New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
ALM.
WWW.NYLJ.COM
VOLUME 268—NO. 104
WEDNESDAY, NOVEMBER 30, 2022

Expert Analysis

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

By **Matthew L. Levine**

Issuance of the second "Monaco Memo" by the Department of Justice in October 2022, which places an even greater emphasis on self-reporting of wrongdoing by corporations, has reignited discussion about the propriety of disclosure to government agencies. Perhaps some of the greatest debates between outside counsel and their corporate clients occur over issues of whether to self-report and, if so, the timing and manner of doing so. Direct and collateral consequences need to be considered, often requiring a complex and nuanced analysis.

Yet this discussion tends to be more settled for entities supervised by the New York State Department of Financial Services (DFS). That is because numerous self-reporting obligations already reside in New York statutes, regulations and supervisory agreements with regulated entities. These rules require or encourage timely—sometimes even immediate—disclosure of a wide range of incidents, misconduct and criminal activity.

DFS Superintendent Adrienne Harris recently described the agency's expectations about self-reporting plainly: "The No. 1 rule that we always try to impress upon people is, as you know, do not surprise your regulator. If we read about it before we hear from you on it, we're already starting off in a bad place."

Yet some institutions supervised by DFS have continued to approach self-reporting in a fashion that placed them in a less advantageous position at the conclusion of a supervisory or enforcement action because of the delay in, or lack of, disclosure. Self-reporting to DFS is guided both by general principles embraced by the agency, as well as specific disclosure obligations set forth in statute, regulation, and by agreement.

Part One of this article discusses these principles and requirements for regulated entities, with a focus on banking organizations, money service businesses, cryptocurrency firms, and insurance companies. Part Two will consider the disclosure regime for reporting of a "Cybersecurity Event" under the DFS cybersecurity regulation for all regulated entities. Part Two will also address the consequences of failing to follow DFS self-reporting requirements as revealed in recent DFS enforcement actions, and will offer guidance on disclosure for regulated entities.

> Perhaps some of the greatest debates between outside counsel and their corporate clients occur over issues of whether to self-report and, if so, the timing and manner of doing so

First Principles for DFS That Guide Self-Reporting Considerations

DFS guiding principles are derived from its enabling laws and issued regulations. Section 201(b)(5) of the Financial Services Law, for example, assigns to DFS the legislative purpose

MATTHEW L. LEVINE *is a partner at Elliott Kwok Levine & Jaroslaw. He previously served as Executive Deputy Superinten ent for Enforcement at the New York State Department of Financial Services*

of encouraging "high standards of honesty, transparency, fair business practices and public responsibility" in financial markets.

Yet DFS is influenced by factors other than these enactments in its approach to supervision. Among its licensees, for example, DFS regulates the foreign branches of many global banks, with some of the larger branches managing assets in the tens of billions of dollars. New York is also a prime location for fintech, cryptocurrency and cybersecurity industries. And with the fourth largest population in the United States, New York is a consumer behemoth. Thus, guiding principles for DFS self-reporting requirements, while sourced in New York laws and regulations, are also reflected in the agency's experience and perspective as the state regulator in the world's financial capital. Key regulatory priorities for DFS include:

• *Safety and Soundness:* DFS is first and foremost a prudential regulator and thus concerned with the safety and soundness of a licensed institution. As with any regulated entity, adequate capitalization, liquidity, and competent operational ability are core focus areas for DFS supervision.

• *Consumer Protection:* DFS is laser focused on protecting customers of regulated entities, especially—but not exclusively—New York residents. Safeguarding customer assets and preventing misleading or abusive sales practices are among its central concerns.

• *Cybersecurity:* Since at least 2017, DFS has been deeply concerned about cybersecurity. While cybersecurity is now squarely on the plate of most other regulators as well, DFS has been in the forefront among financial agencies and sees itself as a regulatory leader. Cybersecurity lapses that result in data breaches, ransomware attacks, and operational paralysis may cause severe damage to a financial institution and its customers, and a single serious incident may cause DFS acute concern.

• *Repeat Compliance Deficiencies:* DFS typically trains its focus on regulated entities it believes are unable to timely correct deficiencies in their compliance programs, particularly around Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and Office of Foreign Assets Control (OFAC) programs, and usually after two or three disappointing examination cycles. Preventing money laundering, terrorist financing and other illicit activity "continues to be incredibly important," according to Superintendent Harris.

New York law imposes fewer specific reporting requirements on insurance companies and producers relating to misconduct, when compared to banking and money service businesses.

• *Transparency:* DFS views transparency as the principal tool by which it accomplishes agency priorities. DFS tends to apply the broadest possible reading to its enabling laws and regulations in support of seeking transparency from regulated entities. This can have a spill-over effect into the broad reach of its jurisdiction—at least as DFS perceives it.

Self-Reporting by Banks and Money Service Businesses

3 N.Y.C.R.R. §300.1: Banks and money service businesses are subject to this mandatory reporting regulation for certain types of misconduct. Under §300.1, a covered entity must *immediately* report any of the following: "embezzlement, misapplication, larceny, forgery, fraud, dishonesty, making of false entries and omission of true entries, or other misconduct, whether or not a criminal offense, in which any director, trustee, partner, officer, employee (excluding tellers), or agent of such organization is involved." Thus, certain offenses in the nature of a theft of funds by an employee or officer is immediately reportable.

More nuanced analysis may be required when determining whether an incident constitutes "*other misconduct*" that is reportable involving management or an employee. DFS does not restrict its reading of §300.1 to "theft-of-funds" type events, even though it may be read this way under the principle of ejusdem generis.

DFS also applies a generous reading to the term "making of false entries and omission of true entries" with respect to reporting obligations. Because there is no express requirement of malign intent in this section, DFS may apply this requirement expansively to a variety of activities arising from unintentional conduct.

Accordingly, when analyzing whether to disclose under §300.1, consideration should be given to reporting events such as: (a) an incident evidencing a systemic breakdown in controls, particularly in an

area of primary concern to DFS; (b) an event that involves a pattern or practice of noncompliance, particularly where it has been called out by DFS previously in a report of examination or other formal context; (c) an event that involves a particularly egregious situation or substantial reputational damage, even if it is an isolated event and even if the institution's involvement is tangential; (d) an incident concerning a compliance issue that senior management has determined requires disclosure to the Board; and (e) an event being reported to FinCEN, OFAC or another regulator or government agency through mandatory or voluntary reporting.

As noted, §300.1 calls for "immediate" reporting. Oftentimes, for large financial institutions, the full scope of the misconduct to be reported is not apparent at first. Consideration should be given to reporting in piecemeal fashion as factual development occurs. As noted by the DFS Superintendent, having the agency discover an incident via other means, e.g., from another licensed entity, after an SEC filing, from press reports, or by way of a whistleblower, may seriously undermine the supervisory relationship between a regulated entity and DFS. It is not unusual, for example, for a large financial institution to give advance notice to DFS personnel—supervision staff, enforcement staff, or both depending on the regulatory posture—shortly before an unfavorable media report about the institution is going to be released.

3 N.Y.C.R.R. §300.3: Section 300.3 essentially requires a reporting entity to update DFS on any "material developments" relating to an initial report under §300.1, along with a "statement of actions taken or proposed to be taken with respect to such developments." Additionally, this section requires a reporting entity to submit "a statement of the changes, if any, in its operations which are deemed desirable and feasible by its directors or trustees in order to avoid repetition of similar events."

While most responsible entities reporting under §300.1 will also update DFS on material developments and any remediation necessary, §300.3 is noteworthy because it specifically assigns this responsibility to the entity's Board of Directors or Trustees.

3 N.Y.C.R.R. §300.7: Entities also should be aware of §300.7, which states, "[e]very organization which discovers or experiences any of the incidents described in §300.1 of this Part is strongly urged to report the details thereof to the appropriate State and local law enforcement authorities, to the local office of the Federal Bureau of Investigation, if appropriate, and to the insurance carrier, even though such incident may not be required to be reported to the department because of the size of the loss involved."

Two factors should be considered here. First, while the regulation "strongly urges" the regulated entity to report to law enforcement, it is still a discretionary call, and a decision if and when to report to law enforcement may be complex. Second, it is almost never an excuse not to report to DFS because reporting has already been made to law enforcement. While the FBI will occasionally suggest that an entity delay reporting to a regulator, it is almost never a good idea to unquestioningly follow this "suggestion"—the regulations do not offer a grace period, and great care should be exercised if this course is ever considered as a basis to delay notification to DFS.

3 N.Y.C.R.R. §300.4: Section 300.4 creates another category of mandatory reporting, addressing circumstances where an entity discovers a "plan or scheme" potentially of interest to similar DFS entities. Specifically, an entity must report "any other incident if there are indications that it, or any act therein involved, relates to a plan or scheme and would be of interest to similar organizations located in the same area or throughout the State." No explicit timing requirement is embedded in the regulation but prompt reporting is contemplated. The type of reporting anticipated by this regulation is gauged by the nature of the plan or scheme identified by the regulated entity.

What to report is not easily defined. The regulation is broadly worded, calling for both judgment and open-mindedness. This regulation was enacted in approximately 1971—well before consumer and commercial use of the internet, and its drafters likely had in mind incidents such as an organized ring of bank robbers or check kiters. As with many regulations, it has to be viewed in terms of advances in technology and has taken on greater significance in light of widespread cybercrime directed at or adjacent to financial institutions.

Where there is a significant, unique or fast-moving criminal event or course of suspicious conduct that impacts a regulated entity, or otherwise comes to its attention, the entity should strongly consider immediately notifying DFS under §300.4. Indicia suggesting the existence of a scheme or plan, such as clear evidence of interconnections among actors, or common electronic fingerprints such as IP addresses, suggest it is a reportable event.

Section 300.4 does not specify the timing required for this type of reporting category. Consideration should be given to how well developed the information is, whether the plan or scheme may have a substantial impact on other institutions, and how the reporting institution became aware of the information.

Supervisory Agreements: Certain notice and reporting requirements are typically included in the supervisory agreement between DFS and a regulated entity. Supervisory requirements generally include reporting concerning material events, such as lawsuits, regulatory subpoenas, or investigations by other government agencies. Such notice and reporting obligations are binding, and a violation of these written requirements will subject an entity to all available penalties under the Banking and Financial Services Laws.

Self-Reporting by Cryptocurrency Firms

23 N.Y.C.R.R. §200.14: Section 200.14 applies to entities that have received a virtual currency license (BitLicense) from DFS. Subsection (e) of this provision requires each regulated entity to "submit a report to the superintendent immediately upon the discovery of any violation or breach of law, rule or regulation related to the conduct of activity licensed under this Part."

This subsection is concrete in the sense that it mandates reporting only when a regulated entity has identified an actual (or very likely) violation or breach of a law, rule or regulation, and it applies with certainty to DFS laws and regulations. Because it is broadly written, it might also apply where an entity has determined to self-report a criminal violation like potential wire fraud, criminal spoofing or antitrust violations. Special attention should be given to potential violations of federal civil or criminal law, including federal banking laws and regulations. Indeed, DFS typically expects notification even where a licensee has determined it violated the laws or regulations of other jurisdictions, and sometimes even other nations.

Separate subsection 200.14(c) only requires notification to DFS where a criminal or bankruptcy proceeding has actually been commenced against the licensee or any of its "directors, Principal Stockholders, Principal Officers, and Principal Beneficiaries." In such an instance notification should be immediate.

For cryptocurrency firms that have received a "limited purpose trust charter" from DFS, they are separately regulated under the Banking Law, and thus subject to §§300.1, 300.3, 300.4 and 300.7 discussed above.

Self-Reporting by Insurance Companies and Producers

New York law imposes fewer specific reporting requirements on insurance companies and producers relating to misconduct, when compared to banking and money service businesses. Assets and funds held by insurance companies do not belong to customers and insurance companies typically are not active market participants, like banks and crypto firms or their customers, so immediate reporting may be understood as less necessary.

One specific reporting requirement, Insurance Law §405, obligates any person or entity licensed pursuant to the insurance laws to report an insurance transaction or life settlement that is or may be fraudulent within 30 days after making such a determination. According to DFS, this requirement resulted in more than 34,000 reports of suspected fraud in 2021, resulting in 283 new investigations by the DFS Insurance Frauds Bureau, a team of experienced criminal investigators.

This summary describes a number of important self-reporting requirements for DFS entities. As noted, Part Two of this article will continue with a discussion of the disclosure regime for reporting of a "Cybersecurity Event" under the DFS Cybersecurity Regulation, some relevant DFS enforcement actions, and guidance on disclosure for regulated entities.