3 Cybersecurity Imperatives For Financial Cos. In 2022

By **Shardul Desai** (January 19, 2022)

Shardul Desai

Following the SolarWinds Corp. and Colonial Pipeline Co. cyberattacks, the Biden administration emphasized a shift toward mandatory cybersecurity requirements.[1] Consistent with those efforts, at the end of 2021, federal agencies promulgated final rules concerning cybersecurity requirements for the financial services sector.

The Federal Trade Commission amended its Gramm-Leach-Bliley Act Safeguards Rule to require FTC-regulated financial institutions to develop and implement detailed cybersecurity requirements as part of an information security program.[2] The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corp. issued cybersecurity incident notification requirements.[3]

Additionally, the U.S. Securities and Exchange Commission and the New York Department of Financial Services announced their first-ever enforcement actions against financial services companies for the alleged failure to comply with the agencies' cybersecurity requirements.[4]

These developments will affect the financial services industries in three respects in 2022:

1. Financial services companies should develop and implement a comprehensive cybersecurity program.

2. Financial services companies should design an internal cybersecurity reporting system to ensure timely notification to regulators within hours of discovering a cybersecurity incident.

3. Financial service companies should encourage a culture of compliance on cybersecurity matters to prepare for potential enforcement investigations by financial regulators.

1. Develop and Implement a Comprehensive Cybersecurity Program

Mandatory Cybersecurity Requirements

The GLBA requires financial institutions to protect the security and confidentiality of their customers' personally identifiable financial information.[5] As a result, the various federal financial regulatory agencies have promulgated Safeguards Rules to establish information security standards to protect their customers' information.

The FTC has regulatory authority over financial institutions that are not subject to another agency's regulatory authority, which includes, but is not limited to, mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors, financial advisers, tax preparation firms, credit unions that are not federally insured, personal property appraisers, certain investment advisers, certain travel agencies and certain automobile dealerships.[6]

On Oct. 27, 2021, the FTC amended its GLBA Safeguards Rule. Preliminarily, the FTC expanded its jurisdiction to include finders, which are companies that bring together buyers

and sellers of a product or service for transactions that the parties themselves negotiate and consummate.[7]

In addition, the FTC final rule requires financial institutions with 5,000 or more consumers to develop and implement specific cybersecurity requirements within their information security program. Some of these requirements include the following:[8]

- Develop written risk assessments;
- Review access controls periodically;
- Encrypt customer information in transit and at rest;
- Implement multifactor authentication, or MFA;
- Log user activities;
- Monitor continuously or test periodically through annual penetration testing and bi-annual vulnerability assessments;
- Establish a written incident response plan; and
- Provide, at least annually, written reports to the board of directors or equivalent governing body concerning the financial institution's information security program.

The FTC final rule is a significant departure from the previously required information security program. These new FTC requirements are similar to the NYDFS Cybersecurity Regulations,[9] although the FTC final rule does not require senior leadership to certify the information security program.[10]

With both the NYDFS and FTC requiring financial services companies to implement detailed cybersecurity requirements, the OCC, Fed and FDIC likely will consider adopting similar requirements where they are currently lacking such regulation.

Last year, the NYDFS also started enforcement actions against financial service companies for the alleged failure to comply with the NYDFS Cybersecurity Regulations, which became fully effective in 2019.[11]

Similarly, although the FTC rule has an applicability date of Dec. 9, 2022, regulated financial institutions have a short window to implement these substantive cybersecurity requirements before regulators turn their attention to enforcement.

Key Takeaways for 2022

More regulators are moving toward the NYDFS model of requiring a comprehensive cybersecurity program. With the FTC's adoption of a similar program in 2021, the OCC, Fed, FDIC and SEC may not be too far behind.

Although FTC-regulated financial institutions have until Dec. 9, 2022, to comply with the FTC's cybersecurity requirements, this may not be sufficient time to implement such requirements. These requirements may require a complete reassessment of an institution's information technology environment and significant financial investment toward IT upgrades

and projects. This may leave institutions scrambling toward compliance.

Institutions regulated by the FTC need to immediately assess their IT environments and develop a plan to ensure compliance with the FTC's cybersecurity requirements. The NYDFS recently published guidance on MFA after witnessing repeated errors in MFA implementation.[12] Thus, institutions should determine a method of ensuring these requirements are implemented effectively.

Institutions that are not subject to detailed cybersecurity standards should consider developing and implementing a written cybersecurity program similar to those required by the NYDFS Cybersecurity Regulations and the FTC cybersecurity requirements. Not only would such a program better protect institutions from potential cyberattacks, but such a requirement may be forthcoming.

2. Design an Internal Disclosure System for Cybersecurity Incidents

Notification Regulations

On Nov. 18, 2021, the OCC, Fed and FDIC issued a joint final Computer Security Incident Notification Rule that requires banking organizations[13] to notify their primary federal regulator of any computer security incident that rises to the level of a notification incident within 36 hours of determining such an incident occurred.[14]

A computer security incident is "an occurrence that results in actual harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits."[15]

Notification incidents are a subset of computer security incidents that have

> materially disrupted or degraded, or [are] reasonably likely to materially disrupt or degrade, a banking organization's 1) ability to carry out banking operations, activities or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business, 2) business line(s), including associated operation, services, functions and support, that upon failure would result in a material loss of revenue, profit or franchise value, or 3) operations, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.[16]

System outages, successful ransomware attacks and successful distributed denial of service attacks are likely notification incidents.[17] However, determining whether an incident is a notification incident is a fact-dependent analysis.

Notifications are not exempt from Freedom of Information Act requests. Although the agencies received a comment requesting such exemption, they rejected the suggestion in lieu of their confidentiality rules.[18] Additionally, banking organizations should be careful not to disclose, and thereby potentially waive, privileged information as part of their notification to regulators.

The joint final rule also does not replace or eliminate other notification obligations. Under the agencies' Safeguards Rules, covered entities are to notify their primary federal regulator as soon as possible when they become aware of an incident involving unauthorized access to or use of sensitive customer information.[19] As a result, the joint final rule creates

bifurcated notification obligations for certain financial institutions.

In addition, other government agencies require regulator notification for cybersecurity events. The NYDFS Cybersecurity Regulations require cybersecurity events to be reported to the NYDFS within 72 hours.[20] The SEC requires public companies to disclose material cybersecurity incidents or risks.[21] Although the FTC currently does not require reporting, the agency announced its intention to adopt a notification requirement for cybersecurity incidents.[22]

The joint final rule also requires bank service providers[23] to notify banking organization customers as soon as possible of any computer security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a covered service for four hours or more.[24]

Banking organizations are required to assess these notifications to determine whether they are notification incidents that need to be reported to their primary federal regulator. The joint final rule is enforceable as of May 1, 2022.[25]

This past year, the SEC also brought enforcement actions on companies that failed to internally report cybersecurity incidents or risks to corporate decision makers in a timely manner. Such internal disclosure controls are critical to ensure timely notification of cyber incidents as required by regulations.

Key Takeaways for 2022

Regulators are requiring notification for cybersecurity incidents and data breaches. The fact that the joint final rule creates bifurcated notification obligations highlights the regulatory convolution in this area. Moreover, the FTC has announced its intentions to join the fray. As such, financial services companies should prepare to notify one or more regulators when they experience a cybersecurity incident.

The joint final rule's 36-hour notification requirement creates a short window between the discovery of a cybersecurity incident and notification. The agencies recognize that the clock only starts upon a banking organization's determination that the incident is a notification incident, and "the agencies anticipate that a banking organization would take a reasonable amount of time to determine that it has experienced a notification incident."[26]

However, this "reasonable amount of time to determine" standard will be subject to agency interpretation and hindsight. Moreover, as the SEC's recent enforcement actions concerning internal disclosure controls inform, regulators can be unforgiving to internal reporting delays.

Notifications to regulators potentially expose financial services companies to litigation and reputational risks. These notifications may be publicly discoverable through a FOIA request, and statements made in these notifications could potentially impact subsequent civil litigation against the financial services companies.

Financial services companies also should be cautious not to include privileged information in these notifications. Additionally, the determination that a cybersecurity incident requires notification often is a legal determination. As a result, financial services companies should consider including their counsel in assessing cybersecurity incidents and in notifying federal regulators of such incidents. The incident response plan also should identify the individual responsible for providing notification.

Financial services companies should consider developing a robust internal disclosure system to ensure cybersecurity incidents are reported to corporate decision makers and counsel almost immediately upon discovery. This is particularly necessary for banking organizations due to the 36-hour notification requirement.

This internal disclosure system should be part of the written incident response plan. In addition, financial services companies' IT teams should be trained on the use and importance of this internal disclosure system, and the internal disclosure system should be tested to ensure effectiveness.

3. Develop Culture of Cybersecurity Compliance

Cultural Considerations

In 2021, the SEC and NYDFS brought enforcement actions against financial services companies for allegedly failing to comply with the agency's cybersecurity requirements. Moreover, Deputy Attorney General Lisa Monaco recently emphasized that the U.S. Department of Justice will evaluate a company's history of compliance issues in future enforcement actions.[27]

As enforcement actions related to cybersecurity standards increase, regulators likely will consider a company's compliance program and culture of compliance in their investigations and enforcement actions.

Key Takeaways for 2022

Cybercriminals are constantly evolving, and new sophisticated cyberattacks will continue to occur in 2022.

Because no IT system is impenetrable, some of these attacks will be successful. This past year, regulators have signaled their intentions to pursue enforcement actions against financial services companies for cybersecurity vulnerabilities. With mandatory notifications, successful cyberattacks will bring regulatory scrutiny and investigations.

Companies should consider incorporating cybersecurity into their existing compliance programs, emphasizing and training IT professionals on cybersecurity compliance, developing robust internal controls for cybersecurity-related disclosures, and developing effective methods to audit their cybersecurity compliance program.

Fostering a culture of compliance and developing a cybersecurity compliance program is a highly effective way to avoid enforcement actions and to reduce potential penalties from such actions.

Conclusion

Cyberattacks and regulators' cybersecurity enforcement actions will continue to increase in 2022. Financial services companies that want to protect themselves from cyberattacks and regulatory investigations should develop and implement comprehensive cybersecurity programs, design internal controls for immediate disclosure of cybersecurity incidents and risks, and foster a culture of cybersecurity compliance.

Shardul Desai is a partner at Holland & Knight LLP. He was previously a federal prosecutor in the Cyber and National Security Section and the Economic Crimes Section at the U.S. Attorney's Office for the Western District of Pennsylvania, where he was the computer hacking and intellectual property assistant U.S. attorney for more than eight years.

[1] See, e.g., Executive Order on Improving the Nation's Cybersecurity (May 12, 2021); National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021); TSA Pipeline Security Directives (July 20, 2021); DOJ Civil Cyber-Fraud Initiative (Oct. 6, 2021); and DOD's CMMC 2.0 (Nov. 17, 2021).

[2] Federal Trade Commission, Standards for Safeguarding Customer Information Final Rule, 86 Fed. Reg. 70,272 (Dec. 9, 2021); FTC Press Release, "FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches," (Oct. 27, 2021).

[3] Computer-Security Incident Notification Requirement for Banking Organizations and their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021); Joint Release, "Agencies Approve Final Rule Requiring Computer-Security Incident Notification," (Nov. 18, 2021).

[4] Law360, Ira Rosner and Shardul Desai, "Managing Risk After SEC's Cyber Enforcement Action."

[5] 15 U.S.C. §§ 6801(a), 6809; 86 Fed. Reg. at 70,3045.

[6] 15 U.S.C. § 6805(a)(7); 86 Fed. Reg. at 70,3045.

[7] Standards for Safeguarding Customer Information Final Rule, 86 Fed. Reg. at 70306 (16 CFR § 314.2(h)(2)(xiii)).

[8] Standards for Safeguarding Customer Information Final Rule, 86 Fed. Reg. at 70,307-08 (16 CFR § 314.4).

[9] NYDFS, Cybersecurity Regulations, 23 CRR-NY 500, et. seq.

[10] Standards for Safeguarding Customer Information Final Rule, 86 Fed. Reg. at 70299.

[11] See, e.g., NYDFS, "DFS Superintendent Lacewell Announces Cybersecurity Settlement with First Unum and Paul Revere Life Insurance Companies" (May 13, 2021).

[12] NYDFS, Guidance on Multi-Factor Authentication (Dec. 7, 2021).

[13] Under the OCC's rule, banking organizations mean national banks, federal savings associations, and federal branches and agencies of foreign banks. Under the FRB's rule, banking organizations means U.S. bank holding companies, U.S. savings and loan companies, state member banks, U.S. operations of foreign banking organizations, and Edge and agreement corporation. Under the FDIC's rule, banking organizations means insured state nonmember banks, insured state-licensed branches of foreign banks, and

insured State savings associations. The definition specifically excludes financial market utilities. See 15 U.S.C. § 6805(a); 12 U.S.C. § 1813 (q); Computer-Security Incident Notification Requirement for Banking Organizations and their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).

[14] Computer-Security Incident Notification Requirement for Banking Organizations and their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).

[15] Id. (to be codified at 12 CFR § 53.1; 12 CFR § 225.301, 12 CFR § 304.22).

[16] Id.

[17] 86 Fed. Reg. at 66,431 (furnishing a list of example notification incidents).

[18] 86 Fed. Reg. at 66,437.

[19] 12 CFR pt. 30, app'x B, supp. A (OCC); 12 CFR part 208, app'x D-2 (FRB); 12 CFR part 225, app'x F (FRB); 12 CFR part 364, app'x B (FDIC).

[20] 23 CRR-NY 500.17.

[21] See SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures (Feb. 21, 2018).

[22] Federal Trade Commission, Standards for Safeguarding Customer Information Final Rule, 86 Fed. Reg. 70,272, at 70,298 (Dec. 9, 2021).

[23] Bank service provider means a bank service company or other person that performs covered services. The rule specifically excludes financial market utilities from the definition. See Computer-Security Incident Notification Requirement for Banking Organizations and their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021) (definition to be codified at 12 CFR § 53.2(b)(2), 12 CFR § 225.301(b)(2), and 12 CFR § 304.22(b)(2).

[24] Computer-Security Incident Notification Requirement for Banking Organizations and their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021).

[25] Id.

[26] Id. at 66432.

[27] "DOJ Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime" (Oct. 28, 2021).