Federal and State Cybersecurity Regulation of Financial Services Firms

By Brian Neil Hoffman, Romaine Marshall and Matt Sorensen

Cybercrime poses an ever-increasing threat to consumers of financial products and services. In 2016, the then-SEC Chair said that cybercrime ranks as "one of the greatest risks facing the financial services industry." Federal law thus requires financial services firms to implement procedures designed to protect their customers' data. Now, individual states are increasingly getting into the game. Two states recently enacted or proposed rules for financial services firms. This may be just the beginning of a national trend toward increased state regulation of cybersecurity matters. Financial services firms and their management should keep a close eye on developing cybersecurity regulations, so as to be better prepared to proactively address the shifting regulatory landscape as it continues to evolve.

Federal Focus on Cybersecurity

The U.S. Securities and Exchange Commission (SEC) has long focused on cybersecurity procedures at registered investment advisers (IAs) and broker-dealers (BDs). The SEC's examination program included cybersecurity as a priority for many years. And the SEC has engaged in outreach discussions with the securities industry about the topic as well.

In April 2015, the SEC's Division of Investment Management issued cybersecurity guidance, recognizing that "both funds and advisers increasingly use technology to conduct their business activities and need to protect confidential and sensitive information related to these activities from their partners, including information concerning fund investors and advisory clients." Among other things, the SEC's guidance encourages firms to:

- Conduct periodic assessments of their information collection; potential threats and vulnerabilities, security controls and processes; and the effectiveness of an organization's governance structure for the management of cybersecurity risk.
- Develop strategies to respond to threats and incidents that include controlling access to various systems and data; data encryption; restricting the use of removable storage and deploying protective software; data backup and retrieval; and development of an incident response plan.
- Implement strategies through written policies, procedures, and training, and engage in ongoing monitoring of compliance.

The guidance further provides:

> "Funds and advisers will be better prepared if they consider the measures discussed herein … when planning to address cybersecurity and a rapid response capability. The staff also recognizes that it is not possible for a fund or adviser to anticipate and prevent every cyber-attack. Appropriate planning … nevertheless … may assist funds and advisers in mitigating the impact of any such attacks and any related effects on fund investors and advisory clients."

Indeed, multiple regulatory tools stand behind the SEC's recommended practices. To start, the SEC expects IAs and BDs to maintain appropriate compliance policies and procedures in varied aspects of their businesses, including cybersecurity. Regulation S-P specifically requires registered IAs, BDs, and investment companies to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." And Regulation S-ID requires certain regulated IAs and BDs to adopt and maintain policies and procedures designed to detect, prevent, and mitigate identity theft. An identity theft program under this rule should:

- Identify relevant red flags — that is, potential patterns, practices or specific activities indicating the possibility of identity theft;
- Detect potential red flags, for both new and existing accounts;
- Prevent and mitigate identity theft through an appropriate response to the perceived risk; and
- Issue regular updates and improvements to the program.

The SEC has not shied from pursing enforcement actions for alleged failures in these areas. In June 2016, for example, the SEC announced that an SEC-registered IA and BD agreed to pay a $1 million civil penalty for its alleged failure to adopt written policies and procedures reasonably designed to protect customer data. The respondent allegedly allowed employees to access customer information through internal web portals without appropriate access restrictions or access audits. These alleged vulnerabilities were allegedly exploited by an individual then-employee, who downloaded customer data to his personal device that was then hacked. Prior SEC enforcement actions provide similar cautionary tales.

States Are Also Becoming Active

Many states already have in place general cybersecurity requirements that protect personally identifiable

continued on page 6

Brian Neil Hoffman (bnhoffman@hollandhart.com) is of counsel with Holland & Hart LLP. A former SEC enforcement attorney, he defends clients in government and SRO investigations and litigates shareholder disputes. **Romaine Marshall** (rcmarshall@hollandhart.com) is a partner in the firm. **Matt Sorenson** (cmsorensen@hollandhart.com) is an associate.

continued from page 5

information in a broad range of industries. In 2002, for example, California enacted the nation's first state general data breach notification law. Since then, 46 other states, Washington, DC, and three U.S. territories have enacted similar laws. More recently, two states emerged with their own cybersecurity regulations specifically focused on financial services firms: New York and Colorado. Nor would it be surprising to see other states following suit soon.

NY's Financial Institution Regulations

Effective on March 1, 2017, New York adopted cybersecurity requirements (23 NYCRR 500) that mandate financial institutions implement robust controls to detect, prevent, and report cyber-incidents. Many experts predict that the regulation may soon become the baseline standard for the industry, and may inspire similar cross-industry regulations.

Generally speaking, the New York regulation requires banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services (NYDFS) to establish and maintain cybersecurity programs designed to protect consumers' private data and ensure industry safety. The regulation includes certain minimum standards and encourages firms to keep pace with technological advances.

More specifically, the regulation requires covered entities to:

- Conduct periodic, documented risk assessments, considering changing threats, business needs, and technologies;
- Maintain a cybersecurity program based on the risk assessment and defensive IT infrastructure;
- Include data governance, data classification, asset and device inventory, business resiliency, and incident response in written information security policies;
- Comply with governance and staffing requirement — including appointment of a Chief Information Security Officer with specific, enumerated responsibilities, by August 2017;
- Conduct annual penetration testing and bi-annual vulnerability scans;
- Maintain transaction and server logs sufficient to detect and respond to adverse security events;
- Limit user access privileges;
- Adopt procedures, guidelines and standards to ensure secure application development and software product security evaluation;
- Install a robust third-party service provider risk-management program, policies, and procedures;
- Ensure adequate training and qualifications of personnel and/or procure third-party expertise to operate and perform core cybersecurity functions;
- Use multi-factor authentication (MFA) or risk-based authentication; enforce MFA for all external network access;
- Destroy nonpublic information periodically and securely;
- Implement controls, including encryption or compensating controls;
- Establish a written incident-response plan;
- Provide regular cybersecurity awareness training; and
- Notify NYDFS of any breaches within 72 hours.

The regulation includes transition periods ranging from one to two years for most requirements. Even with the staggered compliance dates, however, full compliance with such an expansive regulation may pose challenges.

Some of the regulation's requirements will apply even to entities that seek exemption. These include conducting a risk assessment, implementing written policies and procedures to secure nonpublic information that is accessible to, or held by, third-party service providers, and establishing policies and procedures for the secure disposal of nonpublic information.

Some persons or entities will be exempt from the remainder of the regulation's requirements: small covered entities of "fewer than 10 employees" or "less than $56 million in revenue in each of the last three fiscal years," designees covered by another covered entity, entities that do not possess or handle nonpublic information, and captive banks or insurance companies that only handle the nonpublic information of the corporate parent company.

Exempted covered entities must still file a certificate of exemption within 30 days.

Notably, the New York regulation does not expressly apply to IAs and BDs, unless those entities are otherwise licensed by the NYDFS in another capacity, for example as an insurance broker or agent.

Colorado Focuses on IAs and BDs

Colorado's Division of Securities recently announced proposed additions to the Colorado Securities Act (Rule 51-4.8 and 51-4.14) that would require Colorado IAs and BDs to establish and maintain written procedures "reasonably designed to ensure cybersecurity" and to include cybersecurity as part of their risk assessments.

These proposed additions are designed "to clarify what a broker-dealer and investment adviser must do in order to protect information stored electronically." Specifically, the additions would require firms' procedures to, the extent reasonably possible, provide for:

- An annual cybersecurity risk assessment;
- The use of secure email, including use of encryption and digital signatures;
- Authentication practices for employee access to electronic communications, databases and media;
- Procedures for authenticating client instructions received via

continued on page 11

Delaware Rulings

continued from page 10

creditor to sue the controlling members of an LLC for breach of fiduciary duty and related claims in connection with allegations that those members deceived the creditor into lending money on false pretenses. In *Trusa v. Nepo*, C.A. No. 12071-VCMR (Del. Ch. April 13, 2017), the court determined that the creditor had no standing for such claims — nor did a power of attorney provide a basis for standing.

Background

The creditor involved in this matter was verbally seduced into making an investment in the LLC, and was led to believe that his investments would be secured. One of the provisions in the loan documents was a power of attorney that allowed for certain default remedies. After the LLC defaulted on the loans, the creditor learned of various dishonest dealings and misrepresentations regarding the status of the company and what the funds were used for.

Before the Chancery suit was filed, a complaint was filed in the Delaware Superior Court and a default judgment was entered. This Chancery suit was brought claiming that the managing members breached their fiduciary duties. The creditor also sought a dissolution of the LLC in addition to asserting fraud and related claims.

Key Legal Principles

The most noteworthy aspect of this decision is the court's holding that a creditor has no standing to bring derivative claims on behalf of an LLC for breach of fiduciary duty, based primarily on Section 18-1002 of the Delaware LLC Act. Together with Section 18-1001 of the Act, it remains unambiguous that only members and assignees can assert derivative claims on behalf of an LLC. Prior opinions by Chancery and the Delaware Supreme Court endorsed the foregoing interpretation of the Act. *See CML V, LLC v. Bax (Bax I)* 6 A.3d 238 Del. Ch. 2010) aff'd *CML V, LLC v. Bax (Bax II)*, 28 A.3d 1037, 1043 (Del. 2011), highlighted on these pages. S*ee also In Re Carlisle Etcetera LLC*, 114 A. 3d 592, 604 (Del. Ch. 2015) (explaining that although they are barred from derivative actions, creditors have adequate remedies at law to protect their interests such as liens on assets. This case also addresses equitable dissolution.)

The court also explained that the creditor's power of attorney does not and cannot provide standing that is otherwise denied for the derivative claims attempted by him. The court observed that such a contrary argument ignores the fact that the power of attorney is expressly limited to pursuing remedies provided in the loan agreement.

No Standing for Dissolution Either

Regarding the dissolution claims, Section 18-802 of the Act limits a request for dissolution of an LLC to either a member or a manager. The creditor in this case likewise failed to establish standing for his request for dissolution. Section 18-203(a) of the Act provides seven ways that a certificate of cancellation of an LLC may be filed. The ability to file such a certificate did not help this creditor because only after dissolution and winding up of an LLC may a creditor seek appointment of a trustee or a receiver in connection with a prior dissolution.

Regarding the extreme remedy of "equitable dissolution," the court found insufficient facts in the record to justify such an exercise of the court's authority.

Fraud Claim Fails

The court emphasized the truism that a simple breach of contract cannot be bootstrapped into a fraud claim. For example, the court quoted from prior case law holding that: "a party's failure to keep a promise does not prove the promise was false when made, and that the plaintiff did not adduce evidence showing that the defendant intended to renege as of the time it made the promise."

Material Omission

The court found that the claim that a material omission amounted to fraud was not adequately alleged for several reasons. The court explained that in an arm's-length negotiation: "where no special relationship between the parties exists, a party has no affirmative duty to speak and is under no duty to disclose facts of which he knows the other is ignorant even if he further knows the other, if he knew of them, would regard them as material in determining his course of action in the transaction in question."

The court further reasoned that a fraud claim cannot start from an omission in an arm's-length setting. Rather, if a party chooses to speak, then he cannot lie, and "once the party speaks, it also cannot do so partially or obliquely such that what the party conveys becomes misleading."

—❖—

Cybersecurity

continued from page 6

electronic communication; and

- Disclosure to clients of the risks of using electronic communications.

Colorado does not appear to expect a "one-size-fits-all" solution among firms. Rather, the proposed additions enumerate a list of factors that the Commissioner may consider when determining whether a firm's procedures are reasonably designed. These include:

- The firm's size;
- The firm's relationships with third parties;
- The firm's policies, procedures, and training of employees with regard to cybersecurity practices;
- Authentication practices;
- The firm's use of electronic

continued on page 12

Cybersecurity

continued from page 11

communications;

- The automatic locking of devices used to conduct the firm's electronic security; and
- The firm's process for reporting lost or stolen devices.

If approved, the rules would likely take effect later in 2017. The additions may not have a significant impact on larger organizations, many of which already have in place fairly substantial cybersecurity guidelines and procedures. Yet the additions could expose small- and medium-sized IAs and BDs to new, and fairly complex, regulatory risks.

Other States May Soon Follow Suit

New York and Colorado are likely just the first in the series of states to consider and adopt their own cybersecurity regulation regimes. Indeed, other states already appear to be paying close attention. Idaho, for example, recently issued an advisory reminding investors about the importance of understanding how their personal information is being protected by financial firms. Such advisories may sometimes end up being the first step towards new regulation. Texas is likewise attuned to the need for additional information on cybersecurity, having posted a list of cybersecurity resources to assist state-registered IAs and other professionals.

Several Practical Takeaways

Due to continued federal and state regulatory focus, cybersecurity compliance has rapidly become an additional cost of doing business in the financial services industry. Firms are thus well advised to proactively review their policies and procedures, and assess potential improvements as appropriate. Some specific proactive steps that firms may consider:

… cybersecurity compliance has rapidly become an additional cost of doing business in the financial services industry.

- Generating awareness and support among executives; sharing accountability for cybersecurity with legal, compliance, IT, and operations business lines.
- Funding information security initiatives and monitoring security expenditures as a percentage of overall operational and IT budgets.
- Getting help — finding and retaining information security professionals with top-down support of security initiatives, paid training, and professional certifications.
- Ensuring relevant personnel remain up-to-date on applicable legal compliance requirements.
- Ensuring risk assessments appropriately consider threats, vulnerabilities, and safeguards.
- Adopting a cybersecurity framework such as NIST's Cyber Security Framework or ISO 27001.
- Avoiding confusion of risk assessments with system penetration tests and vulnerability scans, with the latter providing additional layers of protection and comfort.

Providing prompt, proactive attention to cybersecurity risks and compliance before an incident goes a long way toward limiting the negative ramifications when (not "if") a cybersecurity incident actually occurs.

—❖—

Lawyers and 'Poker'

continued from page 8

Series of Poker and why many people argue that poker is a game of skill, not chance. In effect, winning poker players are "outcome-blind."

After the fact, when they analyze their play, they focus on the process — Did I bet when I should have? Did I raise the right amount? Should I have folded based on what I knew? — rather than the win-lose result. Amateurs talk about their luck; winning poker players don't.

Lawyers and clients can learn a lot from this approach. Poker players can't control what cards are dealt; they can only make the best bets they can based on the limited information known to them. The same is true for lawyers and clients. There will always be facts and circumstances beyond your control that may affect the outcome of any given case. A witness may crumble; a judge may retire; or a law may change. But, as long as your process is sound and you make the best arguments and decisions you can based on the information you are able to develop, in the long run, you, too, should come out on top.

—❖—