14 December 2015

Practice Groups:

Government Enforcement

Global Government Solutions

Cyber Law and Cybersecurity

Treasury Department Issues Cybersecurity Checklist for Financial Institutions: What Might Apply to Your Financial Services Company?

U.S. Government Enforcement/Cyber Law and Cybersecurity Alert

By: Mark A. Rush, Thomas C. Ryan, Joseph A. Valenti, Samuel P. Reger

On November 17, 2015, Deputy Treasury Secretary Sarah Bloom Raskin devoted her remarks at the Clearing House Annual Conference to financial sector cybersecurity.[1] She concluded with a list of recommendations for handling cybersecurity at financial institutions. In light of them, prudent in-house counsel, compliance officers, and security personnel may want to review their company's cybersecurity plan to determine which of the deputy secretary's recommendations are applicable. This *Alert* recounts Deputy Secretary Raskin's "to-do list" and provides step-by-step suggestions regarding cybersecurity response plans in light of it.

The need for prompt attention to this issue is manifest: cybersecurity concerns are a growing threat. "The epidemic of data breaches has grown over the past decade, now affecting almost every American consumer and inflicting billions of dollars of damage to the U.S. economy. Since 2005, almost 4,500 publicly known breaches have affected over 900 million consumer records."[2]

Step 1: Assess The Applicable Legal Landscape

The United States does not currently have a one-size-fits-all law for financial services companies to follow in securing consumer data or reporting breaches to consumers. Companies should examine the markets they serve and the data they store to determine what federal or state laws and rules apply, the first step in building a robust and compliant cybersecurity program.

[1] https://www.treasury.gov/press-center/press-releases/Pages/jl0276.aspx.

[2] http://www.privacyrights.org/content/data-breach-readiness-and-follow-being-prepared-inevitable.

Treasury Department Issues Cybersecurity Checklist for Financial Institutions: What Might Apply to Your Financial Services Company?

	Law that Might Apply	Action[3]
If your company is broadly defined as a "financial institution" (engaged in significant financial activities),[4] then	Under the Gramm-Leach-Bliley Act, the FTC's Privacy Rule and Safeguards Rule may apply.[5]	Your company may be required to have measures in place to keep consumer data secure, such as a written, risk-based information security plan. A cybersecurity framework, discussed below, can assist in meeting this requirement.
If your company is broadly defined as a "financial institution" and is subject to SEC regulation, then	Under the Gramm-Leach-Bliley Act, the SEC's Regulation S-P may apply.[6]	Your company may be required to establish appropriate standards to safeguard consumer data, such as encryption and mandating antivirus software.
If your company is subject to SEC regulation, issues securities, and is publicly held,[7] then	Parts of the Sarbanes-Oxley Act may apply.[8]	Your company may be required to develop internal controls and report on the controls to ensure that a security breach did not affect the accuracy of financial results. Consider, as part of a cyberattack response plan, immediate notification to those who are responsible for the accuracy of financial results that a cyberattack occurred.
If your company maintains consumer credit reporting information, then	The Fair Credit Reporting Act may apply.[9]	Your company may be required to ensure accurate collection of credit data and to properly dispose of consumer information. Routinely auditing internal and external cybersecurity measure can assist in meeting this requirement.

[3] Beyond the "action" listed in this column, companies may also have to take other physical, administrative, and technical protection measures to comply with the applicable law.

[4] "An institution that is significantly engaged in financial activities is a financial institution," which includes banks, credit unions, and credit card companies. 16 C.F.R. 313.3(k)(1). The FTC also provides other less apparent examples financial institutions: "check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services," noting that the provisions apply "regardless of size." *See* https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[5] 16 C.F.R. § 313 (Privacy Rule); 16 C.F.R. § 314 (Safeguards Rule).

[6] 17 C.F.R. § 248, (Regulation S-P).

[7] 15 U.S.C. § 7262 and 15 U.S.C. § 7241 (reporting statutes under Sarbanes-Oxley) applies to companies that file annual reports under 15 U.S.C. § 78m(a) or 15 U.S.C. § 78o. Companies that file reports under § 78m(a) or § 78o are companies that issue securities pursuant to 15 U.S.C. § 78. An issuer is "any person who issues or proposes to issue a security," among other definitions. 15 U.S.C. § 78c(8). For the lengthy definition of "security" *see* 15 U.S.C. § 78c(10).

[8] 15 U.S.C. § 7262; 15 U.S.C. § 7241.

[9] 15 USC § 1681.

Treasury Department Issues Cybersecurity Checklist for Financial Institutions: What Might Apply to Your Financial Services Company?

In addition to federal regulation, at least 46 states have passed laws that require companies to protect the sensitive personal information of their residents and to notify affected residents and regulators of a data breach.[10] The nuances of these state laws vary widely. However, these laws generally follow a framework that imposes a requirement of reasonable security measures, defines to whom or what the law applies, what information should be protected, what constitutes a breach, and what penalties apply in case of enforcement.[11]

Noncompliance with these laws and/or regulations can lead to enforcement by both federal and state regulators. For example, the Federal Trade Commission ("FTC") is authorized to protect consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace under section 5 of the Federal Trade Commission Act.[12] The FTC's primary legal authority comes from this section.[13] In the data-security context, the FTC uses this authority to bring administrative or civil actions against financial institutions that have misled consumers by "failing to maintain security for sensitive consumer information."[14] The FTC also has the authority to enforce "a variety of sector specific [privacy] laws" such as the Truth in Lending Act and the Fair Credit Reporting Act.[15] Since 2002, under Section 5 of the FTC Act, the FTC "has settled more than 30 matters challenging companies' claims about the security they provide for consumers' personal data and more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice."[16] For example, in August 2014, the FTC settled charges against Fandango and Credit Karma stemming from allegations that the companies misrepresented the security of their mobile apps to consumers because they "disabled a process called SSL certification" on their mobile service platform, leaving consumers' sensitive personal information vulnerable.[17] The penalty was composed of a requirement that the companies "establish comprehensive security programs designed to address security risks … and to undergo independent security assessments every other year *for the next 20 years*."[18] Also for misleading consumers, the same 20-year monitoring period was imposed on cord blood bank, Cbr Systems, Inc., related to a data breach that exposed Social Security numbers and credit card information of nearly

---

[10] Gina Stevens, *Data Security Breach Notification Laws*, Congressional Research Service, Summary, 2012, available at https://www.fas.org/sgp/crs/misc/R42475.pdf.

[11] *Id.*

[12] 15 U.S.C. § 45(a)(2). *See also* http://www.klgates.com/files/Publication/a1882ede-dc6d-4e70-9c52-06aa81f51a7f/Presentation/PublicationAttachment/06100034-2e47-4448-8c97-0bd2254cef5a/Law360_Heiman_March2015.pdf.

[13] *See* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[14] *See* https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. Recently, the Third Circuit upheld the FTC's ability to bring data-security actions under the FTC Act. *See FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015).

[15] *See* https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.

[16] *See* Gina Stevens, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices Authority*, Congressional Research Service, Summary, 2014, available at http://fas.org/sgp/crs/misc/R43723.pdf.

[17] *See* https://www.ftc.gov/news-events/press-releases/2014/08/ftc-approves-final-orders-settling-charges-against-fandango.

[18] *Id.* (emphasis added).

300,000 consumers.[19] At the state level, attorneys general are often tasked with enforcing data-security breaches.[20]

Step 2: Implementing Cyber Security Controls

Implementing cybersecurity controls means building a framework that complies with relevant laws and regulations and is reasonably designed to thwart attacks by cybercriminals. Deputy Secretary Raskin identified "three key things that each executive … can do at their own [financial] institution that collectively will make a difference [in combating cyber attacks]."

1. Ensure that cyber risk is part of your institution's risk management framework and cybersecurity is embedded in your governance, control, and risk management framework.
2. Engage in basic cyber hygiene, those essential practices that bolster the security and resilience of computer networks and systems.
3. Press your institution to prepare a response and recovery playbook for significant cyber incidents. This playbook should be well thought out and routinely tested all the way up to the board, and externally through exercises with the financial sector and the government.

Below are recommendations to implement these three keys:

1. Embedding Cybersecurity in Corporate Governance

Financial services companies should consider appointing a chief information security officer ("CISO"), a dedicated and trained executive, in charge of managing information security. Appointing a CISO demonstrates a financial institution's commitment to protecting itself and its consumers from cyber threats, and, in the aftermath of a cyberattack, it may protect the financial institution from extended liability by demonstrating that it took reasonable steps to protect consumer data. [21]

Soon, financial institutions with any operations in the global financial hub of New York may not have a choice in the matter. The New York Superintendent of Financial Services has said his office intends to move forward with a proposed rule requiring covered entities to have a CISO "responsible for overseeing and implementing its cybersecurity program and enforcing its cybersecurity policy. The CISO would also be required to submit to the Department an annual report, reviewed by the entity's board, which assess the cybersecurity program and the cybersecurity risks to the entity"[22] Other steps a financial-services company should consider include:

- Conducting a risk assessment to understand key data repositories and vulnerabilities.
- Planning for and providing training on cyber crisis management.
- Obtaining appropriate cyber insurance coverage.

[19] *See* https://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers.
[20] *See* http://www.mass.gov/ago/news-and-updates/press-releases/2015/2015-02-05-anthem-data-breach.html.
[21] The CEO and board can also play an important advisory and oversight role in preventing cyber attack risk.
[22] http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf.

Treasury Department Issues Cybersecurity Checklist for Financial Institutions: What Might Apply to Your Financial Services Company?

2. Engaging in Cyber Hygiene

Companies should develop and implement a cybersecurity framework that is tailored to its business and the attendant risks. On February 12, 2013, President Barack Obama issued an executive order to improve the nation's cybersecurity by developing a set of industry standards. In response, the National Institute of Standards and Technology (an agency of the U.S. Department of Commerce dedicated to establishing technical and scientific standards) developed a framework that, "regardless of size, degree of cybersecurity risk, or cybersecurity sophistication[,]" can assist in developing an appropriate risk-based cybersecurity program for a company.[23] Steps a financial-services company should consider under this framework include:

- Routinely auditing internal and external cybersecurity measures.
- Drafting and implementing data-management and -security policies.
- Continuously implementing remedial improvements based on discovered vulnerabilities.

3. A Response and Recovery Playbook

Companies should consider drafting a written cyberattack response plan. This written plan should define the members of cyber response team, a group of employees that will be available to respond to a cyberattack at any time. The first 24 to 48 hours of the plan are the most critical. During that time, the cyber response team should be prepared to accomplish certain tasks, such as determining what systems were affected, how the attack originated, and what information was stolen. Further, the response team should attempt to isolate the affected system and document its activity. Thorough documentation will help law enforcement and will defend against potential civil actions, either from the government or private citizens. Other steps a financial services company should consider include:

- Planning for and providing training on cyber crisis management.
- Providing any statutorily or contractually mandated notice to affected parties.
- Abiding by legal requirements and preserving evidence of cybercrime to avoid obstruction-of-justice charges, spoliation issues, and related problems.
- Appropriately working with law enforcement regarding response and best practices, which may include training and designating a law enforcement coordinator to interact with law enforcement and counsel to handle the matter.[24]

Conclusion

Deputy Secretary Raskin's recommendations may, in time, be seen as more of a floor than a ceiling regarding the measure of preparedness expected by the federal government. In any event, her remarks underscore the need for financial institutions to consider evaluating the internal controls and procedures in place for responding to a data breach. They also serve

[23] *See* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[24] *See* Mark A. Rush & Joseph A. Valenti, *What Companies Can Learn from Cybersecurity Resources in Pittsburgh*, Cyber Security Law Report, (Nov. 11, 2015), available at http://www.klgates.com/files/Publication/db4c329c-0d9a-4d5c-a7f4-004deed4f74a/Presentation/PublicationAttachment/2a35347e-281c-48c3-a3db-3a0ab26c1b38/CSLR-What_Companies_Can_Learn_from_Cybersecurity_Resources_in_Pittsburgh.pdf.

as a reminder that companies should self-evaluate and assess the degree to which they are subject to federal and state laws governing data security, because the current environment suggests stepped-up enforcement activity by regulatory agencies.

U.S. Government Enforcement questions related to this article may be directed to any of the attorneys listed below:

Pittsburgh - Mark A. Rush (mark.rush@klgates.com, +1.412.355.8333

Pittsburgh - Joseph A. Valenti (joseph.valenti@klgates.com, +1.412.355.8398)

Boston - Michael D. Ricciuti (michael.ricciuti@klgates.com, +1.617.951.9094)

Chicago - Clifford C. Histed (clifford.histed@klgates.com, +1.312.807.4448)

Dallas - Brandon N. McCarthy (brandon.mccarthy@klgates.com, +1.214.939.4983)

Harrisburg - Anthony R. Holtzman (anthony.holtzman@klgates.com, +1.717.231.4570)

Los Angeles - Michael J. Quinn (michael.quinn@klgates.com, +1.310.552.5046)

New York - Walter P. Loughlin (walter.loughlin@klgates.com, +1.212.536.4065)

Pittsburgh - Thomas C. Ryan (thomas.ryan@klgates.com, +1.412.355.8335)

Washington, D.C. - Stephen G. Topetzes (stephen.topetzes@klgates.com, +1.202.778.9328)

Authors:

Mark A. Rush
mark.rush@klgates.com
+1.412.355.8333

Thomas C. Ryan
thomas.ryan@klgates.com
+1.412.355.8335

Joseph A. Valenti
joseph.valenti@klgates.com
+1.412.355.8398

Samuel P. Reger
samuel.reger@klgates.com
+1.412.355.6258

Treasury Department Issues Cybersecurity Checklist for Financial Institutions: What Might Apply to Your Financial Services Company?

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates comprises more than 2,000 lawyers globally who practice in fully integrated offices located on five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.