Author
Sharon Cohen Levin
Partner
WilmerHale

The Convergence of AML and Cybersecurity

Cyber breaches have become an unwelcome staple of our era, from the report that 1 billion Yahoo accounts were hacked to the massive theft of data from the Office of Personnel Management and ongoing threats and breaches at financial institutions, hospitals, technology companies and military contractors.

Financial institutions are particularly attractive targets for cyber attacks, given their massive store of sensitive data accessible on electronic information systems. Cybersecurity has thus emerged as a high priority for financial regulators and the institutions they supervise. During the past year, we have seen the convergence of cybersecurity with another pressing topic in the financial industry: Anti Money Laundering (AML). We expect this convergence to accelerate in 2017.

Financial institutions have traditionally handled cybersecurity and AML compliance separately, with cybersecurity responsible for protecting information systems while AML compliance monitors transactions for indicia of money laundering and terrorist financing. The two groups typically operate with separate personnel and reporting lines. While there are practical reasons for financial institutions to maintain separate cybersecurity and AML units, U.S. regulators have come to expect that financial institutions will take a holistic view of cyber threats and incorporate information about cyber-events and cyber-enabled crimes in Suspicious Activity Reports (SARs) filed pursuant to their Bank Secrecy Act obligations.

In October 2016, the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued an advisory (the "Advisory") addressing a financial institution's suspicious activity reporting obligations related to cybercrime.[1] The Advisory states that even if a cyber-event does not result in a "transaction," a financial institution must still file an SAR if it "knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate or effect a transaction or series of transactions."[2] Under this broad mandate, financial institutions should consider the possibility of filing an SAR after any cyber-event, even if the primary objective does not appear to be the theft of funds. To determine when a cyber-event requires the filing of an SAR, financial institutions must take into account the nature of the event and the information and systems it targeted. In the Advisory and its accompanying set of frequently asked

1 FinCEN, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, FIN-2016-A005 (Oct. 25, 2016), available at https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.
2 Id. at 4.

questions, FinCEN provides detailed guidance on the reporting of cyber-events, cyber-related crimes and cyber-related information.

In the Advisory, FinCEN encourages financial institution cybersecurity units to share information with their AML compliance counterparts. According to FinCEN, such collaboration would "help financial institutions conduct a more comprehensive threat assessment and develop appropriate risk management strategies to identify, report, and mitigate cyber-events and cyber-enabled crime."[3] FinCEN also recommends that financial institutions share cyber-related information among themselves for the purpose of identifying and, where appropriate, reporting potential money laundering or terrorist activities.[4]

In a previous advisory, issued in September 2016, FinCEN warned financial institutions about e-mail compromise fraud schemes in which criminals deceive financial institutions and their customers into transferring funds.[5]

The September advisory noted that this type of cyber-enabled financial crime may trigger a financial institution's suspicious activity reporting requirements under applicable AML regulations. In sum, FinCEN, through these advisories, has set forth the clear expectation that financial institutions will file SARs on cyber-related events and cyber-enabled crime. Failure to do so could result in regulatory scrutiny and possible civil or criminal penalties.

The FinCEN guidance is part of a broader governmental effort to detect and prevent cybercrime. In October 2016, the federal banking regulators issued a joint advance notice of proposed rulemaking concerning cybersecurity regulations and efforts to improve the safety and soundness of the U.S. financial system.[6] State regulatory bodies are also focused on cybercrime and AML, proposing new requirements on the entities they regulate. For example, the New York Department of Financial Services (DFS) has advanced new rules that prescribe minimum criteria for AML and cybersecurity programs and require financial institutions to certify compliance with the standards.

In June 2016, DFS issued a final rule prescribing minimum standards for AML transaction monitoring and filtering programs.[7] The rule, which requires the board or a senior officer of each covered financial institution to certify compliance, went into effect in January 2017. In September 2016, DFS proposed a similar rule with respect to cybersecurity.[8] If issued, the rule would prescribe minimum standards for cybersecurity programs and require the board or a senior officer of each covered financial institution to certify compliance.

Given the regulatory focus on cybersecurity and AML issues, financial institutions need to increase collaboration and communication between their AML compliance and cybersecurity personnel. In particular, financial institutions should ensure that their cybersecurity and AML compliance personnel understand 1) when a cyber-event should be escalated to the attention of AML compliance and 2) the cybersecurity and AML compliance information needed to satisfy emerging reporting requirements from regulators.

3 Id. at 7.
4 To encourage such sharing, Section 314(b) of the USA PATRIOT Act extends a safe harbour from liability to financial institutions that notify FinCEN and satisfy certain other requirements in connection with the information sharing.
5 FinCEN, Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes, FIN-2016-A003 (Sept. 6, 2016), available at https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003.
6 Joint Advance Notice of Proposed Rulemaking, Enhanced Cyber Risk Management Standards (Oct. 19, 2016), available at https://www.federalreserve.gov/newsevents/press/bcreg/bcreg20161019a1.pdf.
7 New York Dept. of Financial Services, Final Rule, Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications (June 30, 2016), available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf.
8 New York Dept. of Financial Services, Proposed Rule, Cybersecurity Requirements for Financial Services Companies (Sept. 13, 2016), available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.