# Cybersecurity Risks, Regulation, and Resources

**By: Shane B. Hansen, Partner**
**Carly Zagaroli, Associate**
**Paul Bratt, Summer Associate**
**Warner Norcross & Judd LLP**

**September 22, 2015**

## 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.

The lucrative black market of "phish mongers" in illegally stolen cyber data from "mass attacks" such as reported by J.P. Morgan Chase,[1] Home Depot, Target, and the U.S. Office of Personnel Management[2] feeds the criminal activities of identity thieves around the globe. Enterprising criminals buy and then use the stolen cyber data to prey upon other targets, such as smaller, "softer" financial services firms through unauthorized account access and client impersonations. Key areas of cyber vulnerability include remote access to client information, remote customer access to accounts, fund transfer requests, risks associated with third-party vendors, and detection of unauthorized activity. Some cyber-criminals have recognized credit monitoring service contracts purchased for victims are often one year in length, so they wait to exploit their inventory of identities until later.

A 2014 pilot survey by state securities regulators[3] 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.[4] With the U.S. government,[5] the Securities and Exchange Commission (SEC),[6] the North

[1] *JPMorgan Chase Hacking Affects 76 Million Households*, New York Times, October 2, 2014, http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0.
[2] For a summary of the OPM's breach see https://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/.
[3] 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).
[4] E.g., *Financial Advisors Cybersecurity Risks: Aponix Financial Technologists Comments on NASAA Survey*, http://finance.yahoo.com/news/financial-advisors-cybersecurity-risks-aponix-174134026.html; Megan Leonhardt, *Cybersecurity Breaches Not Rare, Just Undetected* (September 11, 2014), http://wealthmanagement.com/technology/cybersecurity-breaches-not-rare-just-undetected.

American Securities Administrators Association (NASAA),[7] the Financial Industry Regulatory Authority (FINRA),[8] 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.

In 2014 there were a reported 79,790 security breach incidents affecting more than 700 million account records.[9] Cybersecurity spending worldwide is near $70 billion, and increases 10 to 15 percent every year, but attackers nevertheless manage to stay ahead of the curve.[10] Local small businesses are increasingly being targeted,[11] but the attackers are not afraid to go after the big fish as well, such as the now infamous identity theft scheme against the Internal Revenue Service. Using previously acquired personal information, identity thieves were able to acquire past tax returns of over 100,000 U.S. taxpayers from the IRS's website, including names, addresses, and social security numbers. Thieves proceeded to file approximately 13,000 fraudulent returns by utilizing private data from the previous returns, acquiring $39 million in fraudulent refunds. Although this pales in comparison to the aggregate total $5.9 billion in fraudulent returns this year, the fact that private data was stolen from the IRS' website is highly disconcerting.[12]

Cybersecurity threats intersect legal and regulatory requirements applicable to investment firms at several critical points, including: common law fiduciary duties to protect clients' assets, federal and comparable state consumer privacy and data safeguarding rules, identify theft "red flags" rules, compliance programs, business continuity planning, books and records, state data breach notification laws, and even preventing insider trading.[13] These risks can also intersect your wallet if unauthorized access to clients' accounts or identity theft results in client losses. Civil claims may follow with the inevitable finger-pointing. Third-party vendors typically have limitations of liability and pockets much deeper than a small firm's ability to defend itself.[14]

---

[5] 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.

[6] Cybersecurity Risk Alert, SEC, http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf; see also the SEC's 2014 examination priorities letter, http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf .

[7] *NASAA Survey Finds Mid-Sized IAs Addressing Cybersecurity Risks*, NASAA, http://www.nasaa.org/32570/nasaa-survey-finds-mid-sized-ias-addressing-cybersecurity-risks/.

[8] *Customer Information Protection*, FINRA, http://www.finra.org/Industry/Issues/CustomerInformationProtection/.

[9] *See Verizon 2015 Data Breach Investigations Report* (2015), http://www.verizonenterprise.com/DBIR/2015/; see also *Symantec Internet Security Report* (2015), https://know.elq.symantec.com/LP=1542.

[10] *Cybersecurity fears grow as defenses boosted: study*. Business Insider, June 10, 2015, http://www.businessinsider.com/afp-cybersecurity-fears-grow-as-defenses-boosted-study-2015-6 .

[11] *Hackers Go After Little Fish, Too, While Trawling for Credit Cards*, N.Y. Times, June 11, 2015, http://www.nytimes.com/2015/06/11/business/dealbook/when-it-comes-to-hackers-big-and-small-will-do.html?ref=business.

[12] *IRS Statement on the "Get Transcript" Application*, June, 2, 2015, at: http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application. S*ee IRS Agrees to Give Identity-Theft Victims Copies of Fake Returns*, Bloomberg Business, June 2, 2015, http://www.bloomberg.com/news/articles/2015-06-02/irs-agrees-to-give-identity-theft-victims-copies-of-fake-returns.

[13] *Wells Fargo arm fined $5 million over broker's insider trading*, Washington Post, September 22, 2014, http://www.washingtonpost.com/business/economy/wells-fargo-arm-fined-5-million-over-brokers-insider-trading/2014/09/22/030ddb68-4274-11e4-9a15-137aa0153527_story.html .

[14] See *What Banks Should Know About the Eighth Circuit's Decision in Choice Escrow & Land Title, LLC v. Bancorpsouth Bank*, Lori A. Desjardins, Katie Hawkins, ABA Business Law Today, October 2014, http://www.americanbar.org/content/aba/publications/blt/2014/10/02_desjardins.html , and the cases discussed.

When a criminal theft occurs, "obviously" *somebody* besides the criminal must have been at fault—perhaps even the client's own carelessness with passwords, log-ons, and email accounts.[15] Even if you are ultimately vindicated in litigation or arbitration, defense costs can run into the tens of thousands of dollars, cause years of personal stress, and result in the loss of clients' trust and confidence. There may also be regulatory investigations and enforcement.[16] Remorse for failing to take appropriate steps will not prevent potential financial ruin.

Today's electronic technology is at the core of virtually every business activity and process. We depend upon technology because it is convenient, time-saving, and cost-effective. Key questions to consider include: where is your client data, how did it get there, and what ways can you or anyone else access it? Desktop computers, laptops, tablets, mobile phones, file servers, cloud servers, routers, websites, and the technology that connects or transfers data between them—telephone lines, cables, bluetooth and wireless connectivity, satellite feeds, USB ports, flash drives, DVDs, and CDs—are all potential points of cybersecurity vulnerability. Many of these access points are beyond the four walls of your office—including home computers, current and former representatives and employees,[17] account custodians, account and portfolio management services and platforms, data aggregators, internet service providers, data transmission providers, email platforms and archivers, third-party technology consultants and vendors, and ultimately your clients' homes, offices, and hands. Lest we not forget, people and paper still carry and convey data too, but the risks associated with physical data breaches are better known and generally well-protected by locks, keys, and "clean desk" policies.

Even the best planned technology defenses are not invulnerable,[18] but it is incumbent on everyone to understand cybersecurity risks and regulation in order to become better prepared. Cyber risk management begins in your office, but should include client education too. Many resources are available to get you started, but you will inevitably need more technological expertise. You simply don't know what you don't know.

**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 clients' 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

---

[15] *Leaks of nude celebrity photos raise concerns about security of the cloud*, Washington Post, http://www.washingtonpost.com/politics/leaks-of-nude-celebrity-photos-raise-concerns-about-security-of-the-cloud/2014/09/01/59dcd37e-3219-11e4-8f02-03c644b2d7d0_story.html.

[16] *SEC Charges Brokerage Executives With Failing to Protect Confidential Customer Information*, April 27, 2011, http://www.sec.gov/news/press/2011/2011-86.htm.

[17] *Balancing Client Privacy and Client Service—Regulation S-P Applied to Recruiting Representatives*, Shane B. Hansen, NSCP Currents, http://wnj.com/Publications/Balancing-Client-Privacy-and-Client-Service-Regula.

[18] Feeling overwhelmed? Take a break watching the movie thriller, *Firewall* (2006), starring Harrison Ford, summarized at: http://en.wikipedia.org/wiki/Firewall_(film).

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, DVD, and manual data back-ups 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 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[19] 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.[20]

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.[21] Phishing emails continue to be a common attack strategy.[22] 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. FINRA recently issued an Information Notice to member firms about these attached.[23] 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.[24]

---

[19] See, for example, articles about Dropbox or Google Drive; see also, *Be My Host: What to ask about free services that may be hosting your data*, Inside Counsel, May 23, 2014, http://www.insidecounsel.com/2014/05/23/be-my-host-what-to-ask-about-free-services-that-ma.

[20] See Landa Heinan, *How to share corporate files without compromising your company (or your job)*, St. Louis Bus. J. (2014), http://www.bizjournals.com/bizjournals/how-to/technology/2014/07/how-to-share-corporate-files-without-compromising.html.

[21] William F. Pelgrin, *Why Cybersecurity is Important*, Cybersecurity Tips Newsletter, Vol. 5, Issue 10 (2010), http://msisac.cisecurity.org/newsletters/2010-10.cfm.

[22] The Target security breach may have started with an employee opening a phishing email. S *ee* Samantha Sharf, *What it Means for Home Depot if data breach is Larger than Target's*, Forbes (September 2014) available at http://www.forbes.com/sites/samanthasharf/2014/09/03/what-it-means-for-home-depot-if-data-breach-is-larger-than-targets/.

[23] See FINRA, Information Notice, *Distributed Denial of Service*, issued on June 19, 2015; for an explanation of DDoS attacks, *see* Margaret Rouse, *Distributed Denial-of-Service Attack* (DDoS), http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

[24] Jay McGregor, *Feedly and Evernote Go Down as Attackers Demand Ransom*, Forbes (June 11, 2014), http://www.forbes.com/sites/jaymcgregor/2014/06/11/feedly-and-evernote-go-down-as-attackers-demand-ransom/.

**Customize Your Cyber-protection Program**

Because threats come in all shapes and sizes and not all businesses use the same technology, there is no "one size fits all" strategy to defend against potential attacks. Firms must identify and assess their own cyber risks and develop a game plan to address and manage those risks. Small firms are not immune from various sorts of cyber-attacks or identity theft schemes and scams.[25] A widely held belief is that attackers are only out to get the "big fish"—obviously a logical source for mass quantities of personally identifiable information—but smaller firms are easy targets for remotely converting stolen identities into cash through the convenience of a computer and the internet—no guns or getaway car required.

There appears to be a significant gap between small firms' technology use and their defensive cybersecurity measures. The NASAA Survey found that 92% of state-registered investment advisers use email or other electronic messaging to contact clients and 85% use computers, tablets, smartphones, or other electronic devices to access client information. However, less than 50% of small firms reported having any cybersecurity policies and procedures or training in place. These technologies all pose potential vulnerabilities.

Most small firms have limited financial and staffing resources to devote towards cybersecurity initiatives are inherently limited,[26] even though the associated risks are largely unlimited. Resource allocation decision-making should consider the potential civil liabilities and regulatory penalties that could result from cybersecurity breaches. Mid-size and larger firms have greater resources but also greater risks because of having more confidential information, more representatives and employees, more third-party technology products and vendors, all posing potential cyber risks. Large companies like J.P. Morgan Chase, Home Depot, and Target present the biggest targets to acquire mass quantities of personal information, even if no cash is stolen in the attack.[27] As discussed below, all firms, regardless of size, are subject to data breach notification laws. These laws generally require prompt government and client notifications.[28] Compliance with these laws can be tremendously expensive, especially when there are affected clients in multiple states.[29]

Firms may underestimate cyber risks by believing that third-party technology providers are responsible for data protection oversight.[30] However, there are risks and responsibilities associated with outsourcing control and protection of client information. Firms are not relieved from their continuing obligation to comply with applicable laws, even when compliance is

---

[25] Symantec's *Internet Security Threat Report* (2014) reported businesses with less than 250 employees accounted for 30% (2013), 31% (2012), and 18% (2011) of all cyber-attacks, p. 30, http://www.symantec.com/security_response/publications/threatreport.jsp.

[26] Richard Kissel, *Small Business Information Security: The Fundamentals*, NISTIR 7621 (October 2009), http://www.nist.gov/itl/csd/kissel-rich.cfm.

[27] For an in-depth explanation of the Target and Home Depot security breaches, *see* Samantha Sharf, *What it Means for Home Depot if data breach is Larger than Target's*, Forbes (September 2014), http://www.forbes.com/sites/samanthasharf/2014/09/03/what-it-means-for-home-depot-if-data-breach-is-larger-than-targets/.

[28] *See e.g.*, Cal. Civ. Code §§ 1798.80-1798.84 (2007). California was the first state to address reporting issues.

[29] Kissel, *supra* note 11 ("If you have 1000 customers whose data might have been compromised in an incident, then your minimum cost would be $130,000").

[30] *See* FINRA Notice No. 11-14, *Third Party Service Providers* (2011).

outsourced.[31] Firms need to understand how third-party providers will handle their confidential information and confirm that there are contractual provisions to protect the firm's confidential information.[32] After a cyber-breach or fraudulent asset transfer, the finger-pointing starts and those contractual responsibilities and third-party liability limitations become critically important.

**Cyber-related Regulations**

Assessing and planning for cybersecurity risks has become a high regulatory priority among securities regulators. On September 15, 2015 the SEC Office of Compliance Inspections and Examinations (OCIE) issued a release, *Cybersecurity Examination Initiative*, summarizing its past examination priorities and highlighting OCIE's second round of cybersecurity examinations, which will involve more testing to assess implementation of firm procedures and controls.[33] 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.

OCIE's examination findings cover a range of cybersecurity issues for broker-dealers and investment advisers. For example, OCIE found that a vast majority of broker-dealers and investment advisers have written security policies and conduct periodic risk assessments, certainly a good sign for the industry. Almost all have some form of encryption in place. Most have experienced a cyber-attack, whether directly or indirectly through vendors, around half of which have been fraudulent emails impersonating clients. Over a quarter of broker-dealers reported losses of more than $5,000 from fraudulent emails. A majority reported these emails to the Financial Crimes Enforcement Network[34], but only 7 percent reported the emails to law enforcement or regulatory agencies.[35] Drawing in part from the OCIE's findings, the SEC released a guidance document, which recommends, in short, that firms periodically assess their information and data security, as well as particular threats and vulnerabilities, to create a written strategy to prevent, detect, and respond to threats, and to implement the strategy with appropriate policies, training, and education.[36] While not binding on state-registered investment advisers, the SEC's guidance will nonetheless be instructive as industry best practices evolve and a standard of care develops. NASAA is in the process of developing cybersecurity guidance to state-regulated firms.[37]

---

[31] *See* National Association of Securities Dealers (NASD), Notice to Members 05-48, *Outsourcing: Members' Responsibilities When Outsourcing* (2005).

[32] For more information on the risks associated with outsourcing, see Macdonnell Ulsch, *Third-party risk management: Horror stories? You are not alone*, Techtarget (2014), http://searchsecurity.techtarget.com/feature/Third-party-risk-management-Horror-stories-You-are-not-alone .

[33] Available on the SEC website at: http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. *See also* OCIE, National Exam Program Vol. IV, Issue 2, *OCIE Cybersecurity Initiative* (April 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf ; and SEC Cybersecurity Roundtable, March 26, 2014, http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml . *See also* FINRA Targeted Examination Letters-Cybersecurity, http://www.finra.org/industry/regulation/guidance/targetedexaminationletters/p443219 .

[34] *See* FinCEN's website at: http://www.fincen.gov/.

[35] The OCIE exam sweep summary is available at https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf .

[36] The SEC's guidance is available at http://www.sec.gov/investment/im-guidance-2015-02.pdf .

[37] Visit NASAA's website for updates at: http://www.nasaa.org/.

The SEC and FINRA have brought enforcement cases against firms for cybersecurity-related compliance failures.[38] Firms have been cited for inadequate written policies and procedures, failing to enforce such policies and procedures, failing to conduct periodic self-assessments of cybersecurity-related procedures, and failing to respond to self-identified deficiencies. For example, on September 22, 2015, the SEC issued a press release announcing the settlement of an enforcement action against R.T. Jones Capital Equities Management, Inc. The SEC alleged that the firm failed to adopt any written policies and procedures to ensure the security and confidentiality of personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients, and protect it from anticipated threats or unauthorized access.[39] According to the SEC's order the firm's web server was attacked in July 2013 by an unknown hacker who gained access and copy rights to the data on the server. No indications of a client suffering financial harm as a result of the cyber-attack were yet reported. The SEC's order finds that R.T. Jones violated Rule 30(a) of Regulation S-P under the Securities Act of 1933. Without admitting or denying the findings, the firm agreed to cease and desist from committing or causing any future violations of Rule 30(a) of Regulation S-P and agreed to be censured and pay a $75,000 penalty. Concurrently, the SEC issued an *Investor Alert: Identity Theft, Data Breaches and Your Investment Accounts.*[40]

Other enforcement actions have resulted in hefty fines from $100,000 to $450,000.[41] Among other things, FINRA rules require specific policies and procedures, as well as related testing and verification, to defend against identity theft.[42] Besides examinations, SEC and FINRA attention may be prompted by customer complaints about identity theft-related losses. Publicly announced regulatory settlements with firms commonly prompt plaintiffs' attorneys to advertise on the internet for affected clients to assert claims.

The SEC and FINRA are both actively examining for compliance with electronic communications, recordkeeping, and related rules and guidance.[43] These rules include consumer privacy and data safeguarding, identity theft "red flags" rules, compliance programs, and business continuity and disaster preparedness planning.[44] In addition, most states have enacted data breach notification and security "freeze" laws, which are enforceable by state authorities and are likely providing affected clients with civil remedies. These laws impose significant breach-response requirements and related costs upon the unlucky firms targeted by cyber thieves.

---

[38] Dave Michaels, *Hacked Companies Face SEC Scrutiny over Disclosure*, Bloomberg (2014), http://www.bloomberg.com/news/2014-07-02/hacked-companies-face-sec-scrutiny-over-disclosure.html .
[39] The SEC's press release and order are available at: http://www.sec.gov/news/pressrelease/2015-202.html.
[40] Available on the SEC's website at: http://www.sec.gov/oiea/investor-alerts-bulletins/ia_databreaches.html.
[41] Sutherland, *Legal Alert: Cybersecurity Issues in the Financial Services Industry: Fasten Your Cyber Belts, It's Going to be a Bumpy Night* (April 2014), http://www.sutherland.com/NewsCommentary/Legal-Alerts/162857/Legal-Alert-Cybersecurity-Issues-in-the-Financial-Services-Industry-Fasten-your-cyber-belts-its-going-to-be-a-bumpy-night.
[42] See FINRA Rule 3110(c) and its predecessor NASD Rule 3012(a)(2)(B); see also Regulatory Notice 09-64, *Customer Assets: Verification of Instructions to Transmit or Withdraw Assets from Customer Accounts*.
[43] See also SEC Rel. No. 33-7288, *Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information* (May 1996), http://www.sec.gov/rules/concept/33-7288.txt.
[44] SEC Release Nos. IA-2204, IC-26299, *Final Rules on Investment Adviser Compliance Programs*, http://www.sec.gov/rules/final/ia-2204.htm.

**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.[45] The GLB Act directed the SEC,[46] the Federal Trade Commission (FTC),[47] and the federal bank regulatory agencies to adopt consumer privacy regulations. The SEC's and FTC's privacy regulations are similar but not identical, as explained below. For firms switching between SEC and state-registration, it is noteworthy that the FTC has said "the [FTC] does not intend to impose undue burdens on entities that already are subject to comparable safeguards requirements." The FTC does not examine state-registered investment advisers, but may respond to client complaints and referrals from state securities regulators.

Sections 501 and 502 of the GLB Act regulate what firms can do with nonpublic personal information about consumers and customers; generally, these requirements do not apply to corporate or business clients. Section 501 of the Act requires that financial institutions protect confidential personal information by establishing "appropriate standards . . . relating to *administrative, technical, and physical safeguards.*" The safeguards must be designed to "ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; ***and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer***." The GLB Act also prohibits a financial institution from disclosing confidential information to nonaffiliated third parties, unless the institution satisfies certain notice and opt-out requirements. Firms must also adopt and deliver privacy notices describing their handling and use of nonpublic personal information.[48] Privacy notices require statements summarizing the measures taken to safeguard clients' nonpublic personal information—when, in fact, no safeguards have been adopted these statements could be a material misrepresentation.

SEC Regulation S-P, *Privacy of Consumer Financial Information*, applies to SEC-registered broker-dealers and investment advisers.[49] 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". The rule prescribes that these written policies and procedures be "reasonably designed" to:

- Insure the security and confidentiality of customer records and information;

- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

[45] Title V of the Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999), 15 U.S.C. § 6801, *et seq*.
[46] SEC Regulation S-P, *Privacy of Consumer Financial Information*, 17 C.F.R. § 248 (2000).
[47] FTC, *Standards for Safeguarding Customer Information*, 16 C.F.R. Part 314, 67 FR 36493 (2002).
[48] *S*ee also Patricia E. M. Covington, *Consumer Privacy and Information Security Issues*, The Blue Sky Bugle Vol. 2007, No. 3 (November 2007).
[49] Regulation S-P, *supra* note 21.

- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The SEC's rule also requires SEC registrants to properly dispose of nonpublic personal information. This requires reasonable measures to protect against unauthorized access to or use of the disposed information.

State-registered investment advisers are covered by the FTC's *Privacy of Consumer Financial Information* rule.[50] The 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". The FTC-required security program requires that state-registered investment advisers:

- Designate an employee or employees to coordinate your information security program.

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

    - Employee training and management;

    - Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

    - Detecting, preventing and responding to attacks, intrusions, or other systems failures.

Under the current FTC rule, among other things, the firm's information security program must address the firm's use of technology, including hardware, software, and service providers transmitting the data. Besides preventative measures, the program must address detection and response to data breaches. Moreover, it must be "comprehensive" and must be periodically reevaluated—it must be an iterative, not static, policy and process.

**State-mandated Safeguarding Rules**

Federal privacy and safeguarding law and rules do not preempt more restrictive or protective state laws. Indeed, Section 504 of the GLB Act authorized state insurance authorities to implement federal privacy requirements imposed under Title V, *Privacy*.[51] The model rule

[50] 16 C.F.R. 314.

[51] See the model rules adopted by the National Association of Insurance Commissioners (NAIC) at http://www.naic.org/documents/topics_consumer_data_security.pdf .

requires each state insurance licensee to establish a comprehensive, written information security program that includes administrative, technical, and physical safeguards for the protection of customers' nonpublic personal information, appropriate to the size and complexity of the licensee and the nature and scope of its activities. The security program may include provisions such as identifying reasonably foreseeable internal or external threats, assessing their likelihood and potential damage, training staff, regularly testing key controls, and exercising due diligence in selecting service providers. A violation is deemed to be an unfair method of competition or an unfair or deceptive act and practice in the conduct of the business of insurance in the state.[52]

Generally, state regulators may lack direct statutory authority to enforce specific federal laws and rules, such as the federal Safeguarding and Red Flags Rules (discussed later). However, related state-enforceable requirements may be affected, such as fiduciary duties, books and records, compliance programs, or business continuity planning rules. Federal violations may prompt state referrals to federal agencies having enforcement powers. In addition, federal violations may prompt states to institute administrative proceedings to revoke, suspend, condition, limit or deny a state registration after a state registrant has received notice and an opportunity for a hearing.

**SEC – CTFC 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).[53] These two rules are, in substance, the same as rules adopted by the FTC and federal banking agencies. The SEC-CTFC Red Flags Rules apply to SEC and CTFC registrants; the FTC's Red Flags Rule applies to state-registered investment advisers, including private fund advisers that are not SEC-registered.

The SEC's Red Flags Rule applies a broader interpretation of "financial institution" and "covered accounts" than does the FTC's rule. The SEC's rule explicitly covers broker-dealers and investment advisers who have any ability to direct withdrawals or transfers from client accounts to third-parties. The FTC's rule is less specific because it covers all other "financial institutions" that are not regulated by the SEC, CFTC, or federal banking agencies. In practice, the FTC's rule may come to be construed in light of the SEC's position.

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. The rules also require a financial institution to periodically

[52] *See* Chapter 5 of the Michigan Insurance Code, *Privacy of Financial Information*, added by Public Act 24 of 2001, June 18, 2001.

[53] *Identity Theft Red Flags Rules*, Release Nos. 34-69359, IA-3582, IC-30456; File No. S7-02-12 (2013). The SEC Red Flags Rule is codified at 17 C.F.R. 248. The CTFC Red Flags Rule is codified at 17 C.F.R. 162, Subpart C.

reassess whether it offers or maintains covered accounts that would require it to have a place in a prevention program. The identity theft prevention program must address four elements: identify relevant red flags, detect those red flags, respond appropriately to detected red flags, and periodically update the program to reflect changes in risks. The SEC-CTFC and FTC rules include helpful guidance about each of these elements.[54]

**FINRA Cybersecurity Rules and Guidance**

FINRA applies and examines broker-dealers for compliance with federal law, the SEC's rules, and FINRA rules. FINRA's website provides cybersecurity guidance and resources for brokerage firms.[55] FINRA has provided guidance about cybersecurity issues, including risks related to wireless fidelity (Wi-Fi) and remote access networks.[56] 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.[57] FINRA Rule 3110 requires the establishment of a supervisory system and adoption of written policies and procedures, which should be reasonably designed to achieve compliance with applicable securities laws and regulations. FINRA Rule 3120 requires firms to have supervisory controls to test the policies and procedures and to amend them if necessary. FINRA Rule 3130 requires the firm's CEO to certify that a process is in place to adopt adequate supervisory policies.

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.

Drawing from its 2014 exam sweep of broker-dealers as well as recent data, FINRA published an extensive report on cybersecurity best practices earlier this year, which includes helpful guidance for firms in preparing for and addressing cybersecurity threats. FINRA recommends that senior-level employees engage in addressing cybersecurity issues, and to train all staff in preparedness. FINRA also recommends reaching outside the firm itself, by exercising due diligence in vendor relationships, and collaborating with other firms in terms of defense

[54] 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 .
[55] FINRA Customer Information Protection, http://www.finra.org/Industry/Issues/CustomerInformationProtection/ ; and Firm Identity Theft, http://www.finra.org/Industry/Issues/CustomerInformationProtection/p117442 .
[56] 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 .
[57] On December 1, 2014, FINRA Rule 3110 superseded NASD Rule 3010, FINRA Rule 3120 superseded NASD Rule 3012, and FINRA Rule 3130 superseded NASD Rule 3013, which previously imposed similar requirements.

strategies and intelligence-sharing. Further details and recommendations can be found in the useful report.[58]

**State Breach Notification Laws**

Forty-seven states require security breach notifications.[59] 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.[60] However, as noted above, the SEC has not adopted notification requirements. Forty-seven states have also enacted "security freeze" laws that allow customers to 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.[61] 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 so should 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.

Business continuity planning (BCP) refers to a firm's preparation for any event that may cause a business activity disruption. A BCP is primarily a safeguard to protect from natural disasters, but also applies to other disasters such as terrorism, civil unrest, and cyber strikes.[62] The aim of a BCP is to avoid, mitigate, and recover from such disruptions. 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.[63]

---

[58] The report can be found at http://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

[59] 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.

[60] The following 15 states' breach notification laws do not contain an exception or safe harbor for compliance with federal law or related rules governing data breaches: California, District of Columbia, Georgia, Illinois, Louisiana, Montana, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Texas, Vermont, and Washington.

[61] For more information, *see* http://www.Consumersunion.org/campaigns/learn_more/003484indiv.html .

[62] Lorna A. Schnase, *Business Continuity Planning for Advisers*, NSCP Currents (September 2013).

[63] 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*.

In its 2003 release adopting SEC Rule 206(4)-7, *Compliance Procedures and Practices*, the SEC noted that "an adviser's fiduciary obligation to its clients includes the obligation to take steps to protect the clients' interests from being placed at risk as a result of the adviser's inability to provide advisory services." The SEC further stated that "clients of an adviser that is engaged in the active management of their assets would ordinarily be placed at risk of the adviser ceased operations." The Rules' joint adopting release notes that, at minimum, policies and procedures should be established to address, among other things, an investment adviser's BCP.[64] Although mentioned, the SEC did not elaborate on the requirements for a BCP. Because no specific requirements exist, firms have the flexibility to create and implement plans that work for them. NASAA has adopted a model business continuity plan rule that is recommended to the states for adoption.[65]

**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). The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework is industry neutral, so 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*,[66] 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**. It 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.

---

[64] SEC Release Nos. IA-2204, IC-26299, *Final Rules on Investment Adviser Compliance Programs*, http://www.sec.gov/rules/final/ia-2204.htm.

[65] *See* NASAA *Model Rule on Business Continuity and Succession Planning*, April 13, 2015, http://www.nasaa.org/wp-content/uploads/2011/07/NASAA-Model-Rule-on-Business-Continuity-and-Succession-Planning-with-gu....pdf. Michigan has not yet adopted this model rule.

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

- **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 when prompted by changes and periodically**. 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 on hardware, software, and data handling vendors such as "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.

**Cyber-Planning Resources**

Created by an Executive Order of the President of the United States,[67] 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).[68] The Framework consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The Framework is industry neutral, so relevant to all types of businesses. The NIST's Computer Security Division[69] 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.[70]

[67] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity .
[68] http://www.nist.gov/cyberframework/.
[69] These resources are available at http://csrc.nist.gov/groups/SMA/sbc/library.html.
[70] Available at http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

In addition, the Securities Industry and Financial Markets Association (SIFMA) published useful *Guidance for Small Firms*,[71] 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.

The Cybersecurity Unit of the Department of Justice published a best practices document in April 2015 outlining how to prepare an actionable plan to respond to cyber incidents, and how to execute that plan in the event of an intrusion. The document was drafted with smaller organizations in mind, but nevertheless provides an excellent resource for larger organizations as well. Its recommendations include prioritizing data, efficiently allocating resources, and to organize personnel in the most appropriate way to prepare and respond to an intrusion.[72] The SEC[73] and FINRA[74] guidance documents provide helpful recommendations as well.

The following bibliography provides additional resources on the topics covered in this article and websites offering more information:

**Relevant Regulations**

- FTC *Standards For Safeguarding Customer Information*, 16 C.F.R. Part 314, http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/standards-safeguarding-customer.

- FTC *Identity Theft Rules*, 16 C.F.R. Part 681, http://www.ecfr.gov/cgi-bin/text-idx?SID=129b0f6f5825a7c64a528c718a2c5577&tpl=/ecfrbrowse/Title16/16cfr681_main_02.tpl.

- SEC *Identity Theft Red Flags Rules*, Release Nos. 34-69359, IA-3582, IC-30456; File No. S7-02-12 (2013), codified at 17 CFR Part 248, http://www.sec.gov/rules/final/2013/34-69359.pdf.

- SEC Regulation S-P, *Privacy of Consumer Financial Information*, 17 C.F.R. Part 248 (2000), http://www.gpo.gov/fdsys/granule/CFR-2012-title17-vol3/CFR-2012-title17-vol3-part248-subpartA.

- Title V of the Gramm-Leach Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999), 15 U.S.C. §§ 6801-6831, http://www.gpo.gov/fdsys/granule/USCODE-2011-title15/USCODE-2011-title15-chap94-subchapI-sec6801.

[71] Available at http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/ .
[72] Available at http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.
[73] *Supra* note 37.
[74] *Supra* note 63.

**Articles and Regulatory Statements**

- FTC, *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business, Federal Trade Commission (FTC)*, (May 2013), http://www.business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business .

- FINRA *Regulatory Notice No. 11-14, Third Party Service Providers*, (2011), http://finra.complinet.com/net_file_store/new_rulebooks/f/i/finra_11-14.pdf.

- MarketCounsel, *What Went Down at the SEC's Cybersecurity Roundtable*, http://marketcounsel.com/2014/03/26/what-went-down-at-the-secs-cybersecurity-roundtable/.

- NASAA, *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.

- National Institute of Standards and Technology, *Framework for Creating Critical Infrastructure Cybersecurity*, (February 12, 2014) http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm#.

- National Institute of Standards and Technology, *Small Business Information Security: The Fundamentals*, (October 2009), http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

- SEC Office of Compliance Inspections and Examinations (OCIE) *Cybersecurity Examination Initiative*, September 15, 2015: http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

- SEC *Investor Alert: Identity Theft, Data Breaches and Your Investment Accounts*, September 22, 2015, http://www.sec.gov/oiea/investor-alerts-bulletins/ia_databreaches.html.

- SEC OCIE, *National Exam Program OCIE Cybersecurity Initiative*, Vol. IV, Issue 2 (April 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf.

- SEC Statement, Luis A. Aguilar, *Cyber Risks and the Boardroom*, (June 10, 2014), http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

- SEC Statement, Mary Jo White, *Opening Statement at SEC Roundtable on Cybersecurity*, (March 26, 2014), http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541286468.

- Shane B. Hansen, *The Price of Protecting Privacy–Proposed Regulation S-P Amendments*, NSCP Currents, (April/May 2008), http://www.wnj.com/Publications/The-Price-of-Protecting-Privacy-Proposed-Regulatio.

- Shane B. Hansen, *Standing in the Breach–State Law Requirements When a Customer Data Breach Occurs*, (March 11, 2009), http://www.wnj.com/Publications/Standing-in-the-Breach%E2%80%94State-Law-Requirements.

- Symantec Corporation, *Internet Security Threat Report* (2014), http://www.symantec.com/security_response/publications/threatreport.jsp .

- U.S. Chamber of Commerce, *Commonsense Guide to Cyber Security for Small Businesses*, https://www.uschamber.com/sites/default/files/legacy/reports/cybersecurityguide923.pdf.


**Websites and Other Resources**

- Financial Services Information Sharing and Analysis Website, https://www.fsisac.com/.

- FINRA Business Continuity Planning Template, http://www.finra.org/Industry/Issues/BusinessContinuity/.

- FINRA – SEC Identity Theft Red Flags Rule Template, http://www.finra.org/industry/issues/customerinformationprotection/p118480.

- Homeland Security US-CERT Pages, https://www.us-cert.gov/.

- National Conference of State Legislatures State Security Breach Notification Laws, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

- National Institute of Standards and Technology Computer Security Resource Center, http://csrc.nist.gov/groups/SMA/sbc/index.html.

- National Institute of Standards and Technology general website, http://www.nist.gov/.

- Securities Industry and Financial Markets Association (SIFMA) Cybersecurity Resource Center, http://www.sifma.org/issues/operations-and-technology/cybersecurity/overview/.

10833985-13