatically discharged $5.8 billion in loan balances for disabled borrowers, affecting 323,000 individuals nationwide.

Debt forgiveness is expected to continue to be a hot topic as COVID-19 payment relief programs expire in 2022 and student loan borrowers are required to resume regular payments.

Department of Education

The Department of Education significantly ramped up its regulatory activity this year, after being relatively dormant under the prior administration.

In August, the department issued a new regulatory interpretation, which took the position that federal law only narrowly preempts state and local efforts to regulate the servicing of federal education loans "in limited and discrete respects." This represents a significant reversal from a 2018 interpretation (issued under the prior administration), which posited that federal law broadly preempted all state-level attempts at regulation. Among other salient points, the new interpretation expressly finds that federal disclosure requirements do not preempt state laws prohibiting misrepresentations by loan servicers.

The Office of Federal Student Aid (FSA), now led by former CFPB director Richard Cordray, relaunched an Office of Enforcement in October, intended to "strengthen oversight of and enforcement actions against postsecondary schools" that participate in federal loan programs. Kristen Donoghue, previously the CFPB's enforcement director, has been tapped to lead this office, signaling an intent to revitalize a regulatory body that was not extremely active under the previous administration. Although the focus is largely on post-secondary institutions, the Enforcement Office also will investigate "indicators of potential misconduct or high-risk conduct by…third-party servicers" and collaborate with other regulatory bodies, like the CFPB and FTC.

Other big changes happened in October, with the FSA announcing newly negotiated contract terms with its student loan servicers, touting "stronger standards for performance, transparency, and accountability … aimed at protecting borrowers."

Among other changes, servicers will now be regularly evaluated based on how responsive they are to customer communications. Consistent with the department's new position on the limitations of federal preemption, servicers are also now expressly required to comply with all state and local laws.

Perhaps as a result of the enhanced regulation and associated costs of compliance, some servicers are taking steps to exit the federal student loan servicing industry altogether. According to the 2021 Annual Report of the CFPB Education Loan Ombudsman, four of the nine federal student loan servicers have stopped servicing federal loans.

According to the 2021 Annual Report of the CFPB Education Loan Ombudsman, four of the nine federal student loan servicers have stopped servicing federal loans.

CFPB

The CFPB was also increasingly active in the student lending space in 2021.

In March, the CFPB filed a lawsuit against a student loan debt relief company, alleging that it unlawfully charged advance fees to access otherwise free debt relief programs and violated the Telemarketing Sales Rule (TSR). The lawsuit remains pending. Debt relief companies continue to be a favorite target for regulators at both the state and federal level.

In September, the CFPB took legal action against a provider of income share agreements (ISAs). Unlike traditional student loans, income share agreements provide students with the funds to pay for post-secondary education, and in exchange the students agree to pay a percentage of their future income back to the provider for a period of time or up to a certain amount. The CFPB took the position that this arrangement was still fundamentally a loan transaction, so its providers are still required to abide by the laws and regulations applicable to student loans. The action was resolved by a consent order in which the provider agreed to accurately represent its products, provide disclosures required by federal law and reform its contracts.

Despite the CFPB's activities, the 2020 *Selia Law LLC v. Consumer Financial Protection Bureau* case continued to impact the CFPB in 2021. In *Selia Law*, the U.S. Supreme Court found the CFPB's structure unconstitutional. In March, a Delaware federal court dismissed a CFPB enforcement action alleging unfair debt collection practices by several student loan trusts, relying on *Selia Law* to find that the prosecution of the lawsuit could not be ratified by the current CFPB director. Following dismissal, the CFPB filed an amended complaint. The defendants filed a motion to dismiss the amended complaint, contending that as "paper entities" without any actual employees, they are not "covered persons" subject to CFPB enforcement under the Consumer Financial Protection Act (CFPA). The court has not yet ruled on the second motion to dismiss and recently ordered supplemental briefing from the parties.

State Regulation

In addition to action on the federal level, 2021 saw several interesting developments in state regulation and enforcement related to student lending. These developments involved both legislation and enforcement.

Legislative

In 2021, Minnesota joined a handful of other states in enacting a Student Borrower Bill of Rights aimed at regulating student loan servicers. Under the new law, servicers will be required to communicate accurate account information, evaluate students for income-based repayment options and provide notice when the loan is transferred to a new servicer.

The District of Columbia also has legislation pending, called the New Student Loan Borrower

Bill of Rights Amendment Act of 2021 (B-170), which proposes enhanced legal protections for student loan borrowers and generally prohibiting unfair, deceptive, or abusive acts and practices in connection with student loan servicing. The proposed legislation also expressly gives a private right of action to student loan borrowers under the District's existing consumer protection laws.

State and local legislation is expected to increase in the years to come, especially in light of the Department of Education's recent interpretation of law, which decreases the likelihood that state laws will be deemed preempted by federal law.

Enforcement

The California Department of Financial Protection and Innovation (DFPI) led the charge in enforcement actions this year. In February, the DFPI announced an investigation of student loan debt relief companies to determine whether they complied with the state's newly enacted California Consumer Financial Protection Law (CCFPL), which became effective January 1, 2021.

In May, the DFPI entered into a consent order with an online computer programming school, settling claims brought under the state's new California Consumer Financial Protection Law that the school's marketing materials and financing contracts were misleading.

In August, the DFPI entered into an agreement with a company involved in Income Share Agreements (ISAs) used to finance education, which includes an agreement that the ISAs are "student loans" subject to regulation under California's Student Loan Servicing Act. The agreement was negotiated as part of the company's attempt to obtain a license under the Act.

In March, a Washington state court found that a national loan servicer violated the Consumer Protection Act by engaging in unfair and deceptive conduct. The case, filed by the state attorney general, resulted in a partial summary judgment opinion finding that the servicer's "co-signer release" program misrepresented the way the loan servicer actually implemented the program. Other claims against the servicer are scheduled for a trial in 2022.

In April, the attorney general for Pennsylvania entered into an agreement with a debt buyer who had purchased a pool of loans related to a now-defunct school that had lost its accreditation and failed to meet federal education requirements. The debt buyer – who acquired the loans after the school closed – agreed not to engage in any collection efforts related to the loans. The agreement effectively resulted in the cancellation of approximately $2.6 million in loans.

TELEPHONE CONSUMER PROTECTION ACT

Looking Back

2021 was an eventful year for Telephone Consumer Protection Act-related (TCPA) issues for consumer-facing companies. The Supreme Court weighed in with a long-anticipated ruling on the meaning of automated telephone dialing systems (ATDS), courts began the first steps of interpreting that ruling, and the Federal Communications Commission (FCC) issued new guidance and postponed other regulations.

Supreme Court Answers the Call to Define Autodialer

In April, the Supreme Court in *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021) finally answered one of the most vexing, yet fundamental questions underlying the TCPA: What is an ATDS?

The case concerned one of Facebook's optional security features that sends its users a text message whenever there is an attempt to access their account from an unknown device or browser. Respondent Noah Duguid received several of such texts, despite the fact that he did not have a Facebook account. Thus, he alleged Facebook violated Section 227(b)(1)(A) of the TCPA by utilizing an ATDS that stored his number and contacted him without his prior consent. Facebook argued this interpretation ran counter to the statutory text since it did not send these text alerts to randomly or sequentially generated numbers.

Section 227(a)(1) of the TCPA defines an ATDS as "equipment which has the capacity – (A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers." This definition generated significant disagreement between the various circuit courts. The Ninth Circuit, as well as the Second and Sixth circuits, sided with Duguid's argument — that storage of telephone numbers, without random or sequential number generation, was enough to meet the first prong of the definition. The Third, Seventh, and Eleventh circuits, on the other hand, concluded that a system must have the capacity to generate random or sequential numbers to qualify as an autodialer.

Ultimately, the Court decided that "Duguid's quarrel is with Congress," not the courts, and left the possibility of redefining an ATDS to the legislative branch.

Rejecting the Ninth Circuit's approach, the Supreme Court held unanimously that an ATDS under Section 227 must have "the capacity to use a random or sequential number generator to either store or produce phone numbers to be called." The Court based its decision on twin pillars of textual construction and congressional intent. Applying "conventional rules of grammar," Justice Sotomayor wrote that the series of verbs ("to store" and "produce") are modified by the subsequent clause ("using a random or sequential number generator"). The respondent's argument would divorce the effect of the statute from "the most natural reading of the sentence" by making it illegal to store and automatically dial a telephone number. Moreover, the congressional intent behind the TCPA was to restrict telemarketing calls, so accepting respondent's arguments would put virtually all cell phone users who store and dial telephone numbers at risk of violating the TCPA, thereby taking a "chainsaw to these nuanced problems where Congress meant to use a scalpel."

Ultimately, the Court decided that "Duguid's quarrel is with Congress," not the courts, and left the possibility of redefining an ATDS to the legislative branch.

Post-*Facebook* Fallout: The New Landscape of ATDS Litigation

Although the Supreme Court defined what constitutes an ATDS under Section 227(a)(1) in *Facebook, Inc. v. Duguid*, questions remained on how lower courts would apply the decision, particularly in the early stages of litigation. In the months following the *Facebook* decision, courts have already diverged on how to address this issue. Below are some of the notable trends and outcomes in the early stages of post-*Facebook* TCPA litigation.

Footnote 7 Analysis

In several cases, plaintiffs have attempted to shoehorn claims involving calls made to preproduced lists into Footnote 7 of the *Facebook* opinion. Footnote 7 describes Congress' intent to include both "stor[ing]" and "produc[ing]" telephone numbers in the definition of ATDS to "clarify the domain of prohibited devices," so including "store" was not superfluous. 141 S. Ct. 1163, 1172 n.7 (2021). However, the footnote also states that "an autodialer might use a random number generator to determine the order in which to pick phone numbers from a preproduced list." *Id.*

Plaintiffs in various jurisdictions have clung to this last sentence to support the proposition that a system that randomly dials numbers from a preproduced list still constitutes an ATDS. However, courts have been generally unreceptive to such claims. For example, in *Brickman v. Facebook, Inc.*, the district court dismissed the plaintiff's allegations that unauthorized birthday texts sent to Facebook users violated the TCPA's ATDS prohibitions. No. 16-CV-00751, 2021 WL 4198512, at *1 (N.D. Cal. Sept. 15, 2021). Surveilling the landscape of prior decisions under Footnote 7, the court held that the plaintiff had failed to "plausibly allege use of an ATDS where the number called by the defendant … was not itself created by the random or sequential number generator." *Id.* at *2.

Motion to Dismiss or Summary Judgment?

Courts have also diverged in whether to follow a commonsense interpretation of *Facebook* and release defendants on a motion to dismiss or to reserve rulings on whether a system qualifies as an ATDS for summary judgment.

In the latter cases, courts deferred decisions on the merits to summary judgment, where plaintiffs alleged sufficient facts to show they were contacted in an impersonal and generic fashion, allowing the court to infer that a random or sequential number generator had been used. See *Miles v. Medicredit, Inc.*, No. 4:20-CV-01186, 2021 WL 2949565, at *4 (E.D. Mo. July 14, 2021) (allegations of debt collection calls attempting to reach a third party, unconnected to plaintiff, were sufficient to survive a motion to dismiss); *Montanez v. Future Vision Brain Bank, LLC*, No. 20-CV-02959, 2021 WL 1697928, at *8 (D. Colo. Apr. 29, 2021) (although defendant's affidavit raised serious questions regarding the use of an ATDS, the plaintiff's allegations of a lack of "human involvement" met threshold for pleading TCPA claim).

On the other hand, numerous courts have dismissed cases that involved targeted outreach or failed to plead automation or random generation. *See Camunas v. Nat'l Republican Senatorial Comm.*, No. CV 21-1005, 2021 WL 2144671, at *6 (E.D. Pa. May 26, 2021) (granting motion to dismiss because the complaint did not plead sufficient facts regarding content, phone number, or lack of any prior relationship); *Watts v. Emergency Twenty Four, Inc.*, No. 20-CV-1820, 2021 WL 2529613, at *3 (N.D. Ill. June 21, 2021) (granting motion to dismiss because the plaintiff failed to show use of random or sequential number generator).

Recently, a district court in the Southern District of California reversed course and granted on reconsideration a previously denied motion to dismiss. *Gross v. GG Homes, Inc.*, No. 3:21-cv-00271, 2021 WL 4804464, at *1 (S.D. Cal. Oct. 14, 2021). The court originally refused to dismiss the plaintiff's Section 227(b) claim because it could not determine from the pleadings whether the dialer stored or produced telephone numbers using a random or sequential generator, and it thought "[t]he newly clarified definition of an ATDS is more relevant to a summary judgment motion than at the pleading stage." *Id.* at *2. After considering persuasive authority from the intervening months, however, the court acknowledged that "[t]he targeted nature of the underlying texts contradicts the notion that

Plaintiff's telephone number could have been produced through a random or sequential number generator." *Id.* at *3. Because this contradiction "fatally undermin[ed] Plaintiff's ATDS claims," the court dismissed the plaintiff's claim without leave to amend. *Id.*

A few of the other highlights from the district court level include:

- ***McEwen v. Nat'l Rifle Ass'n of America*, No. 2:20-cv-00153 (D. Me. Apr. 14, 2021):** Noted in dicta that while the defendant had not moved to dismiss the TCPA claims based on ATDS use, the plaintiff had only alleged automation, not use of a random or sequential generator, and therefore may not have adequately stated its ATDS claims.
- ***Atkinson v. Pro Custom Solar LCC*, No. SA-21-CV-178 (W.D. Tex. June 16, 2021):** Denied the defendant's motion to dismiss and held that pleading use of a dialing system with present capacity to dial numbers in a random or sequential fashion was sufficient to present a question of fact for summary judgment.
- ***Hufnus v. DoNotPay, Inc.*, No. 3:20-cv-08701 (N.D. Cal. June 24, 2021):** Granted the defendant's motion to dismiss and held that the platform chatbots were not autodialers because they only contacted numbers provided by consumers, not identified or obtained in a random or sequential fashion, cabining Footnote 7.
- ***Borden v. eFinancial LLC*, No. C-19-1430 (W.D. Wash. Aug. 13, 2021):** Granted motion to dismiss and held that use of a random or sequential number generator to order calls did not transform a system into an ATDS, particularly where the plaintiff had originally provided his number to the defendant.
- ***Marshall v. Grubhub, Inc.*, 19-cv-3718 (N.D. Ill. Sept. 27, 2021):** Denied motion to dismiss without reaching the question of whether the plaintiff had adequately pled use of an ATDS because the plaintiff had sufficiently alleged a TCPA violation based on use of a prerecorded voice.
- ***Poonja v. Kelly Services, Inc.*, No. 20-cv-4388 (N.D. Ill. Sept. 29, 2021):** Denied motion to dismiss and held the plaintiff's allegations of a generic message sent by a toll-free number with automated reply functions were sufficient to survive pleading stage.
- ***Smith v. Direct Building Supplies LLC*, No. 20-3583 (E.D. Pa. Oct. 7, 2021):** Granted a motion to dismiss without prejudice and held that while the plaintiff had not alleged adequate facts regarding the identity of the caller, but allegations of a pause

and lack of a prior business relationship were sufficient to support an ATDS inference.

For additional information, Troutman Pepper tracks decisions interpreting the *Facebook* decision here.

Florida Strengthens Its Mini-TCPA

Immediately following the Supreme Court's *Facebook* decision, the Florida legislature amended its state version of the TCPA to impose new requirements for telephonic sales calls using an automated system.

The legislation, which became effective on July 1, 2021, required callers to obtain "prior express written consent" from the person to be called before making telemarketing calls. "Prior express written consent" consists of (1) a written agreement; (2) the signature and telephone number of the called party; (3) authorization for telephonic sales calls using an automatic system; and (4) a clear disclosure that the called party is not required to directly or indirectly sign the written agreement as a condition of purchasing any property, goods, or services. The amendment was a marked departure of the prior version of the law, which did not prohibit the use of an automated telephone dialing system with live messages if (1) the calls were made solely in response to calls initiated by the called party; (2) the numbers called were screened to exclude anyone on the Florida Department of Agriculture and Consumer Services' "no sales solicitation calls" list; or (3) the calls made concerned goods or services previously ordered or purchased by the called party.

Additionally, the new law created a private right of action against violators and imposed limits on the timing, number, and technology of telephonic sales calls, whether made through automated dialing, prerecorded messages, or live calls. Furthermore, because the Florida statute addresses different telephone technology — an "automated system," rather than an ATDS — the *Facebook* decision provides little in the way of a safe harbor for companies.

FCC Stalls on Pre-Recorded Message Limits

Following the FCC's December 2020 promulgation of proposed rules limiting the number of exempted pre-recorded calls companies could make to landlines, companies braced for fundamental changes in their compliance strategies. While the FCC published part of its proposed rule in February 2021, incorporating its previous guidance for pre-recorded calls to cell phones into the TCPA's implementing regulation, the FCC appears to have temporarily tabled the most significant changes.

The FCC's new rule would limit callers to three informational or non-telemarketing pre-recorded calls per 30-day period, or three health care-related calls per week (and no more than one per day) to landlines unless they obtained consent to place additional calls. The current rule allows companies to place an unlimited number of noncommercial calls without consent.

Industry leaders have noted an apparent drafting error in the FCC's rule, however. While the FCC's order explains that callers can use their three exempted calls to obtain consent to place additional calls, the proposed regulation itself would require the caller to receive the consumer's prior express *written* consent to exceed the three-call limits. Requiring prior express written consent for noncommercial calls would further deviate from the current regulatory framework, which only requires prior express written consent for *telemarketing* calls. Trade associations have submitted formal requests to the FCC to correct this apparent error, but the FCC has yet to respond or indicate when the call limit regulation will go into effect.

FCC Issues Guidance on "Advertising"

In January 2021, in response to a petition from Acurian seeking clarification on the noncommercial purpose exemption, the FCC held that prerecorded calls to residential phone numbers seeking participants for FDA-mandated clinical pharmaceutical trials did not constitute "advertising" or "telemarketing" under the TCPA because they "do not identify property, goods, or services offered for sale by Acurian." Therefore, these types of calls do not require prior express written consent. Still, the FCC reiterated that calls that offer a free good or service as part of an overall marketing campaign to sell a good or service still constitute commercial advertising, and other "dual purpose" calls are also suspect.

[T]he FCC reiterated that calls that offer a free good or service as part of an overall marketing campaign to sell a good or service still constitute commercial advertising, and other "dual purpose" calls are also suspect.

District Court Dismissal Provides Roadmap to Avoid TCPA Liability From Third Parties

In a class action victory for defendants, a district court in the Eleventh Circuit granted DirecTV's motion for summary judgment after finding the company was not liable for unsolicited telemarketing calls placed by its third-party vendor, Telecel. The ruling is instructive for future defendants to avoid such liability under the TCPA.

The class action, *Cordoba et al. v. DirecTV*, No. 1:15-cv-3755, Dkt. 235 (N.D. Ga. Feb. 12, 2021), centered on whether DirecTV was responsible for cold calls placed to individuals on the National Do Not Call Registry by Telecel under various agency law principles. In assessing the agency relationship, Judge Cohen placed considerable weight on the contractual agreements between the companies. In particular, the agreements explicitly prohibited any calls "to residential telephone lines or cellular phones." Moreover, in bolded lettering, DirecTV instructed retailers that it is a violation of company policy to "perform outbound telemarketing unless they are returning a direct inquiry from a customer." The court found that these explicit instructions — which were "not hidden deep within lengthy policy documents and couched in legal jargon" — deprived vendors of any actual authority to make these cold calls. Likewise, the vendors could claim no apparent authority because DirecTV stated in its correspondence to the plaintiff that it did not sanction or condone cold calling by independent retailers. Additionally, the court found DirecTV had not ratified the acts because there was no evidence that DirecTV intended to adopt or encourage Telecel's cold-calling practices, quite the contrary.

The outcome of this case highlights two key takeaways for companies that engage third-party calling services. First, the opinion provides a general roadmap for creating durable internal policies to shield principals from liability of their agents. These policies should explicitly outline prohibited behavior, rather than simply requiring contractors to "comply with all requisite laws and regulations." Second, if a contractor violates the policies, the principal should respond swiftly and proactively to reprimand the offending agent. Ultimately, this decision offers a useful benchmark to assess the strength of a company's internal policies and gauge risk accordingly.

Looking Forward: What to Expect in 2022

With *Facebook* firmly in hand, we anticipate the following trends will take shape in 2022:

- **Increased activity at the state level.** Look for states to start regulating calls to consumers. The Florida TCPA likely will serve as a model for other states to begin enacting statutes to address calls and/or text messages, with additional emphasis on telemarketing communications.
- **Greater focus on prerecorded messages.** The *Facebook* decision was a massive change for the definition of an ATDS, but it did not touch on prerecorded messages. For those companies that use calls involving an automated or prerecorded voice, the TCPA's statutory damage regime remains unchanged.
- **Emphasis on consent.** Though the tide has turned on the definition of an ATDS, now is the time to shore up consumers' consent to receive calls and/or text messages. The *Facebook* decision does not mean that it's time to throw out your TCPA compliance handbooks.

TRIBAL LENDING

Lawsuits involving tribal lending gained significant momentum in 2021. While there were significant victories for tribal lenders in the limitation of class claims under state lending laws and the enforceability of arbitration provisions, tribal lenders received some unfavorable decisions on regularly asserted motion to dismiss theories, such as nonjoinder of sovereign, necessary parties, summary judgment standards in Racketeer Influenced and Corrupt Practices Act (RICO) cases, and issues regarding whether the plaintiffs waived their ability to serve as class representatives. The Ninth and Fourth circuits diverged on the enforceability of arbitration agreements, with the Fourth Circuit set to further address the issue in 2022.

Circuits Split on the Enforceability of Arbitration Agreements

Brice v. Plain Green, LLC – Court of Appeals for the Ninth Circuit

In *Brice v. Plain Green, LLC*, No. 19-15707, 2021 U.S. App. LEXIS 27833 (9th Cir. Sep. 16, 2021), the Court of Appeals for the Ninth Circuit reversed and remanded a decision from the Northern District of California, denying a tribal lender's motion to compel arbitration. The district court denied a prior arbitration motion, finding the arbitration agreement unenforceable because it "prospectively waive[d] Borrowers' right to pursue federal statutory claims by requiring arbitrators to apply tribal law." In reversing the district court, the Ninth Circuit found that the delegation provision in the arbitration agreement required that an arbitrator — not the court — decide the validity of the arbitration agreement and that the arbitrator was permitted to decide enforceability issues under tribal, federal, and state law.

The *Brice* decision confirmed that when a delegation provision exists, "courts first must focus on the enforceability of that specific provision, not the enforceability of the arbitration agreement as a whole." Indeed, "[t]o do otherwise would render the delegation provision a nullity." The Ninth Circuit held that "the delegation provision is enforceable because it does not eliminate Borrowers' right to pursue in arbitration their prospective-waiver challenge to the arbitration agreement as a whole, even though that challenge arises under federal law."

The Ninth Circuit ruled that the provision's plain language did not foreclose the arbitrator from considering enforceability disputes based on federal law. The description of what an arbitrator can decide expressly includes enforceability disputes arising under "federal, state, or Tribal Law … based on any legal or equitable theory." The court went on to state that the "Borrowers' rights to pursue their federal prospective-waiver argument remains intact at this stage of the proceedings and the delegation provision is not facially a prospective waiver."

Hengle v. Treppa – Court of Appeals for the Fourth Circuit

The Court of Appeals for the Fourth Circuit took a contrary approach to arbitration clauses in *Hengle v. Treppa*, No. 20-1062 (4th Cir. Nov. 16, 2021). There, the Fourth Circuit recognized that parties may use a delegation clause to allow an arbitrator to decide gateway issues of arbitrability; however, the Fourth Circuit reiterated its position that arbitration provisions (including delegations clauses) are invalid when they require "application of tribal law to the practical exclusion of other law," waiving federal rights. While the court found the challenged arbitration provisions did not expressly disclaim the application of federal law, the court found the following provisions had the practical effect of "preempting application of other authority" that (1) arbitration "will be governed by the laws of the [tribe];" and (2) the rules of the arbitration forum are applicable "to the extent those rules and procedures do not contradict the express terms of this Arbitration Provision or the law of the [tribe], including the limitations on the arbitrator below."

The court also noted that referring to the Federal Arbitration Act did not cure the delegation clause's deficiencies because "the arbitration provision necessarily restrains the arbitrator from considering federal law defenses to arbitrability," rendering the delegation clause unenforceable. Ultimately, the court found that the arbitration provision and the tribal code waived a borrower's federal rights because the choice-of-law clauses operated as a prospective waiver to the borrower's statutory rights and remedies. The court opined that the arbitration agreement would require federal claims be sent to arbitration, but it would prevent effective vindication of those rights. While the defendants argued that the arbitration provision could be severed, the court disagreed on the grounds that a severability clause cannot save an arbitration provision if the invalid terms are integral to the agreement.

California Federal Court Lowers Bar for Plaintiffs on Summary Judgment in Tribal Lending RICO Dispute

Judge William H. Orrick of the Northern District of California issued an unfavorable opinion to tribal lenders, which (1) denied the defendants' motion for summary judgment, stating the motions required resolution of material, disputed facts; and (2) granted the plaintiffs' motion for partial summary judgment, finding that the contract's choice-of-law provision is unenforceable, that California law applies, and that tribal immunity was inapplicable to the remaining defendants. *Brice v. Haynes Invs.*, 13-cv-01200-WHO, LLC, 2021 U.S. Dist. LEXIS 130649, (N.D. Cal. July 13, 2021).

The court found there was sufficient evidence in dispute for the plaintiffs to maintain a RICO claim at this juncture, because:

- A jury may believe that the defendants had a joint role in creating, funding, and operating lender and the tribal lending operations;
- RICO does not require each defendant to individually collect the debt, only that they have a role in conducting the enterprise; and
- The plaintiffs have submitted sufficient evidence to satisfy the "injury investment rule" under Section 1962(a) as money gained through the lender was used to:
  - Fund tribal lending operations; or
  - Reinvest in the lender.

The court found the plaintiffs' California state law claims survive the defendants' motion for summary judgment since:

- The unjust enrichment claims, though outside the two-year statute of limitations, may be equitably tolled as the contract terms may have "lulled plaintiffs into not attempting to file suit;" and
- Usury claims do not require direct consumer-to-defendant payments — only that tribal entities received payments.

The court granted summary judgment to the plaintiffs on three issues, finding:

1. The contracts' choice-of-law provisions are uniformly unenforceable, because:
   - The defendants cannot identify any provision in the applicable tribal laws "that would enforce the state and federal statutory rights of plaintiffs;" and
   - This lack of provision providing for state and federal rights, combined with the arbitration agreement provision limiting the law the arbitrator can provide, unambiguously waives the plaintiffs' rights.
2. California law applies as, without the choice-of-law provision, it "is the only law left that could apply to the plaintiffs" claims.
   - Even if there were another choice or law, federal common law (applying the Restatement of Conflict of Laws) would find California has a materially greater interest in enforcing its usury laws and protecting consumers from usurious conduct than either tribal entity.
3. The court granted summary judgment to the plaintiffs on the defendants' tribal immunity defense, finding it inapplicable as:
   - The defendants admit they are not entitled to assert or invoke sovereign immunity on their own behalf; and
   - Litigation regarding the defendants' personal conduct does not infringe on the tribe's immunity.

The *Brice* decision was significant in that it appeared to set a lower hurdle than hoped for in allowing the plaintiffs to survive summary judgment on RICO claims and also denied a clear statute of limitations defense on equitable tolling principles. This decision also joined other courts in diminishing the role of tribal sovereignty in these enterprises, paying short shrift to the tribe's legal interests in a conflicts-of-law analysis to find that California state law would apply in the absence of a choice-of-law provision (and whether it should withstand challenge in the first instance).

Virginia Federal Court Rules Class Actions Not Proper Vehicle to Evaluate Many States' Lending Laws in One Action

On September 23, 2021, a judge in the Eastern District of Virginia issued a *sua sponte* order, dismissing without prejudice all non-Virginia state law causes of action that "assert various and sundry claims." The two-page order is direct and to the point, but cogently expresses that class-action treatment is not an appropriate vehicle to adjudicate the differing complexities between various state legislative lending schemes in one class.

The defendants in the tribal lending arena have seen a proliferation of class cases that take consumers from one jurisdiction and then assert classes alleging injuries under different states' laws, despite the no-named plaintiff having suffered injury under those other states' laws. Statutory standing challenges have been the primary and first-line defenses against these tacked-on claims, but the Eastern District of Virginia took a direct approach and stated plainly that the differences between various states' laws present "complex issues best decided by the courts of those states" and then declined to exercise jurisdiction over state law claims, citing "28 U.S.C. § 1367 and the superiority factor of Fed. R. Civ. P. 23."

This decision makes eminent sense. Litigating the nuances that arise under multiple legislative schemes would naturally require mini trials and not present the most effective means of uniformly resolving an entire class' claims. Realizing this inevitable consequence, the court stated it would "confine the proceedings henceforth to the federal claims and to such Virginia claims as may be viable under Virginia law."

UNIFORM COMMERCIAL CODE AND BANKING

In a tumultuous year with post-election civil strife and a new administration, emerging variants of COVID-19, and law firms and financial institutions coping with strained operations from remote work environments, financial institution litigation continued at a high level. Bank litigators saw mortgage foreclosure litigation drop from the high levels of the past decade, but Uniform Commercial Code (UCC), check, and bank operation litigation flourished as new issues sprouted in wire fraud, Payroll Protection Plan (PPP) litigation, and on the regulatory front.

Check and Bank Operation Litigation

A district court in Pennsylvania reaffirmed the long-standing principle that a bank does not owe a fiduciary duty to a deposit customer and has no duty to monitor the customer's transactions. In *Basement Sols., LLC v. Wells Fargo Bank, NA*, No. 21-104, 2021 WL 352012 (E.D. Pa. Feb. 2, 2021), two business partners each owned half of the business titled Basement Solutions LLC, which had two business accounts with Wells Fargo Bank. The partnership dissolved and one of the partners became the sole owner. The departing partner, without the consent or knowledge of the sole owner partner, closed out the business accounts at Wells Fargo, created two new accounts in the name of the business, and transferred the funds into the new accounts. When the sole owner partner learned of this, he demanded that Wells Fargo close the new business accounts immediately and return the funds to the business. Wells Fargo refused. The sole owner partner sued the departing partner for a series of common law claims, and sued the bank for facilitating the theft and allowing the departing partner to open new business accounts in the business's name. The court granted Wells Fargo's motion to dismiss, finding that the relationship between the bank and its customer is not a fiduciary relationship and the bank did not have a duty to monitor the customer's transactions.

Similarly, in *Perlberger Law Associates, P.C. v. Wells Fargo Bank, N.A*. Case No. 21-2287, 2021 WL 3403510 (E.D. Pa. Aug. 3, 2021), the court found a bank did not have a duty to protect a deposit account from misuse. In *Perlberger*, a law firm brought action against its bank for UCC violations and breach of contract. Plaintiff improperly based its wire fraud claim on a returned fraudulent cashier's check. The bank moved to dismiss for failure to state a claim. The court allowed the breach of implied contract claim, which alleged that the bank had assumed contractual duties such as fraud detection measures, to proceed because it was unclear at that early stage what the bank had represented to plaintiff about the status of the forged check before the funds transfer, and so could not conclude that the "unusual" breach of contract claim was fully redressable by the UCC. The court dismissed the remaining counts as Article 4A governs wire transfers and not cashier's checks. Specifically, the court held that the bank did not have a fiduciary duty to monitor, protect, and guard against dissipation of the firm's funds by a third party.

A federal court in Nevada addressed the familiar fraudulent bookkeeper scenario in *Dog Bites Back, LLC v. JPMorgan Chase Bank, N.A.*, No. 2:20-cv-01459, 2021 WL 4395042 (D. Nev. Sept. 24, 2021). Plaintiff's employee forged counterfeit checks processed by the bank defendant. The plaintiff notified the bank when it discovered the forgeries and demanded reimbursement. Plaintiff brought claims against the bank for breach of contract, breach of the implied covenant of good faith and fair dealing, negligence, and UCC violations. While the court recognized that some UCC provisions create causes of action by an employer against a depositary bank to recover instruments fraudulently endorsed by an employee if the bank fails to exercise ordinary care, it held that the ordinary care standard did not require the bank to examine an instrument for potential forgeries if its policies and procedures did not require it to do so. Since the plaintiff failed to identify any of the bank's procedures concerning check forgery or how the forgeries violated the bank's policies and

procedures, and also did not allege the specific ways that the bank lacked ordinary care, it failed to state claims under the UCC. The court dismissed all counts except the claim for breach of implied covenant of good faith and fair dealing, finding the plaintiff had plausibly alleged these claims. The bank does not appear to have raised a UCC preemption argument.

In *Iron Bridge Mortgage Fund, LLC v. Bank of America*, No. 20-cv-08581, 2021 WL 1947546 (N.D. Cal. May 14, 2021), a lender brought an action against a borrower and the borrower's bank for various UCC violations arising from checks issued by the lender intended for the borrower's vendors. The lender argued that the borrower had converted and deposited the checks in its own account. The bank moved to dismiss the lender's causes of action against it. The court granted the motion to dismiss because the UCC violations were time-barred as to all but one check. As to the one remaining check, the claims failed on the merits for multiple reasons. First, the plaintiff had failed to plead facts that would demonstrate that the bank had failed to exercise ordinary care or that the borrower was acting as the bank's independent contractor, causing the negligence claim to fail. Second, the warranties alleged to have been breached protected the bank as the drawee, not the lender as the drawer. Third, the plaintiff had not pled a direct contractual relationship with the bank or that it was an intended third-party beneficiary of the contract between the bank and the borrower, causing both the breach of contract and declaratory relief claims to fail. Finally, the plaintiff's unfair competition claim failed because it depended on the plaintiff's other failed claims.

Likewise, the district court in New Jersey granted a motion to dismiss various UCC violations and common law claims in *Perry v. National Credit Union Administration*, No. 1:19-cv-00167, 2021 U.S. Dist. LEXIS 11615 (D.N.J. Jan. 21, 2021), *aff'd*, 2021 U.S. App. LEXIS 34397 (3d Cir. 2021). Here, unauthorized individuals made withdrawals from the plaintiff's bank account. The plaintiff filed a complaint asserting claims for breach of contract, negligence, and UCC violations. The bank defendants filed motions to dismiss. The court granted the motion to dismiss finding that the plaintiff failed to sufficiently plead his causes of action because the damages sought exceeded the court's jurisdiction under the Tucker Act and did not identify with any specificity the contractual provision allegedly breached, and plaintiff admitted that his account documents did not contain any provision imposing the duties he alleged.

The court found that the check, while it might have been a counterfeit, was not "altered" within the meaning of the UCC. The court explained that alteration under the UCC required physical modification of an original check, not digital alteration.

In *Provident Savings Bank, F.S.B. v. Focus Bank*, No. 1:19-cv-151, 2021 WL 2915088 (E.D. Miss. July 12, 2021), the depositary bank brought an action against a payor bank claiming that the payor bank was liable for a fraudulent check that the payor bank failed to return within the midnight deadline under the UCC after the depositary bank presented it for payment. The parties filed motions for summary judgment. The court found that the check, while it might have been a counterfeit, was not "altered" within the meaning of the UCC. The court explained that alteration under the UCC required physical modification of an original check, not digital alteration. According to the summary judgment record, the check was a digitally altered copy of a genuine check that had been scanned, modified, and printed on commercially available check stock, and was thus a new, different physical document. The lack of alteration under the UCC precluded the payor bank's affirmative defense alleging breach of presentment warranty. The court also found that fact issues remained as to whether the depositary bank had actual knowledge that the signature of the purported drawer was unauthorized.

"Mistaken" Wires, Business Email Compromise, and Article 4A

The Southern District of New York issued a ruling as to whether Citibank would be able to recover hundreds of millions of dollars after a "mistaken" wire. In *In re Citibank August 11, 2020 Wire Transfers*, 520 F. Supp. 3d 390 (S.D.N.Y. 2021), Citibank, acting in its capacity as the administrative agent for a syndicated term loan taken out by Revlon, Inc., brought actions for unjust enrichment, conversion, money had and received, and payment by mistake. Citibank mistakenly wired approximately $900 million of its own funds to lenders rather than wiring approximately $7.8 million in interest payments to Revlon's lenders. The issue was whether Citibank was entitled to return of the funds or if the lenders are allowed to keep the funds. The court held that the lenders were not on constructive notice that payments were made by mistake. Under New York law, when a beneficiary receives money that was erroneously wired, the beneficiary should not have to wonder whether it may retain the funds. Instead, the beneficiary should be able to consider the transfer of funds as a final and complete transaction that is not subject to revocation. The court found that Citibank was not entitled to get its money back. Citibank appealed the ruling to the Court of Appeals for the Second Circuit and a decision is pending.

A Georgia federal court addressed whether the intended recipient of a wire was entitled to payment after the sender was tricked by a compromised business email into wiring millions to the wrong account. In *Peeples v. Carolina Container, LLC.*, No. 4:19-cv-21-MLB, 2021 WL 4224009 (N.D. Ga. Sept. 16, 2021), Carolina Container was supposed to wire $1.71 million to the plaintiff as part of an asset purchase. The funds were wired to a fraudster who hacked the email account of the plaintiff's attorney and sent Carolina Container fraudulent payment instructions. The court granted the plaintiff's summary judgment motion and denied Carolina Container's motion for summary judgment. The court found that Carolina Container agreed to pay the plaintiff a certain amount and it failed to do so. Plaintiff suffered losses as a result. The court also found that Carolina Container had not shown that it should be excused from its obligation to pay.

In *Jasper v. Bank of America Corp.*, No. 20-2842, 2021 U.S. Dist. LEXIS 149321 (D.N.J. Aug. 5, 2021), a scammer tricked the plaintiff into depositing a settlement payment into a third party's Bank of America account rather than the intended party's account. The scammer subsequently withdrew the funds via wire transfer. The plaintiff sued Bank of America for violations of New Jersey's UDAP statute, the Consumer Fraud Act, as well as various common law claims. The court granted summary judgment to Bank of America on the Consumer Fraud Act claims, ruling that "a bank that processes checks in accordance with the governing provisions of the UCC" will not be held to have "engaged in an unconscionable business practice." Further, it held that because the plaintiff's Consumer Fraud Act claim was based on the bank's response to reports of a fraudulent wire transfer, Article 4A of the UCC, governing wire transfers, precluded the claim. The court also granted summary judgment to the bank on its common law claims to the extent they arose from the funds transfers out of the third party's account, since those claims were also precluded by Article 4A.

In another case involving business email compromise, the Northern District of Georgia granted a motion to dismiss a complaint, including negligence, Bank Secrecy Act, and UCC claims. *Hofschutle v. SunTrust Banks, Inc.*, No. 1:20-cv-01676, 2021 WL 5230732 (N.D. Ga. Mar. 4, 2021) involved allegations that a hacker intercepted emails between the plaintiff and her broker, used information in those emails to open accounts at the defendant's banks in the name of the broker, and then tricked the plaintiff into making wire transfers to the hacker's accounts. The court declined to find preemption, ruling that negligence claims were only preempted if inconsistent with the duties imposed by the UCC. However, the court held that the plaintiff had still failed to state a claim for negligence because she had not alleged any direct relationship between her and the banks, banks do not owe common law duties to noncustomers to vet applicants for new accounts, and the account opening was not the proximate cause of plaintiff's injury. The court also rejected the Bank Secrecy Act claim, finding that the statute only created duties to the government, not to noncustomers. Finally, the court dismissed the plaintiff's claims under

Article 4A of the UCC, holding that Article 4A-201 governing security procedures only applied to the bank which initiated the wire transfer at the plaintiff's behest, not to the beneficiary bank where the funds were sent.

Bankruptcy and Creditor's Rights

In *City of Chicago v. Fulton*, 141 S. Ct. 585 (2021), the Supreme Court issued a ruling regarding creditors' rights under 11 U.S.C. § 362 of the Bankruptcy Code, which mandates that the filing of a bankruptcy petition operate as a "stay" of "any act" to "exercise control" over the property of the bankruptcy estate. The respondents had filed bankruptcy petitions and requested that the City of Chicago return their vehicles, which had been impounded for failure to pay motor vehicle-related fines. The lower courts had held that the city's refusal to return the vehicles post-petition-filing violated § 362's automatic stay. The Supreme Court reversed, holding that § 362 only prohibits affirmative acts, not merely retention of property, that would disturb the status quo as of the time of the bankruptcy petition's filing. The Court reasoned that the respondents' reading would render another section of the Bankruptcy Code, § 542, which requires entities in possession of certain estate property to turn over that property, effectively superfluous and would require turnover of *all* property, including the property otherwise exempted from the turnover command by § 542. Therefore, the Court held that creditors had the right to retain property in their possession at the time of a bankruptcy filing, at least to the extent permitted by § 542.

Additionally, the Sixth Circuit issued a ruling in a case involving an attempt by a bankruptcy trustee to unwind payments from the bankrupt company to one of the bankrupt company's creditors who had aided in its Ponzi scheme. The trustee argued the payments were fraudulent transfers under Ohio's Uniform Fraudulent Transfer Act (OUFTA). In *Bash v. Textron Financial Corp.*, No. 21a0216p.06, 2021 U.S. App. LEXIS 27302 (6th Cir. Sept. 10, 2021), the Sixth Circuit affirmed the district court's rejection of the trustee's attempt to unwind the transfers. The OUFTA allows for unwinding of certain fraudulent transfers of assets, but excludes property encumbered by a valid lien from the definition of asset. The trustee argued that alleged bad-faith actions taken by the creditor post-lien creation could invalidate its lien, allowing the transfers to be avoided. However, the court ruled that lien validity for purposes of OUFTA was based solely on whether it was effective against a later judicial lien. While bad faith could impact priority vis-à-vis two competing creditors under the UCC, bad faith did not directly affect the validity analysis. Further, to impact priority, the bad faith must be within a relationship between the two competing creditors, which is impossible between a current creditor and a hypothetical future judicial lien. Therefore, a creditor's bad faith did not allow the debtor's trustee to unwind the transfer under the OUFTA and UCC.

PPP Litigation

The American Rescue Plan Act of 2021, which created the Restaurant Revitalization Fund, directed the Small Business Administration (SBA) to prioritize

applications from restaurants owned by women, veterans, and the socially and economically disadvantaged. The SBA implemented this directive by stating that for the first 21 days, it would accept applications from all eligible applicants, but only process those from priority group applicants. In *Greer's Ranch Café v. Guzman*, No. 4:21-cv-00651-O, 2021 U.S. LEXIS 102243 (N.D. Tex. May 18, 2021), the plaintiff sought a temporary restraining order enjoining the use of race and sex preferences in the distribution of the Restaurant Revitalization Fund. The court granted the temporary restraining order, holding that the plaintiff was likely to succeed on its claim that the SBA's policy violated the U.S. Constitution's Equal Protection Clause and had a substantial threat of irreparable harm given that the applications from priority applicants were likely to drain the fund within the first 21 days.

In *Vestavia Hills, Limited v. U.S. Small Business Administration*, 630 B.R. 816 (S.D. Cal. 2021), a senior housing community applied for a Paycheck Protection Program loan through a federally insured participating lender, after filing for Chapter 11 bankruptcy but continuing to operate. The lender refused to submit the application to the SBA because the housing complex, as a bankruptcy debtor, did not meet the SBA's eligibility criteria. The housing complex sought a preliminary injunction, which the bankruptcy court granted. The district court vacated the bankruptcy court's grant of a preliminary injunction, holding that the housing complex was not likely to succeed on the merits. The court explained that the SBA had acted within its delegated authority in promulgating criteria for PPP loan eligibility under the CARES Act that excluded debtors. The SBA's interpretation of the statute was a permissible construction of the statute entitled to deference, and it had not acted arbitrarily and capriciously in adopting its bright-line rule. The court also held that the appeal was not moot even though the SBA had already disbursed PPP funds, because the outcome of the appeal would affect whether the housing complex qualified for loan forgiveness. *See also Agaña v. U.S. Small Bus. Administration*, No. 19-00010, 2021 Bankr. LEXIS 460 (Bankr. D. Guam Feb. 23, 2021) (granting SBA's motion to dismiss on the same basis).

A district court in Pennsylvania found that lenders neither owe a duty of care nor have a fiduciary duty to borrowers who apply for a PPP loan. In *Albino Construction Co. v. Wells Fargo Bank, N.A.*, No. 21-35, 2021 U.S. Dist. LEXIS 114781 (E.D. Pa. June 17, 2021), a construction company electronically applied to Wells Fargo for a PPP loan, but did not submit all the required documentation. As a result, Wells Fargo informed the company that its application could not be approved. The company sued Wells Fargo for negligence and breach of fiduciary duty, arguing that it should have flagged the application's deficiencies for the company to correct. The court granted Wells Fargo's motion to dismiss, finding that Wells Fargo, as a lender, did not owe any duty of care to a borrower in the processing of a loan application under Pennsylvania law, and even if a duty of care was owed, it did not require Wells Fargo to extend loans to borrowers with deficient applications or notify them of mistakes in those applications. The court further found that lenders have no fiduciary duty to borrowers, and Wells Fargo did not act in bad faith by denying the company's loan due to a deficient application.

In *Perlberger Law Associates, P.C., supra*, the plaintiff also advanced a cause of action for breach of fiduciary duty based on COVID-19 relief programs. The plaintiff claimed that it had to use the PPP funds to make the account whole after the fraudulent cashier's check was returned and the funds were already wired, which resulted in its inability to obtain forgiveness on the PPP loan. The court dismissed the PPP claim, finding that the debtor-creditor relationship did not usually confer a fiduciary relationship, and the plaintiff had not pled that the bank's role in administering COVID-19 relief resulted in the bank assuming control of the plaintiff's operations, which would have been the only possible exception to the general rule.

Regulators and Bank Examination Privilege

Finally, in *Leopold v. United States DOJ*, No. 19-3192, 2021 U.S. Dist. LEXIS 6236 (D.D.C. Jan. 13, 2021), the District Court for the District of Columbia determined whether a report detailing HSBC's compliance with anti-money laundering and sanctions laws and remedial measures proposed by an independent monitor was protected by Exemption 8 to the Freedom of Information Act.

In doing so, the court compared Exemption 8 to the bank examination privilege. The court noted that the report was similar to bank supervisory and examination reports subject to the bank examination privilege. Protecting the report thus furthered the purposes of Exemption 8: to ensure the security of financial institutions and to safeguard the relationship between banks and their supervising agencies.

Looking Forward to 2022

We expect to see a continued increase in UCC and bank operation litigation, including wire fraud, in 2022. Bank litigators need to impress on courts that the UCC largely insulates beneficiary banks from liability in the wire fraud context, and courts should resist the urge to recognize implied duties of care not recognized by state common law. Nor should courts impose duties of care on the sending bank outside the parameters of the UCC. There is no breach of an implied duty of good faith and fair dealing arising from a contract merely because a bank deposit customer was tricked into wiring funds to the wrong account and the bank followed the customer's instructions. Allowing cases with these allegations to proceed past the motion to dismiss stage increases the cost of litigation where ultimately there is no cognizable claim. We also expect more litigation of claims arising from PPP loans, and increased regulatory activity and enforcement actions as new Biden administration appointees click fully into gear.

CONSUMER FINANCIAL SERVICES LAW MONITOR

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. 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 WEBINAR SERIES

Our complimentary webinar series offers monthly CLE programming related to a variety of consumer financial services topics, including:

- Cybersecurity and Privacy
- Telephone Consumer Protection Act (TCPA)
- Fair Credit Reporting Act (FCRA)
- Fair Debt Collection Practices Act (FDCPA)
- Fair Housing Act (FHA)
- Mortgage Litigation and Servicing
- Bankruptcy
- Background Screening
- Electronic Funds Transfer Act (EFTA)
- State Attorneys General Investigations
- Consumer Financial Protection Bureau (CFPB) Enforcement and Regulatory Guidance
- Federal Trade Commission (FTC) Enforcement and Regulatory Guidance
- Case Law Updates

We are very interested in ensuring that we deliver the best webinar content to help you navigate the most complex business issues including litigation, regulatory enforcement matters, and compliance.

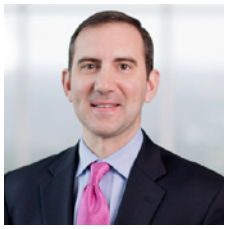
Email cfslawmonitor@troutman.com to submit topic suggestions.

CONTACTS

David N. Anthony
Partner
david.anthony@troutman.com
804.697.5410

Keith J. Barnett
Partner
keith.barnett@troutman.com
404.885.3423

Justin D. Balser
Partner
justin.balser@troutman.com
949.622.2443



D. Kyle Deak
Partner
kyle.deak@troutman.com
919.835.4133

Susan E. Flint
Partner
susan.flint@troutman.com
704.916.1516

Virginia B. Flynn
Partner
virginia.flynn@troutman.com
804.697.1480

Chad R. Fuller
Partner
chad.fuller@troutman.com
858.509.6056

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

Scott Kelly
Partner
scott.kelly@troutman.com
804.697.2202

Michael E. Lacy
Partner
michael.lacy@troutman.com
804.697.1326

CONTACTS

Kalama M. Lui-Kwan
Partner
kalama.lui-kwan@troutman.com
415.477.5758

John C. Lynch
Partner
john.lynch@troutman.com
757.687.7765

Jason E. Manning
Partner
jason.manning@troutman.com
757.687.7564

Ethan G. Ostroff
Partner
ethan.ostroff@troutman.com
757.687.7541

Stephen C. Piepgrass
Partner
stephen.piepgrass@troutman.com
804.697.1320

Ronald I. Raether
Partner
ronald.raether@troutman.com
949.622.2722

Timothy J. St. George
Partner
tim.st.george@troutman.com
804.697.1254

Ashley L. Taylor, Jr.
Partner
ashley.taylor@troutman.com
804.697.1286

Amy P. Williams
Partner
amy.williams@troutman.com
704.998.4102

Alan D. Wingfield
Partner
alan.wingfield@troutman.com
804.697.1350

Mary C. Zinsner
Partner
mary.zinsner@troutman.com
202.274.1932