SECURITIES EXCHANGE

# CYBERSECURITY RISKS, REGULATION, AND RESOURCES

By: Shane B. Hansen - Partner, Carly Zagaroli - Associate, Paul Bratt - Summer Associate
WARNER NORCROSS & JUDD LLP

**OHIO SECURITIES EXCHANGE**

**Table of Contents**



**DISCLAIMER**

The views and opinions expressed in the Ohio Securities Exchange solely represent those of the contributors. The Ohio Division of Securities takes NO position in the material discussed.

**OHIO SECURITIES EXCHANGE**

The Ohio Securities Exchange provides a platform where views and opinions relating to the securities industry can be shared from sources outside the Division.

The Division encourages members of the securities community to submit articles pertaining to securities law and regulation in the state of Ohio.

If you are interested in submitting an article, please contact the Editor-In-Chief,

Kyle Evans
Kyle.Evans@com.state.oh.us

## OVERVIEW

Those convenient 'clouds' of electronically stored or accessed data and personal information also contain 'lightning' that can strike unprepared investment firms and their clients. Criminal enterprises behind these attacks have become more sophisticated and often involve domestic or foreign organized crime syndicates, foreign nationals and even foreign governments—no longer just techno-geeks and petty thieves.

A 2014 pilot survey by state securities regulators[1] found that 4.1% of state-registered investment advisers had experienced a cybersecurity incident and 1.1% had experienced theft, loss, or unauthorized exposure or misuse of confidential information. Cybersecurity experts (including cybersecurity consulting firms marketing their services) believe the "hit rate" is likely higher. With the U.S. government,[2] the Securities and Exchange Commission (SEC),[3] the North American Securities Administrators Association (NASAA),[4] the Financial Industry Regulatory Authority (FINRA),[5] and news media sounding sirens of cyber threats, do not be caught unawares sleeping under a tree when the lightning strikes at your firm and your clients.

## CONNECTIVITY IS CONVENIENT BUT RISKY

Today you need more than gates, guards, and guns to prevent criminals from getting away with the firm's and client's identities or cash. Email, computers, laptops, tablets, internet-based information access or storage, smartphones, internet-connected hardware and related software, flash drives, wireless communications—all the modern conveniences—create ample opportunity for a tech-savvy intruder to monitor, gain access to, and misappropriate confidential information. Smartphone applications like "Swipe" and "Swift Key" include seemingly helpful features that "learn" and adapt to your (bad) typing habits by tracking your every key entry on their remote file servers—convenient, yes, but the person with access to that remote file server can potentially see every password and ID you type. Frequently, hi-tech platforms and data aggregators gather, store, and allow access to both clients' and the firm's own confidential personal information. Access to client information and emails can later be translated into highly convincing identity theft schemes. The days of physical computer tapes, CDs, DVDs, and manual data backups are largely gone—replaced by more reliable third-party "cloud" servers and systems. However, today's remarkable connectivity and convenience through networks, the internet, and the digital cloud create cyber vulnerabilities.

Firms are susceptible to various kinds of cyber threats, some more serious than others. Unencrypted laptops, tablets, smart phones, and similar devices are easy targets if lost or mislaid, particularly if not password-protected. Unencrypted email is easily intercepted, especially when email addresses are stolen from other sources, such as big

*(Continued on page 14)*

[1] North American Securities Administrators Association, Compilation of Results of a Pilot Survey of Cybersecurity Practices of Small and Mid-Sized Investment Adviser Firms (September 2014), http://www.nasaa.org/wp-content/uploads/2014/09/Cybersecurity-Report.pdf ("NASAA Survey").
[2] U.S. Computer Emergency Readiness Team ("US-CERT"), National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security, https://www.us-cert.gov/about-us.
[3] Cybersecurity Risk Alert, SEC, http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
[4] NASAA Survey Finds Mid-Sized IAs Addressing Cybersecurity Risks, NASAA, http://www.nasaa.org/32570/nasaa-survey-finds-mid-sized-ias-addressing-cybersecurity-risks/.
[5] Customer Information Protection, FINRA, http://www.finra.org/Industry/Issues/CustomerInformationProtection/.

**SHANE B. HANSEN** is a partner and co-chairs the Funds and Investment Services Practice in the law firm of Warner Norcross & Judd LLP. His law practice concentrates in the area of financial services regulation, primarily involving federal and state securities and banking laws and related rules.

Mr. Hansen serves as the lead counsel and primary draftsman of H.R. 2274, the *Small Business Mergers, Acquisitions, and Sales Brokerage Simplification Act of 2013*. Mr. Hansen is a member of the Business Law Section Council, State Bar of Michigan (2014-present) and is a long-time active member of both the Section's Securities and Financial Institutions Committees. He is the immediate past chair of the Committee on State Regulation of Securities in the Business Law Section of the American Bar Association (2011-2014). He co-chairs its Subcommittee of Liaisons to Securities Administrators in the U.S. and Canada (2007-present). He is also an active member of the ABA's Committee on Federal Securities Regulation. Mr. Hansen graduated with honors from the University of Michigan Law School in 1982. He graduated with high honors from Albion College in 1979.

*(Continued from page 13)*

box retailers. How often have you forgotten your password to personally access a website and simply clicked to have it emailed to you—are *you* the *only* person receiving it? Many consumer-grade file-sharing websites and systems are not designed with strong cybersecurity protections. These file-sharing systems may be simple and cheap—great for personal photo sharing—but may not be suitable for the type of confidential personal, financial, and business data transmitted and stored by financial services firms.

Malware, digital worms, and key-logging software are commonly spread through e-mail, spurious applications and program updates, Trojan horse file attachments, and visiting infected websites. Phishing emails continue to be a common attack strategy. There are cyber threats to the computer operating systems you use to conduct daily business—not just your own systems, but also third-party systems and websites you rely upon to serve your clients. A "botnet"—short for robot network—is an accumulation of compromised computers (called "zombies") manipulated by a central computer or "controller." Botnets have the ability to overload webservers, to steal data, and may be difficult to detect. Distributed denial of service (DDoS) attacks can stall business operations for hours or even longer—your website or third-party websites you rely upon to monitor portfolios or enter trades. These attacks have been used to extort "ransom" from the web host in exchange for resumed operations. In the meantime, you may be unable to access or use the website.

## CYBER-RELATED REGULATIONS

Assessing and planning for cybersecurity risks has become a high regulatory priority. On September 15, 2015, the SEC Office of Compliance Inspections and Examinations ("OCIE") issued a release, *Cybersecurity Examination Initiative*, summarizing its examination priorities, which will involve more testing to assess implementation of firm procedures and controls.[6] OCIE's focus will include: governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response. The release includes a sample of OCIE's requests for information and documents.

## PRIVACY AND SAFEGUARDING RULES

Important privacy regulations derive from the Financial Services Modernization Act of 1999, more commonly called the Gramm-Leach-Bliley (GLB) Act.[7] The GLB Act directed the SEC,[8] the Federal Trade Commission (FTC),[9] and the federal bank regulatory agencies to adopt consumer privacy regulations. The FTC does not examine state-registered investment advisers, but may respond to client complaints and referrals from state securities regulators.

SEC Regulation S-P, *Privacy of Consumer Financial Information*, applies to SEC-registered broker-dealers and investment advisers. Regulation S-P implemented sections of the GLB Act and the Fair Credit Reporting Act (FCRA) for entities registered with and regulated by the SEC. SEC Rule 30 (Safeguarding Rule) requires registrants to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information."

State-registered investment advisers are covered by the FTC's *Privacy of Consumer Financial Information* rule. The

*(Continued on page 15)*

[6]Available at: http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. See also FINRA Targeted Examination Letters-Cybersecurity, http://www.finra.org/industry/regulation/guidance/targetedexaminationletters/p443219.

[7]Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999), 15 U.S.C. § 6801, *et seq*.

[8]SEC Regulation S-P, Privacy of Consumer Financial Information, 17 C.F.R. § 248 (2000).

[9]FTC, Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, 67 FR 36493 (2002).

(Continued from page 14)

FTC's rule is more rigorous than the SEC's Regulation S-P. Notably, it requires state-registered firms to "develop, implement, and maintain a *comprehensive information security program* that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."

## SEC – CFTC IDENTITY THEFT RED FLAGS RULES

As the name implies, the federal identity theft rules direct covered firms to take steps to prevent losses caused by identity theft through unauthorized account orders or access, including impersonations. The SEC and the Commodities Futures Trading Commission (CFTC) jointly adopted rules implementing identity theft red flags and guidelines under the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended the Fair Credit Reporting Act (FCRA). The SEC's version is Regulation S-ID, Section 248.201, and the CFTC's version is Subpart C, Section 162.30, both titled *Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft* (Red Flags Rules). The SEC-CFTC Red Flags Rules apply to SEC and CFTC registrants; the FTC's Red Flags Rule applies to state-registered investment advisers.

Generally, the Red Flags Rules require a covered financial institution to develop, implement, and administer a written identity theft prevention program. The program's purpose is to detect, prevent and mitigate identity theft in connection with the direct or indirect opening or maintenance of a covered account.[10]

**CARLY A. ZAGAROLI** joined Warner Norcross & Judd LLP's Grand Rapids, Michigan office in September 2014. She received her law degree from the Michigan State University College of Law summa cum laude where she was a King Scholar. She also holds a bachelor of arts magna cum laude in sociology from Saint Mary's College in Indiana. Zagaroli has served as an extern in the 17th Circuit Court for the Hon. G. Patrick Hillary and the Hon. George J. Quist.

Paul Bratt interned as a Summer Associate in Warner Norcross & Judd LLP's Grand Rapids, Michigan office during the Summer of 2015. Paul is currently enrolled at the University of Michigan Law School.

## FINRA CYBERSECURITY RULES AND GUIDANCE

FINRA's website provides cybersecurity guidance and resources for brokerage firms.[11] FINRA has provided guidance about cybersecurity issues, including risks related to wireless fidelity (Wi-Fi) and remote access networks.[12] Accordingly, a broker-dealer's written supervisory and control procedures must address compliance with the SEC's Safeguarding and Red Flags Rules under FINRA Rules 3110, 3120, and 3130.

Cybersecurity and identity theft prevention measures intersect in FINRA Rule 3110(c)(2). This rule requires brokerage firms to have policies and procedures to address safeguarding customer funds and securities; transmittals of funds (e.g., wires or checks, etc.) or securities from customers to third party accounts; from customer accounts to outside entities (e.g., banks, investment companies, etc.); from customer accounts to locations other than a customer's primary residence (e.g., post office box, in care of accounts, alternate address, etc.); and between customers and registered representatives, including the hand-delivery of checks. Policies and procedures must also build controls around changes of customer account information, including address and investment objectives changes and validation of such changes. These are among the leading circumstances surrounding identity theft losses.[13]

## STATE BREACH NOTIFICATION LAWS

Forty-seven states require security breach notifications.[14] Firms must report identified data breaches to all affected customers and, typically, to government authorities. Requirements do vary significantly by state and are not preempted by federal law. Twenty-nine of those laws contain exceptions or safe harbors for firms that are subject to, and/or comply with federal privacy laws and related rules promulgated by their federal regulator. However, the SEC has not adopted breach notification requirements, so its rules likely do not preempt state laws. Forty-seven states have also enacted "security freeze" laws that allow customers to

(Continued on page 16)

[10]See also Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business, FTC, May 2013, http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business.
[11]FINRA Customer Information Protection, http://www.finra.org/Industry/Issues/CustomerInformationProtection/; Firm Identity Theft, http://www.finra.org/Industry/Issues/CustomerInformationProtection/p117442.
[12]NASD Notice to Members 05-49, Safeguarding Confidential Customer Information (2005), http://www.nasd.com/web/groups/rules_regs/documents/notice_to_members/nasdw_014772.pdf.
[13]The FINRA report is available at http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.
[14]See National Conference of State Legislatures website for a list of states at: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

*(Continued from page 15)*

freeze their credit reports in the event of a security breach. The national credit reporting agencies charge for security freezes, likely an expense of the firm whose cybersecurity was breached. Firms with clients in multiple states will be subject to multiple state laws with differing reporting obligations.

## BUSINESS CONTINUITY PLANNING AND DISASTER PREPAREDNESS

Cyber-attacks on a firm or on a third-party vendor upon which the firm relies can have a devastating impact on normal operations and should therefore be among the risks addressed in business continuity and disaster recovery planning. For example, ransomware is a flavor of malware restricting access to the computer system that it infects. The infection is then accompanied by extortionate demands for access to be restored. Ransomware may encrypt files on the computer's hard drive, lock up the system, or simply threaten data erasure if the ransom is not promptly paid. Denial of service attacks are another form of business interruption. Cybersecurity risks intersect with recordkeeping requirements when books and records are stored or archived in the cloud. Specifically, if records are stored in electronic form it must be protected from alteration, loss, or destruction.[15]

## CYBERSECURITY RESOURCES AND PLANNING

Commonly cited by cyber-industry experts, the National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, released the first version of the *Framework for Improving Critical Infrastructure Cybersecurity* on February 12, 2014 (Framework).[16] The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework is industry neutral, and therefore relevant to all types of businesses. The NIST's Computer Security Division published NISTIR 7621, *Small Business Information Security: The Fundamentals*, to help small businesses and small organizations implement the fundamental components of an effective information security program.

In addition, the Securities Industry and Financial Markets Association (SIFMA) published useful *Guidance for Small Firms*,[17] including a *Small Firm Cybersecurity Checklist*. These resources are useful to all business models, not just broker-dealers. These resources will aid in your development of a firm-specific approach to cybersecurity risks as you develop policies, procedures, and a program to safeguard your clients' and firm's information.

So, how to get started? Each firm's circumstances will be different, so each cybersecurity risk assessment and each program will be different, but here are some basic suggestions:

**Muster an internal team**. Its members should include IT, operations, compliance, and front-line and back-office representatives. Involve senior management. Identify gaps in expertise—likely technology—and engage outside support. Keep records of the team's composition, meetings, and related activities.

**Develop written cybersecurity and identity theft game plans**. Written records are critical in demonstrating your team's efforts to regulators and courts. Set and update written priorities and progress reports.

**The Red Flags Rules include specific guidance with helpful content**. FINRA created a template designed to help small firms develop and document their "red flags" program.

**Start with the basics**. Identify the technology you are using to remotely connect to email and client information, including technology allowing clients' remote access and assess its vulnerabilities—think about all office, home, and mobile devices. Install and update antivirus software, implement passwords and user IDs.

**Revisit your plan periodically and when prompted by changes**. When employees, representatives, and third-party vendors change, change log-ins and user access rights. New offices, new employees and representatives, new services, new vendors, and new technologies should trigger a reassessment of related cybersecurity risks.

**Password management**. Require and train all employees and representatives to use and periodically change passwords and user IDs on all electronic devices (e.g., computers, tablets, and other mobile devices).

**Antivirus Software, Patches, and Encryption**. Install and update antivirus software on all electronic devices. Check for application updates and promptly install security patches. Install encryption software on files, emails, and mobile electronic devices.

**Vendors**. Do your due diligence before contracting with cloud service providers. Beware of free cloud services for data storage, back-up, and file sharing.

**Train and Educate**. Train employees and representatives, and educate clients, on common cybersecurity risks and defensive strategies.

[15]For SEC-registered investment advisers, see Rule 204-2(g), 17 C.F.R. 275.204-3; state law imposes similar requirements on state-registered investment advisers. For broker-dealers, see SEC Rules 17a-3 and 17a-4, 17 C.F.R. 240.17a-3 *et seq*.

[16]Nat'l Inst. of Standards and Tech., Framework for Improving Critical Infrastructure Cybersecurity (February 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[17]Available at http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/.