New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW. NYLJ.COM
ALM.
JANUARY 24, 2023

Self-Reporting Misconduct to NYDFS: It's Not Your 'Monaco Memo' (Part Two)

This article discusses a specific disclosure requirement for a critical self-reporting obligation under what is known as "Part 500", the DFS Cybersecurity Regulation. It also addresses the consequences of failing to follow DFS self-reporting requirements, as revealed in recent DFS enforcement actions, and concludes with some general guidance on self-disclosure for DFS practitioners and regulated entities.

By Matthew L. Levine

By **Matthew L. Levine**

As noted in Part One of this article, issuance of the second "Monaco Memo" by the U.S. Department of Justice in October 2022 sparked debate anew about the self-reporting of misconduct by corporations. Settlements between the Justice Department and several large companies since then have brought greater clarity to the approach taken by Deputy Assistant Attorney General Lisa Monaco to corporate self-disclosure.

While these are notable developments for practitioners who defend corporations, they should be placed in context for counsel that represent entities supervised by the New York State Department of Financial Services (DFS). Numerous self-disclosure obligations already reside in New York statutes, regulations and supervisory agreements, as described more fully in Part One of this article. These requirements continue to be the North Stars guiding disclosure considerations for DFS-regulated entities.

This Part Two discusses a specific disclosure requirement for a critical self-reporting obligation under what is known as "Part 500" (23 N.Y.C.R.R. §500 et seq.), the DFS Cybersecurity Regulation. The article next addresses the consequences of failing to follow DFS self-reporting requirements, as revealed in recent DFS enforcement actions. The article concludes with some general guidance on self-disclosure for DFS practitioners and regulated entities.

Cyber Incident Reporting for Regulated Entities

DFS asserts it has "strengthened New York's leading position in cybersecurity" by creating a Cybersecurity Division which, among other things, has its own dedicated examiners. The regulator receives many hundreds of reports under its Cybersecurity Regulation each year. In 2021, these reports led the DFS cyber incident response team to investigate over 200 such events.

In other words, DFS takes reporting of Cybersecurity Events seriously. The two-pronged reporting regime under 23 N.Y.C.R.R. §500.17 requires a covered entity to notify DFS "as promptly as possible but in no event later than 72 hours" after determining a qualifying "Cybersecurity Event" has occurred.

Subsection 500.17(a)(1) requires reporting within 72 hours where "notice is required to be provided to any government body, self-regulatory agency or any other supervisory body[]." So, for example, where a data breach notice must be given to a state attorney general (e.g., N.Y. Gen. Bus. L. §899-aa), notice also should be provided to DFS within 72 hours of such determination.

Subsection (a)(2)—the one more likely to apply—requires 72-hour reporting where a Cybersecurity Event has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." Examples include where a malign actor penetrates an information technology system through phishing, social engineering, or a patch vulnerability, and then extricates or exposes customer data. Building on prior guidance, DFS directed regulated entities in December 2020 to report whether they had been impacted by the SolarWinds supply chain attack, an instruction that resulted in nearly 100 regulated institutions providing reports to DFS under §500.17.

Despite this weighty obligation, DFS has offered only modest guidance on Cybersecurity Event reporting, with just five FAQs addressing this requirement.

FAQ 25, for example, states that "to the extent a Cybersecurity Event involves material consumer harm, it is covered by [§ 500.17(a)(2).]" It bears emphasis that DFS is not just interested in cybersecurity incidents that impact New York consumers, as its regulatory focus is on the entity's cybersecurity program as a whole. DFS takes the view that, because it licenses the entity and it is the entity that operates the cybersecurity program, the entity is responsible for all consumer impact—not just effects on New York residents.

DFS also notes that Cybersecurity Event reporting is not limited to "successful" attacks. FAQ 21 provides lengthy but ultimately vague guidance about when to report "unsuccessful" attacks and includes this observation: "The Department anticipates that most unsuccessful attacks will *not* be reportable, but seeks the reporting of those unsuccessful attacks that, in the considered judgment of the Covered Entity, are sufficiently serious to raise a concern." In determining whether a particular unsuccessful attack should be reported, then, a Covered Entity might consider whether responding to the attack required measures or resources well beyond those ordinarily employed by the Covered Entity, like exceptional attention by senior personnel or the deployment of unusual tools.

DFS has also issued guidance about reporting ransomware attacks: "regulated companies should assume that any successful deployment of ransomware on their internal network should be reported to DFS as promptly as possible and within 72 hours at the latest pursuant to 23 NYCRR §500.17(a). Likewise, any intrusion where hackers gain access to privileged accounts should be reported." Even where there is no other harm caused or detected, DFS expects reporting of an incident where ransomware has been detected on a network within the required 72-hour window.

Certain DFS guidance on cyber incident reporting also has implications for reporting under a separate, more general disclosure provision applicable to banks and money service businesses, 3 N.Y.C.R.R. §300.4 (discussed in Part One of this article). Briefly, §300.4 mandates that banks and money service businesses report to DFS circumstances where an entity discovers a "plan or scheme" potentially of interest to similar DFS entities.

In industry guidance released in March 2021, DFS stated "[r]egulated entities … are reminded to report Cybersecurity Events pursuant to [§]500.17(a) as promptly as possible and within 72 hours at the latest … . *Reports of unsuccessful attacks have been useful in identifying techniques used by attackers and enabling DFS to respond quickly to new threats and continue to protect consumers and the financial services industry*." Implicitly, then, DFS suggests that cyber incidents that otherwise might not meet the threshold for reporting under §500.17(a)(2) nonetheless may be reportable by banks and money service businesses under 3 N.Y.C.R.R. §300.4, because such incidents might "relate[] to a plan or scheme and would be of interest to similar organizations located in the same area or throughout the State."

DFS recently issued proposed amendments to Part 500, including revisions to §500.17. These amendments appear to take into account some of the existing guidance discussed above, and also make explicit a reporting requirement for Cybersecurity Events occurring at a third-party service provider. As a result, decisions concerning whether to report an incident under §500.17 may become more complex and nuanced.

DFS Enforcement Actions Involving Self-Reporting Violations

Recent DFS enforcement actions addressing violations of reporting requirements under various laws and regulations provide practitioners with

insights into the regulator's expectations for self-disclosure.

Violations Involving Cybersecurity Event Reporting: DFS has repeatedly taken an enforcement action where it determined a regulated entity violated the cyber incident reporting requirement in §500.17(a). In *In the Matter of Carnival Corporation* (2022), for example, DFS penalized the cruise line for allegedly failing to report a damaging Cybersecurity Event pursuant to §500.17(a) for nearly a year—instead of within 72 hours—"due to the omission of the Department's notification requirement from the Carnival Companies' incident response plan."

In *In the Matter of Coinbase* (2022), the Department alleged that Coinbase, the cryptocurrency exchange, violated §500.17 when it delayed reporting that approximately 6,000 Coinbase customers were victims of a phishing scam that ultimately led to unauthorized access of the customers' accounts. DFS noted that Coinbase had reported the event to the U.S. Secret Service several months before notifying DFS.

Similarly, in *In the Matter of National Securities Corporation* (2021), DFS asserted there were at least three Cybersecurity Events experienced by this insurance company that either were reported late, or went unreported. In at least one of the instances, National Securities had notified customers and four other government agencies of the cyber incident, but did not timely report it to DFS.

And in *In the Matter of Residential Mortgage Services* (2021), DFS penalized a mortgage originator because it found that the firm waited nearly 18 months to undertake an appropriate investigation of harmful a Cybersecurity Event and

then make appropriate disclosures under various state notification laws, "and only after prompting by the Department." Together, these enforcement actions demonstrate that DFS places a significant onus on regulated entities to timely comply with the cyber event notification requirement.

Violations Involving §300.4 Reporting: Perhaps one of the most aggressive applications of 3 N.Y.C.R.R. §300.4 occurred in *In the Matter of Goldman Sachs Group* (2020), an enforcement action that penalized Goldman Sachs with a significant fine of $150 million. There, DFS found that several high-level personnel in Goldman Sachs Group's international broker-dealer were involved in a theft and bribery scheme involving billions of dollars of economic development funds borrowed by the Malaysian government. These funds had been raised through bond offerings underwritten by Goldman's international broker-dealer.

Goldman also has an affiliate that is a retail bank regulated by DFS, known as Goldman Sachs Bank USA (GSBUSA). Red flags and other information identified by transaction review committees in other Goldman affiliates about the Malaysian bond sale would have been of substantial interest to GSBUSA, according to DFS findings, as well as to other entities regulated by DFS.

Among other things, an affiliate of a *different* DFS licensee purchased a significant amount of the Malaysian bonds at issue, which DFS alleged were materially at risk of default due to the corruption scandal. Goldman's holding company and GSBUSA were penalized for the failure of the holding company to impart information to GSBUSA, where that entity then would have been required to share with DFS the information about the red flags discussed above under §300.4. This was a novel and impactful application of that regulation by DFS.

Violations Involving §300.1 Reporting: In *In the Matter of UniCredit AG* (2019), DFS found that an affiliate of a European bank, UniCredit A.G., processed approximately $61 million in payments through the U.S. banking system that were illegal under federal economic sanctions laws. To carry out the scheme, DFS alleged that UniCredit employed opaque payment messages that intentionally concealed the nature of these payments from DFS examiners, including some messages transmitted through other financial institutions regulated by the Department.

DFS determined that this constituted a violation of the self-reporting requirement contained in 3 N.Y.C.R.R. §300.1 because UniCredit failed to report it "immediately upon discovering … [the] making of false entries or omission of true entries." Notably, DFS also found a separate violation of 3 N.Y.C.R.R. §300.4, because UniCredit failed to report these illegal transactions that flowed from an unlicensed UniCredit affiliate and then through other DFS-licensed entities, which would have wanted to be warned about them.

Supervisory Agreements: In *In the Matter of Robinhood Crypto* (2022), DFS had entered into a Supervisory Agreement with the crypto arm of Robinhood Financial, which has a "Bitlicense" from the Department that allows it to operate a cryptocurrency business. Among other provisions, the Supervisory Agreement required Robinhood Crypto to "promptly notify DFS of any actual or material potential action, proceeding, or similar process that has been or may be instituted against [Robinhood Crypto] or any affiliated entity by any regulatory body or government agency." As part of a sweeping enforcement action, DFS found that Robinhood "failed to disclose investigations by federal and state regulators of [a Robinhood] affiliated entity, in violation of reporting obligations governed by [the] Supervisory Agreement." Although no particular investigation was identified by DFS, Robinhood reported in public filings that, at least by Aug. 4, 2021, it had received subpoenas and investigatory demands from several federal and state government agencies.

Guidance in Self-Reporting to DFS

In light of the agency's history, practices, and guiding laws and regulations, several additional factors may aid practitioners in weighing how to approach a decision about self-reporting to DFS:

- As discussed above and in Part One, disclosure requirements are sourced in law, regulations and agreements. These deserve careful and periodic review by a regulated entity's legal and compliance personnel, and should be matched by timely updating of policies and procedures related to DFS notification requirements.
- For licensed entities, a constructive relationship with DFS is best fostered through transparency, an approach that helps maintain the regulator's trust in the entity's conduct such that—when an issue does arise—DFS staff will extend the benefit of the doubt to the entity.
- Even where an incident is not "required" to be reported to DFS, consideration nevertheless should be given to self-disclosure in circumstances where: (1) there is a change in key personnel; (2) an event will be reported in the media or SEC filings and may cause reputational harm to the entity; or (3) an unusual incident occurs involving a high-profile or high-level manager or a Board member.

In sum, engagement with clients regulated by DFS about self-reporting is usually around when and how to self-report—not about whether to report. DFS laws, regulations, agreements and practice strongly counsel this approach.

Matthew L. Levine *is a partner at Elliott Kwok Levine & Jaroslaw. He previously served as Executive Deputy Superintendent for Enforcement at the New York State Department of Financial Services and as a federal prosecutor.*