TREASURY DEPARTMENT ISSUES CYBERSECURITY CHECKLIST FOR FINANCIAL INSTITUTIONS: WHAT MIGHT APPLY TO YOUR FINANCIAL SERVICES COMPANY?

Date: 14 December 2015

Government Enforcement/Cyber Law and Cybersecurity Alert

By: 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.

	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.

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

To read the full alert, click here.

Notes:

[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.

[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.

[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).

[19] *See* https://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers.

KEY CONTACTS

MARK A. RUSH
PARTNER

PITTSBURGH, WASHINGTON DC
+1.412.355.8333
MARK.RUSH@KLGATES.COM

THOMAS C. RYAN
PARTNER

PITTSBURGH
+1.412.355.8335
THOMAS.RYAN@KLGATES.COM

