CalSurance®

May 2015

Risk Reduction & Loss Prevention

Identity Theft And Cyber Security: What The SEC and FINRA Think You Should Know

By Janene Marasciullo and Carlos Provencio
Wilson Elser

The Internet has forever changed the way we invest. It has led to the proliferation of online brokerage firms, easier account access and more efficient trade execution. However, the increasing use of electronic communications has created an increased risk of cyber crime, such as identity theft, corporate espionage and hacking attacks designed to disrupt businesses and undermine public confidence.

Cyber crime is not new. In 2000, the Securities and Exchange Commission (SEC) promulgated Regulation S-P (Reg S-P) to ensure that broker-dealers complied with privacy obligations set forth in the 1999 Graham Leach Bliley Act (GLB). Since then Congress, state legislatures and regulators have imposed a myriad of obligations on broker-dealers and financial institutions to combat cybercrime and particularly, identity theft. In 2007, the Federal Trade Commission (FTC), along with several other agencies, issued "Identity Theft Red Flags Rules" designed to help financial institutions prevent identity theft and combat money laundering.

Nonetheless, identity theft and cyber crime continues to plague the financial industry and consumers alike. Therefore, when Congress passed the 2010 Dodd-Frank Wall Street Reform Act, it directed the SEC to issue regulations concerning identity theft. The SEC responded in May 2013 by promulgating Reg S-ID, which requires certain financial institutions to adopt a written program to detect, prevent and respond to identity theft (Identify Theft Prevention Program or Program). Reg S-ID largely mimics the FTC's 2007 Identity Theft Red Flag Rules but extends the obligations to a broader spectrum of financial industry participants. After Reg S-ID became effective, FINRA conducted an industrywide examination of cybersecurity practices. In February 2015, FINRA published a 46-page report (FINRA Report), which made detailed recommendations about how to identify, prevent and respond to cyber breaches.

2007 IDENTITY THEFT RED FLAG RULES

↓

2010 DODD-FRANK WALL STREET REFORM ACT

↓

2013 REG S-ID

↓

2015 FINRA REPORT

Although the SEC and FINRA recognize that cyber attacks are inevitable, they have imposed obligations on the financial industry to combat identity theft and cyber crime, and claim these obligations have existed for years. Accordingly, any firm that experiences a cyber intrusion should be prepared to demonstrate that it adopted a written Program and to answer questions regarding its cybersecurity policies or expect disciplinary action and customer complaints. While this obligation may seem daunting, most firms already are taking steps to fulfill these responsibilities.

This article is the first in a two-part series which will summarize the requirements of Reg S-ID and the guidance set forth in the FINRA Report. Part One identifies the types of organizations and individuals who must adopt a written Identity Theft Prevention Program, and the basic elements of a compliant Program. It also

discusses the "red flags" that regulators have identified as signs of cyber breaches and the steps necessary to detect and prevent them. Part Two, which will be published later this summer, will examine the more challenging question of how to respond to identity theft or cyber breaches.

1. Financial Institutions and Creditors: Required Participants

Reg S-ID, which was designed to protect customers' identities, imposes obligations on a broad array of financial service industry participants. Pursuant Reg S-ID, every "financial institution" or "creditor" that holds a "covered account" must adopt a written Identity Theft Prevention Program. The definitions of financial institution and creditor set forth in Reg S-ID are broad. Any bank, credit union or individual who holds a consumer transaction account – an account where the account holder can make withdrawals by negotiable instrument – is a financial institution, and any person who advances funds to or on behalf of a person is a creditor. Thus, all broker-dealers are financial institutions and any broker-dealer that offers margin accounts, securities lending services or short selling services is a creditor. Similarly, any RIA who is required to register under the Investment Advisors Act of 1940 and who allows clients to draw on an account or makes payments on behalf of clients from an account is a financial institution. Likewise, any investment company registered under the Investment Company Act or as a Business Development Company (BDC) is a financial institution. Although only financial institutions or creditors that hold covered accounts need to comply with Reg S-ID, the definition of a "covered account" is also broad. A covered account is any account that is "designed to permit multiple payments or transactions," or "where there is a reasonable foreseeable risk" that identity theft will harm the customers or the soundness of the financial institution or creditor.

Thus, many more financial professionals are subjected to the requirements of Reg S-ID than were subjected to the privacy requirements of Reg S-P and the FTC's Red Flag Rules. The SEC broadened the scope of Reg S-ID to investment advisors who have the ability to direct transfers of funds or make payments on behalf of customers because they "are susceptible to the same types of risks of fraud as other financial institutions."

2. The Elements of An Identity Theft Prevention Program

The SEC has indicated that the prevention of identity theft should be treated as a priority. Reg S-ID requires all financial institutions and creditors ("firms") to adopt a written Identify Theft Prevention Program. In addition, either the board of directors or senior management must approve the Identity Theft Prevention Program and be involved in the administration of the Program.

The SEC has not identified specific actions it expects financial institutions to take in connection with its Program, but has required firms to adopt policies designed to:

1. Identify relevant red flags of identity theft
2. Detect actual red flags of identity theft
3. Respond to red flags of identity theft
4. Ensure that the Identify Theft Prevention Program is updated on a regular basis.

Notably, Reg S-ID allows financial institutions to outsource the development and administration of Identity Theft Prevention Programs to third-party service providers. However, the SEC has clearly stated that the firm "remains legally responsible for compliance with the rules."

Thus, the first element of a compliant Identity Theft Prevention Program is a written plan that has been approved by senior management. However, Reg S-ID allows firms flexibility to determine the content of the Program, based on its "size and complexity" and nature and scope of its activities. Consequently, a program designed for small RIAs with employees and customers in one state would look very different from a program for a national full-service broker-dealer.

3. Understanding the Red Flags of Identity Theft

Appendix A to Reg S-ID identifies five specific signs of identity theft: 1) alerts from credit reporting agencies and fraud detection

services; 2) suspicious documents, particularly those that appear to have been altered or forged; 3) presentation of suspicious personal identification information such as new or incorrect email addresses or physical addresses; 4) unusual or suspicious account activity; and 5) notices from customers or law enforcement. The SEC also has directed firm to consider the type of accounts they offer and the available methods to access them to detect identity theft. The SEC and FINRA have also stated that unusual patterns of access are red flags of identity theft and/or unauthorized cyber intrusions.

Most firms already monitor for these red flags as part of their anti-money laundering (AML) efforts, and hence should incorporate their AML policies into their written Program. Additionally, a firm that is capable of monitoring account activity and access patterns may want to identify suspicious account activity and access as red flags. However, a firm without this capability should not include it as a red flag for fear that regulators and customers could argue the company violated its own procedures.

4. Detecting Red Flags

According to the SEC, firms that were required to comply with the FTC's 2007 Red Flags should already have procedures in place to detect suspicious activity. Notably, Reg S-ID requires firms to obtain information to verify customers' identities at account opening. This obligation is not new to broker-dealers, which have been required to obtain identifying information, including name, social security number, date of birth, address, and picture identification, for some time. Thus Reg S-ID does not impose any new obligations when accounts are opened. However, Reg S-ID advises firms to authenticate customers' identities when transactions are made or upon receipt of a change of address request. The SEC suggests that firms may need to supplement these policies, but made no recommendations.

In contrast, the FINRA Report recommends several steps that its members could take to detect both identity theft and cyber intrusions. Among other things, FINRA Report suggests monitoring the manner in which customers, employees and vendors access accounts and/or data to detect problematic patterns of use. It also recommends that firms set triggers to flag accounts, users or databases for further review. Additionally, the FINRA Report advises firms to adopt access management guidelines which limit access to the firm's accounts, systems and data and immediately terminate access when it is no longer needed. It recommends testing the efficacy of cybersecurity with penetration testing, which entails hiring a computer security company to "hack" the system and provide a report evaluating the cybersecurity. However, a firm must be prepared to address any vulnerabilities identified by the testing and may wish to have counsel oversee the testing and subsequent communications regarding the report are treated as privileged. Finally, FINRA recommends firms consider the National Institute of Standards and Technology (NIST) six-point framework to evaluate vulnerability to cyber attacks, which includes: 1) identifying and documenting asset vulnerabilities; 2) reviewing threat and vulnerability information sharing sources; 3) identifying internal and external threats; 4) identifying potential business impacts; 5) using threat and vulnerability data to determine risk; and 6) prioritizing risk responses.

CONCLUSION

Reg S-ID imposes an additional obligation to adopt a written Identity Theft Prevention Program. However, the content of the Program reflects long-standing requirements to protect customer information. A written Program should be approved by senior management and state that the firm will monitor for the red flags of identity theft and incorporate existing procedures for verifying customer identity when an account is opened, a transaction is executed and an address change is requested. Depending on a firm's business model and capabilities, it may want to adopt some of FINRA's recommendations, which could enhance the institution's cybersecurity. However, firms should not include aspirational capabilities in their Programs because adopting policies which cannot be implemented could create exposure to disciplinary action and serious customer complaints.

About the Authors: Janene Marasciullo is a Partner and Chair of the Securities Litigation Practice at Wilson Elser. Carlos Provencio is Of Counsel to Wilson Elser and is a member of the Securities Litigation Practice.

Stay tuned... for a follow up article in which we will break down the SEC's Reg S-ID requirements for responding to red flags of identity theft and FINRA's recommendations for responding to cyber threats.