MCINTYRE | LEMON

It's Not Just Gasoline Shortages – A $1.5 Million Reminder that Cybersecurity Policies Are Hand-In-Glove with Anti-Money Laundering Protocols

C. Dirk Peterson
McIntyre & Lemon

I. INTRODUCTION

The hacking of Colonial Pipeline inflicted painful costs in the form of regional gasoline shortages, panic hoarding, price gouging, and a temporary halt in distribution systems. Contemporaneous to the unfolding events surrounding the unauthorized access to Colonial Pipeline's electronic distribution network, the Securities and Exchange Commission ("SEC" or "Commission") issued a much less publicized Cease and Desist and Remedial Order ("SEC Order") against a registered broker-dealer for breakdowns in its anti-money laundering policies in the face of pervasive takeovers of customer securities accounts. [1]

Two key takeaways from the SEC Order, as described in more detail below, are the importance of cybersecurity protocols in a financial institution's AML regime and the Commission's application of a *per se* suspicious activity standard in the face of unauthorized attempts to access customer accounts, thus triggering the filing of Suspicious Activity Reports ("SARs") with the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN").

II. BACKGROUND

A. Bank Secrecy Act and Cyber-Events

For context, the Bank Secrecy Act ("BSA"), first enacted in 1970 and most notably amended in 2001 by Title III the USA PATRIOT Act, is the primary U.S. anti-money laundering law and prophylaxis for deterring, detecting, and disrupting terrorist financing networks. An important tool for fulfilling the BSA's purposes is the requirement of robust AML programs, including reporting and record-keeping regimes, to assist in protecting the nation's financial systems and end users against bad actors.

The requirement of an AML program applies to all "financial institutions," a term expressly defined by the BSA to include broadly, among others, various depository and banking institutions, securities brokers and dealers, investment companies, and insurance companies. [2] Because of the threat of cyber-events and cyber-enabled crimes on consumers and the U.S. financial system, FinCen has periodically reminded financial institutions of their BSA reporting obligations. [3]

---

1 *In the Matter of GWFS Equities, Inc.*, Securities Exchange Act Release No. 91853 (May 12, 2021).

2 *See* 31 U.S.C. §5312(a)(2)(A)-(F) (for banks and other banking institutions), 31 U.S.C. §5312(a)(2)(G)-(H) (for securities brokers and dealers), 31 U.S.C. §5312(a)(2)(I) (for investment companies), and 31 U.S.C. §5312(a)(2)(M) (for insurance companies).

3 *See, e.g.,* FinCen, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime,* FIN-2016-A005 (Oct. 25, 2016) ("FinCen Advisory").

B. The SEC Order

In addition to FinCen, the SEC has focused on cybersecurity issues for many years notably by the creation four years ago of a cyber unit of its Division of Enforcement and the annual emphasis in past years of cybersecurity as an examination priority of its Division of Examinations.[4] The SEC Order at issue applied to the particular context of a securities broker-dealer and its responsibilities pursuant to Rule 17a-8 under the Securities Exchange Act of 1934 ("Exchange Act"), a 1982 SEC rule that requires broker-dealers to comply with the express AML reporting and record-keeping requirements of the BSA. The broker-dealer in this case serviced the retirement investments of 401(k) and 403(b) accounts of retirement plan participants.

Over a three-year period, fraudsters obtained personal identifying information of plan participants in pervasive attempts to obtain access to their retirement accounts. In some instances, fraudsters were successful in directing fraudulent distributions from retirement accounts, some in amounts collectively up to $400,000 in one instance. Notwithstanding apparently robust AML procedures and an internal investigation of each account takeover, the firm inexplicably failed to file SARs on 130 occasions contrary to formal decisions to do so and, in cases where SARs were filed, the firm's submissions in 297 filings were materially incomplete compared to information gleaned from the firm's internal investigations.

The SEC (i) found that these breakdowns in execution of the firm's AML procedures constituted a willful violation of Section 17(a) of the Exchange Act and Rule 17a-8 under the Exchange Act and (ii) entered a fine of $1.5 million against the firm among other remedial measures.

III. ACTION ITEMS AND TAKEAWAYS FOR FINANCIAL INSTITUTIONS

The SEC Order is a reminder to all financial institutions, not just broker-dealers, of the need for dynamic AML programs that evolve to face the challenges of persistent and fraudulent cyber-events. The following are some points from the SEC Order that financial institutions may wish to consider in implementing their AML programs:

- Financial institutions should review no less frequently than annually their AML programs in light of enforcement actions, not only of their functional regulator, but of other regulators having AML regulatory jurisdiction over similarly situated financial institutions, to ensure that their programs sufficiently address up-to-date applications of the BSA and relevant regulations.

- An AML program is only as good as its implementation from start to finish. That is, many financial institutions devote considerable resources to AML oversight and detection, as was the case at hand, but need a system of verification reasonably ensuring their AML programs are executed as directed. In the case at hand, the financial institution did not establish a system to verify that SARs filing directives were in fact executed to completion or that the SARs that were filed contained pertinent information to ensure complete filings.

[4] *See Cybersecurity and Resiliency Observations,* Office of Compliance, Inspections, and Examinations, U.S. Securities and Exchange Commission, at 1. *See also 2021 Examination Priorities,* SEC Division of Examinations.

- In the case of filed SARs, financial institutions should consider multiple levels of content review by those charged with investigating suspicious activities to ensure that content standards are satisfied when compared to information obtained in the course of an internal investigation. As noted by the FinCen Advisory, cyber-criminals typically leave a digital footprint, the proverbial fingerprint as it were, and thus the kind of information a firm should expect to uncover in an investigation and to disclose in a SAR would include: (i) IP address and timestamps, (ii) description and magnitude of the cyber-event, (iii) device identifiers, (iv) methodologies used, and (v) indicators of compromise.[5]

- To ensure a complete investigation and materially complete SAR, collaboration among legal, cybersecurity oversight, AML compliance, and risk management should be standard procedure. A system of collaboration could mitigate against the risk that material information is omitted from an investigation and a required SARs filing.

- Financial institutions should consider risk management that takes into account their exposure in cases where personal identification protections have been breached through no fault of the financial institution. Notably, the SEC Order did not allege that the account takeovers at hand were the result of lax protection of personal identification by the firm. Rather, it appeared that breaches of personal identification protections were with the end user (plan participants). Recognition of this risk exposure should direct firms how to mitigate cyber-events with the potential to adversely affect customer accounts and the timeliness of incident response and resiliency.

- Implicit from the SEC Order is the emphatic declaration that impermissible access and attempts at access to customer accounts are *per se* suspicious and must be reported to FinCen. In practice and as a matter of law, cyber-events that have the effect of misuse or theft of amounts of $5,000 or more in the aggregate require a SARs filing.[6] The FinCen Advisory, on the other hand, does not articulate this obligation emphatically when it advises that a known or suspected cyber-event "should be considered" a suspicious transaction. The SEC Order is reminder that cyber-vents involving impermissible take overs of customer accounts *are* suspicious transactions subject to a SARs filing full stop. With this *per se* standard, firms are able to direct their resources to mitigating weaknesses in their customer protection systems and investigating the five elements of who, what, when, where, and why to assess the level of potential breaches to their customer protection systems and for purposes of completing fulsome SARs.

IV. CONTACT

McIntyre & Lemon, PLLC is a financial services regulatory boutique that advises financial institutions on a variety of regulatory matters, including securities regulatory matters affecting broker-dealers and investment advisers. Do not hesitate to C. Dirk Peterson at dpeterson@mcintyrelf.com or (202) 659-3905, if you have any questions or seek additional information on this Legal Alert or issues raised.

---

5 In short, a five-element test of who? what? when? where? and why? establishes the content standards of a SAR. For example and according to the SEC Order, the firm uncovered significant identifying information about the bad actor impermissibly accessing a plan participant's account, such as routing information to a bank account added to the plan participant's account and certain identifying information of the bad actor as holder of the fraudulently added bank account. Yet, the SAR did not contain this known and materially relevant information. Rather, the content contained generic information from a standard disclosure template, which the SEC found deficient.

6 31 C.F.R. §1023.320 sets forth the SARs filing requirements for broker-dealers. Other financial institutions are subject to similar rules.

MCINTYRE | LEMON

C. Dirk Peterson

OF COUNSEL

202-659-3905

202-296-4202

dpeterson@mcintyrelf.com