Articles + Publications | February 28, 2024

2023 Year-In-Review: Key Enforcement Initiatives and Cases in Crypto, Cyber, SPACs, Whistleblowers, and the Future of Administrative Law Proceedings

WRITTEN BY

Ghillaine A. Reid | Timothy J. “Tim” Bado | Jay A. Dubow

It was a busy year for enforcement activity in the cyber, crypto, SPAC, and whistleblower spaces, with several pending actions that will likely have wide-ranging implications in 2024. We are also awaiting a ruling from the U.S. Supreme Court that could alter the landscape on administrative law proceedings. From the SEC’s release of expansive cybersecurity rules to the largest whistleblower award ever issued, 2023 had plenty of exciting developments. A detailed summary of key developments by category can be found below.

Crypto

Cryptocurrency enforcement saw a major uptick this year across a number of federal agencies including, the Department of Justice (DOJ), Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), Treasury’s Office of Foreign Asset Control (OFAC), and the Financial Crimes Enforcement Network (FinCEN), to name a few. In its 2023 enforcement results announcement, the SEC noted that it more than doubled its crypto enforcement actions from 18 in 2022 to 44 in 2023. The SEC made clear that crypto will be a top priority again in 2024. As crypto continues to expand and grow in popularity, and federal agencies continue to get more adept at investigating and enforcement, expect 2024 to be another major year of growth in this space.

A brief overview of some of the most notable crypto actions can be found below.

SEC Sues FTX, Sam Bankman-Fried, and Other Executives

While the criminal prosecution and subsequent conviction of former FTX co-founder and CEO Sam Bankman-Fried grabbed headlines in 2023, the SEC also sued Bankman-Fried and a number of former FTX executives in connection with a multibillion dollar fraudulent scheme. The SEC alleged Bankman-Fried orchestrated a years-long fraud to conceal from FTX’s investors: (a) the undisclosed diversion of FTX customers’ funds to Alameda Research LLC, his privately held crypto hedge fund; (b) the undisclosed special treatment afforded to Alameda on the FTX platform, including providing Alameda with a virtually unlimited “line of credit” funded by the platform’s customers and exempting Alameda from certain key FTX risk mitigation measures; and (c) undisclosed risk stemming from FTX’s exposure to Alameda’s significant holdings of overvalued, illiquid assets.

Sam Bankman-Fried is scheduled to be sentenced in March 2024 and the SEC’s lawsuit is yet to be resolved. This will likely be a story to continue to watch in 2024.

Binance Settles With the DOJ, CFTC, OFAC, and FinCEN

On November 21, 2023, Binance, the world's largest cryptocurrency exchange, reached an agreement with the DOJ, CFTC, OFAC, and FinCEN that required Binance to pay $4.3 billion across the four agencies. FinCEN will receive the largest portion of the settlement at $3.4 billion and $968 million will go to OFAC, it's largest settlement ever. The settlement resolved a multiyear investigation brought by the agencies and a lawsuit brought by the CFTC. The agencies alleged Binance violated the Bank Secrecy Act and multiple sanctions programs by failing to implement programs to prevent and report suspicious transactions. As a result, the agencies alleged Binance processed over 100,000 suspicious transactions involving terrorist organizations, ransomware, child exploitation, and darknet scams.

As part of the settlement, the company pleaded guilty to conspiracy to conduct an unlicensed money transmitting business and violation of the International Emergency Economic Powers Act. The plea deal requires Binance to engage in remedial compliance measures during a three-year probationary term and imposes an independent compliance monitor. Binance founder, Changpeng Zhao, also pleaded guilty to failing to maintain an effective anti-money laundering program.

SEC Files Enforcement Action Against Kraken

On November 20, 2023, the SEC sued Kraken, the third-largest crypto exchange in the world, alleging that the company operates as an unregistered securities exchange, broker, dealer, and clearing agency. These types of allegations have become commonplace against crypto exchanges, as federal agencies continue to jockey for jurisdiction to enforce crypto-related activity.

According to the SEC's complaint, since at least September 2018, Kraken has made hundreds of millions of dollars unlawfully facilitating the buying and selling of crypto asset securities. Kraken allegedly intertwined the traditional services of an exchange, broker, dealer, and clearing agency without having registered any of those functions with the SEC. As a result, Kraken has allegedly deprived investors of protections, including inspection by the SEC, recordkeeping requirements, and safeguards against conflicts of interest.

Cyber

Cybersecurity and cyber enforcement remain a top priority for a number of state and federal agencies due in large part to the explosion of popularity in artificial intelligence (AI) and high-profile cyber-attacks. Most notably, in July, the SEC voted to finalize a rule requiring public companies to make certain public disclosures regarding material cybersecurity incidents within four days. The New York State Department of Financial Services (NYDFS) and Federal Trade Commission (FTC) also created additional cyber governance and reporting obligations for financial institutions by making significant updates to their existing regulations. While tightening regulations took center stage, a few enforcement actions also gained attention in 2023 that put corporate entities on notice that agencies are willing to come after alleged violators.

SEC Cyber Disclosure Rules

On July 26, 2023, the SEC adopted new cybersecurity incident reporting rules for public companies subject to the

reporting requirements of the Securities Exchange Act of 1934 (the Exchange Act). The rules require public companies to publicly report any cybersecurity incident that they determine to be "material" within four business days of making the determination the incident was "material." The company must disclose the incident through an 8-K filing and describe the "material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably material impact of the incident … including its financial condition and results of operations." Importantly, the materiality determination must be made "without reasonable delay." The new rules further require periodic disclosures about cybersecurity risk management, strategy, and governance.

In many respects, these rules will require a massive overhaul of companies' current cybersecurity practices. The rules themselves have already raised a number of questions. Namely, what is considered a "material" incident under the rules? Practically, cyberattacks are not contained, investigated, or resolved within just a few days. Companies often do not know how their networks were accessed, whether there are remaining vulnerabilities, what was compromised, or how to resolve the incident. Determining whether the incident was material appears to be highly subjective and could take considerable time to determine.

Similarly, public disclosure of an incident could prompt further attacks by bad actors or derail negotiations between a company and the bad actor. While there is a limited law enforcement exception to the rules, the exception needs to be approved by the U.S. attorney general (AG) within the four-day discovery deadline and the AG must determine "that the disclosure of the cybersecurity incident rather than the incident itself poses a substantial risk to national security or public safety." Recent guidance issued by the FBI and DOJ on how victims can request DOJ to authorize a disclosure delay for national security and public safety reasons make clear this delay will almost never be approved.

SEC Sues SolarWinds Corp.

On October 30, 2023, the SEC filed a complaint against SolarWinds and Chief Information Security Officer Timothy Brown, alleging that misrepresentations were made about cyber risk, internal control failures, and committed securities fraud related to a sophisticated supply chain cyberattack of SolarWinds network management software that was orchestrated by a foreign government. This is the first time the SEC charged a corporate individual for their role in a cybersecurity failure. This sends a clear message that the SEC intends to hold individuals personally accountable for cybersecurity lapses.

The SEC alleges that from October 2018 through January 12, 2021, the defendants defrauded investors and customers through misstatements and omissions that allegedly concealed the company's poor cybersecurity practices and increased security risks. The company allegedly misled investors by only disclosing hypothetical and generic cybersecurity risks when it knew of specific vulnerabilities, poor controls and increased risk. After learning about the cyber-attack, the company allegedly made incomplete and misleading disclosures in its Form 8-K filing.

New York Department of Financial Services Cyber Rules

On November 1, 2023, NYDFS finalized amendments to its cybersecurity rules. The amendments not only bring additional companies under the umbrella of the rules, but also impose additional requirements. Each "Class A" company — those with at least $20 million in gross annual revenue in each of the last two fiscal years, and either more than 2,000 employees or more than $1 billion in gross annual revenue in each of the last two fiscal years

from the business and its affiliates — are now required to “design and conduct independent audits of its cybersecurity program based on its risk assessment”, monitor its privileged access activity, deploy a method for blocking commonly used passwords, and implement end point detection. The rules will become effective over time and allow covered entities lead time to comply with the new requirements. Covered entities will be required to comply with the incident reporting obligations within 30 days of the effective date of December 1, 2023.

The new rules impose additional requirements in the areas of incident reporting, extortion payment reporting, governance, and security controls. In short, each requirement requires companies to comply with certain reporting requirements after an incident has occurred, and requires specific policies and procedures to appropriately safeguard company information and address risk.

The NYDFS rules generally align with heightened requirements from other state and federal regulators and oversight by chief information security officers and boards. In the backdrop of the SEC’s new cybersecurity disclosure rules, companies will need to implement robust cybersecurity compliance measures and prepare for a wave of enforcement activity against those who allegedly violate these new rules.

Special Purpose Acquisition Companies

Special purpose acquisition company (SPAC) interest has cooled significantly over the past few years due to enhanced SEC scrutiny after reaching a peak in 2020-2021. But SPAC litigation and regulatory enforcement is alive and well. Shareholders have challenged a significant percentage of de-SPAC transactions in Delaware Chancery Court and federal courts across the U.S. Several high-profile suits have survived motions to dismiss (at least in part), and at least one matter was resolved through a substantial settlement.

To this point, we have largely seen SPAC lawsuits focus on alleged conflicts of interest and the accuracy of disclosures regarding targets’ business prospects.

A summary of recent cases and decisions is below.

In January 2023, the Northern District of California decided a matter against Lucid Motors involving allegations of misleading statements made before the de-SPAC transaction closed. The statements were made by the target’s CEO before the merger was announced. News of a potential merger between Lucid Motors and the SPAC leaked in January 2021, while news of the merger was formally announced in February 2023.

During that one-month interval, Lucid’s CEO made allegedly misleading statements about how many cars Lucid expected to produce in 2021 and about the operational status of the company’s Arizona factory. Lucid allegedly published an investor presentation that contradicted the CEO’s previous statements, and the SPAC’s stock price plunged —although the merger still closed as expected in July 2021.

Investors who purchased shares in the SPAC during the one-month interval before the merger announcement sued Lucid and its CEO for fraud under Section 10(b). The defendants moved to dismiss on the ground that the alleged misstatements had been made about Lucid, not about the SPAC. Notably, the court found the plaintiffs had standing despite that the alleged misstatements concerned a different company from which they had invested. This ruling is contrary to the Second Circuit’s ruling in *Menora Mivtachim Insurance Ltd. Frutarom Industries Ltd.*,

where the court held that to have standing, a plaintiff must have bought or sold the security about which a misstatement was made.

At the end of March 2023, the Southern District of New York dismissed a challenge to a de-SPAC transaction involving CarLotz. The company entered into a merger agreement with a SPAC in October 2020 and completed the merger in January 2021. By July 2021, the company's stock price dropped 50%, prompting a shareholder to sue its CEO, its CFO, and its general counsel for violations of Section 10(b). It was alleged that the defendants made false and misleading statements about the company with the truth coming out only *after* the de-SPAC transaction. Following the holding in *Menora Mivtachim*, the court dismissed 10(b) claim (and all others), holding that each of the statements had been made by a privately held CarLotz, prior to the merger. Further, the plaintiff had been a stockholder of the SPAC and not CarLotz.

Whistleblowers

In a banner year for whistleblowers, the biggest news was the $279 million award issued by the SEC to a single whistleblower, the largest ever award. However, this was far from the only newsworthy development in whistleblower cases in 2023. Some of the notable developments are discussed below.

SEC Whistleblower Program Has Record Setting Year

Fiscal Year 2023 set a record for the SEC's whistleblower program, with an aggregate of all awards issued reaching $600 million. The $279 million award referenced above more than doubled the previous award of $114 million issued in 2020. On August 4, 2023, the SEC announced a separate award of $104 million split between seven whistleblowers, the fourth largest award. Since the whistleblower program's inception in 2011, the SEC has issued $1.6 billion in awards to whistleblowers.

Eleventh Circuit Affirms Rejection of SOX Retaliation Claim

On September 25, 2023, the Eleventh Circuit in *Ronnie v. Office Depot LLC*, affirmed the Administrative Review Board's rejection of a SOX retaliation claim when it held that the employee did not engage in protected activity because he failed to establish that he had an objectively reasonable belief that the employer engaged in conduct that violated SOX.

The employee allegedly reported potential accounting errors to his supervisor that he claimed indicated securities fraud. After reporting the information to his supervisor, the petitioner allegedly complained to human resources that his supervisor was treating him differently. The petitioner was subsequently discharged.

OSHA dismissed the petitioner's complaint and an administrative law judge granted summary judgment to the employer on the grounds he did not establish that he had an objectively reasonable belief that the employer engaged in conduct, which violated SOX.

The Eleventh Circuit subsequently denied the petition, illustrating that the key issue was the evidence a SOX plaintiff must present to support their claim that their employer violated SOX. In order to gain protection under SOX, the Eleventh Circuit followed the Second and Fourth Circuits adopting the "totality of the circumstances

test," requiring a plaintiff to show scienter, materiality, reliance, or loss. Importantly, the court acknowledged that speculation or suspicion falls short of establishing a reasonable belief.

In 2024, it will be worth watching to see whether the U.S. Supreme Court will step in to address a circuit split on the standard in determining what constitutes a reasonable belief.

US Supreme Court Paves Way for DOJ to Dismiss Qui Tam Suits Under False Claims Act

In *Polansky v. Executive Health Resources Inc.*, the U.S. Supreme Court ruled that the DOJ has sweeping authority to intervene and voluntarily move to dismiss whistleblower claims brought under the *qui tam* provision of the False Claims Act (FCA). This authority still exists even when the DOJ previously allowed the claim to proceed.

The petitioner, a doctor who worked for a company that helped hospitals bill for Medicare-covered services, filed a *qui tam* action in 2012. After several years of litigation, the DOJ determined the suit was too burdensome to continue to litigate. The U.S. Supreme Court ruled in an 8-1 opinion that the government could seek voluntary dismissal under Federal Rule of Civil Procedure 41(a) so long as it first intervened in the case. We can now expect the government to increasingly intervene in cases and seek dismissal where it is not feasible to continue litigation.

Jarkesy and the SEC's Administrative Proceedings

In a case that could have wide-ranging implications for federal agencies that seek civil penalties through administrative proceedings, the Supreme Court appears ready to rule that the SEC's administrative proceedings are unconstitutional. The Court recently heard its longest oral argument of the term, taking a detailed approach in reviewing the Fifth Circuit's decision finding the proceedings are unconstitutional, in part because the administrative proceedings deprive the petitioner's right to a jury trial.

The high Court appeared to be hesitant to extend any potential ruling too far. For example, nearly two dozen federal agencies use administrative proceedings to impose civil penalties. If the Court's ruling applied to each of those agencies, every administrative law proceeding would need to be brought in federal court, potentially overwhelming an already overburdened court system.

However, the Court's ruling could be narrower if it found that the petitioner's case should have been brought before a federal court on common law claims, while not holding that the entire administrative system is unconstitutional. Alternatively, the Court could find that only the SEC's proceedings are unconstitutional. This would allow the administrative process across the two-dozen agencies to remain intact. The Social Security Administration employs the overwhelming majority of administrative law judges, deciding social security benefits. Dismantling that process could have a catastrophic effect on the social security system.

This will likely be the most important decision impacting administrative law in quite some time and will be key to watch in 2024.

Conclusion

While 2023 provided a number of key developments in a number of areas and a general uptick in enforcement, we

expect 2024 to be more of the same. Many companies, regardless of industry, will need to closely monitor further development in the cybersecurity space and increased whistleblower activity. We can also expect de-SPAC litigation to continue and potentially see a challenge to the U.S. Supreme Court. While Sam Bankman-Fried's sentencing will grab headlines, it will be far from the only major crypto development. The future of administrative law proceedings is also expected to change dramatically. Indeed, we can anticipate that 2024 will be an exciting year full of major developments in these spaces.

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- White Collar Litigation + Investigations
- Securities Investigations + Enforcement