NEWSLETTER – OCTOBER 2024

REGULATORY RISK PERSPECTIVES

1. Artificial Intelligence and Combating Increasing Cybersecurity Risks

Earlier this month, the New York State Department of Financial Services ("NYSDFS") issued the 'Cybersecurity Risks arising from Artificial Intelligence ("AI") and Strategies to Combat Related Risks' guidance ("Guidance") to help Financial Institutions ("Fis") in understanding and assessing cybersecurity risks associated with the use of AI and the controls that may be used to mitigate those risks[1]. The Guidance acknowledging the benefits of AI, highlights some of the more concerning cybersecurity threats but cautions that the Guidance is not intended to address every possible risk.

Amongst the major items covered by the Guidance are that AI can accelerate the development of new malware variants and change ransomware to enable it to bypass defensive security controls, thereby evading detection. In addition, the AI enabled social engineering which uses more sophisticated and convincing techniques which creates realistic audit, video or text content referred to as 'deepfakes', which can then target individuals via email, telephone, text messaging, videoconferencing and with online postings. These attacks not only impact customers of the financial institutions but also employees and can result in disclosing nonpublic information about systems or customer records or can lead to fraudulent unauthorized wire transactions. The guidance also covers the risks for FIs using AI powered tools/applications involving TPSPs, who may be compromised due to a cybersecurity incident.

The Guidance does not alter any of the existing regulatory requirements concerning cybersecurity and reinforces the programs and plans designed to enhance controls and mitigate cybersecurity risk. However, it adds some useful considerations designed to combat the impacts of heightened cybersecurity risks associated with usage of AIs. These include updating policies, procedures and incident response plans to address AI threats; accessing AI risks attributable to any in-house use of AI, as applicable; understanding vulnerabilities that may be linked to any AI applications in use; evaluating TPSP's AI related risks; evaluating the strength of access controls to combat AI-enhanced social engineering attacks, and ensuring that Mult-Factor Authentication practices are in place; implementing training programs concerning AI across the organization to create an awareness of how AI and social engineering techniques are being used to facilitate cyberattacks, and fraud; enhancing monitoring controls as it relates to system access, system changes and responses to system alerts; and enhancing data management controls with a view to limiting access to non-public and confidential information.

[1] https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks

This is a good reminder of the increasing cyberthreats, including those associated with use of technology and AI. As the year-end approaches it may be advisable to reassess the cybersecurity risks and associated controls, including those associated with AI and use of third-party vendors.

FINCEN UPDATES

1. FinCEN Fines TD Bank $1.3 Billion for BSA Violations

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) assessed a record $1.3 billion penalty against TD Bank, N.A. and TD Bank USA, N.A. for violations of the Bank Secrecy Act (BSA)[2]. This penalty is the largest penalty against a depository institution in U.S. Treasury and FinCEN history and imposes lookback and independent monitorship requirements.

In reviewing the bottom line of this failure, it is revealing to note that, most of the issues cited appear to be standard BSA Program requirements and includes some areas where other financial institutions have been criticized earlier. Some of the failures include:

- Failure to Ensure Sufficient Staffing and Resources for BSA/AML Compliance
- Failures in Governance and Oversight, and severe underinvestment in AML compliance
- Inadequately designed and/or implementation of the AML Program
- Inadequate monitoring, including of high risk customers and payment system activities, and employee activities
- Violations of Suspicious Activity Report (SAR) filing requirements
- Lack of addressing risks associated with funnel accounts and "High-Risk" jurisdictions
- Training gaps
- Failure to implement and maintain appropriate risk-based customer due diligence (CDD)
- Violations of Currency Transaction Report (CTR) filing requirements
- Ineffective Independent Testing

As part of the settlement, TD Bank admitted having willfully failed to implement and maintain appropriate AML program. FinCEN's investigation revealed that TD Bank knew that its AML program was neither appropriately designed nor adequately resourced resulting in inadequate monitoring and reporting.

[2] https://www.fincen.gov/news/news-releases/fincen-assesses-record-13-billion-penalty-against-td-bank

This enforcement action and fine is a good reminder of the importance of ensuring that institutions have a comprehensive, risk-based but robust BSA Program that is implemented and is operating effectively with appropriate staffing, expertise and oversight.

As the year-end approaches it may be a good time to reassess BSA/AML program, especially given the added risks presented by AI, backlogs, gaps and resource constraints.

2. FinCEN Issues New Rules to Combat Illicit Financing

In late August 2024, FinCEN issued two rules to help safeguard the residential real estate and investment adviser sectors from illicit finance[3]. The residential real estate rule requires certain industry professionals to report information to FinCEN about non-financed transfers of residential real estate to a legal entity or trust, which presents a high risk of being an illicit finance transaction. The rule is aimed at increasing transparency and is intended to limit the ability of bad actors to anonymously launder illicit proceeds through the American housing market, and at the same time will provide additional useful information to help law enforcement investigative efforts.

The investment adviser rule applies anti-money laundering/countering the financing of terrorism (AML/CFT) requirements—including AML/CFT compliance programs and suspicious activity reporting obligations—to certain investment advisers that are registered with the U.S. Securities and Exchange Commission (SEC), as well as those that report to the SEC as exempt reporting advisers.

MISCELLANEOUS UPDATES

1. New CFPB Rule Provides Consumers Greater Control of Personal Financial Data

The Consumer Financial Protection Bureau ("CFPB") issued a final rule in October 2024 that provides consumers greater rights, privacy, and security over their personal financial data[4]. The rule requires financial institutions, credit card issuers, and other financial providers to unlock an individual's personal financial data and transfer it to another provider at the consumer's request for free. In giving consumers more control over their financial data, it will enable:

- The transfer of bank data to another bank, ensuring that much of their banking history can be carried over to another financial institution
- Consumers to comparison shop and move to a competitor for better services or rates
- The secure sharing of payments information by consumers.

[3] https://www.fincen.gov/news/news-releases/fincen-issues-final-rules-safeguard-residential-real-estate-investment-adviser

[4] https://www.consumerfinance.gov/rules-policy/final-rules/required-rulemaking-on-personal-financial-data-rights/

This final rule also strengthens protections for consumers' data such as:

- Banning bait-and-switch data harvesting - as a result, third parties can only collect, use, or retain data to deliver the product the consumer requested. They cannot secretly collect, use, or retain consumers' data for their own unrelated business reasons.
- Creating revocation and deletion rights – as a result, when a consumer revokes access, the rule requires that data access end immediately, and deletion would be the default practice.

Compliance with the rule will be implemented in phases, with larger providers subject to the rule sooner than smaller ones. The largest institutions will have to comply by April 1, 2026, while the smallest covered institutions will have until April 1, 2030. Certain smaller banks and credit unions will not be subject to this rule.

2. FFIEC Sunsets the Use of the Cybersecurity Assessment Tool

The Federal Financial Institutions Examination Council ("FFIEC") recently announced that it has decided not to update the Cybersecurity Assessment Tool ("CAT") to reflect new government resource guidance including the National Institute of Standards and Technology ("NIST") Cybersecurity Framework 2.0 and the Cybersecurity and Infrastructure Security Agency's ("CISA") Cybersecurity Performance Goals. FFIEC will sunset the current CAT on August 31, 2025[5].

CAT has been the industry standard for a decade and now Financial Institutions will need to use other tools to ensure that cybersecurity self-assessments include sufficient and updated coverage to adequately identify risks, control gaps and process enhancements as needed. FFIEC recommends using industry developed resources in conjunction with other resources (e.g., frameworks, standards, guidelines, leading practices) to address continuously evolving cybersecurity risks.

3. FFIEC Issues new IT Examination Booklet

Considering the changing technological environment and increasing need for security and resilience, the FFIEC issued a new "Development, Acquisition, and Maintenance" booklet[6] to help examiners assess information technology practices. Among other things, the booklet discusses the interconnectedness of an entity's assets and processes and those of its third-party service providers along with information to help examiners assess whether management adequately addresses risks and complies with applicable laws and regulations.

For further guidance or assistance contact us at: info@RGSGlobalAdvisors.com

[5] https://www.ffiec.gov/press/an082924.htm
[6] https://ithandbook.ffiec.gov/it-booklets/development-acquisition-and-maintenance/