Cybersecurity Regulation and Guidance

by Patti Blenden

It is widely acknowledged that cybercrime poses a significant risk to individuals and entities of all sizes and endeavors. On March 2, 2016, the CFPB instituted its first data security enforcement action, in the form of a consent order against online payment platform Dwolla, Inc., and never declared any evidence of a data breach or evidence of consumer harm. The CFPB enforced never released standards and alleged the company made deceptive customer representations demonstrating its belief there are unarticulated baseline standards of "appropriate" and "reasonable" cybersecurity measures. In the Dwolla consent order, the CFPB did not cite specific regulations, past consent decrees, or government-issued guidance as its basis, but merely cited "industry standards," including requiring encryption and standards issued by the Payment Card Industry (PCI) Security Standards Council. Several recent cybersecurity actions provide framework of what the federal regulators expect financial entities to have including: (1) a written information technology and data security plan, (2) staff data security training, (3) regular risk assessments, (4) appropriate vendor oversight of customer data practices to ensure sufficient protection standards and policies, and (5) encryption of any sensitive data. Review your current cybersecurity programs to identify areas needing additional work. We hope this list of useful guidance documents and statements will assist in organizing your cybersecurity program review.

Resource	Summary of Resource Guidance
Gramm Leach Bliley Act (GLBA) Section 501(b), *"Safeguards Rules"*	The prudential regulators have authority to enforce Section 501(b) information security standards for all covered financial institutions. The CFPB's authority over GLBA privacy provisions does not include Section 501(b).
CFPB's *Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) Examination Procedures*	The CFPB does not have an express cybersecurity mandate or directive, it has enforced cybersecurity expectations use its authority to prevent and penalize unfair, deceptive or abusive practices to include cybersecurity.
FFIEC's Management Booklet, November 2015	The booklet outlines sound information technology (IT) governance principals and how IT risk management relates to enterprise-wide risk management and governance. The updates incorporated the cybersecurity concepts as part of information security with the 2015 release. https://www.ffiec.gov/press/pr111015.htm
FFIEC's *Information Security Booklet*, September 2016	The booklet provides an overview of information security operations, including effective (1) threat identification, assessment, and monitoring and (2) incident identification, assessment and response. It also incorporates cybersecurity concepts, such as threats, controls, and resource requirements for preparedness. https://www.ffiec.gov/%5C/press/pr090916.htm
FFIEC's *Cybersecurity Assessment Tool*, June 2015	The FFIEC developed the Cybersecurity Assessment Tool and implementation tool, including an informative video, to help institutions identify their cybersecurity risks and determine their preparedness. The Tool is a repeatable and metric-based process to assess preparedness over time. https://www.ffiec.gov/cyberassessmenttool.htm
FFIEC's *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement,* November 2014	The FFIEC recommended that financial institutions of all sizes consider participation in the FS-ISAC as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities. https://www.ffiec.gov/press/pr110314.htm
CFPB's *Consumer Protection Principles: CFPB's Vision of Consumer Protection in New Faster Payment Systems,* July 2015	The CFPB outlined principles for protecting consumers as the private sector develops new faster payment systems to ensure any new payment systems are secure, transparent, accessible, and affordable to consumers. The systems should also have robust protections. One principle declares that systems should have strong built-in protections to safeguard against and respond to data breaches. http://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-guiding-principles-for-faster-payment-networks/
CFPB's *Dwolla Consent Order, Payment Processor Deceived Consumers About the Data Security Risks of Using Its Online System*, March 2016	The Consumer Financial Protection Bureau took action against online payment platform Dwolla for deceiving consumers about its data security practices and the safety of its online payment system. As of May 2015, Dwolla had more than 650,000 users and transferred as much as $5 million per day. Despite the CFPB's lack of authority to enforce GLBA's Safeguards Rule, it has interpreted that its UDAAP authority is sufficient to take issue with inaccurate statements such as Dwolla's claims that its data security practices exceeded industry standards, setting "a new precedent for the payments industry." http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/
SEC Cease and Desist Order against Morgan Stanley Smith Barney LLC (MSSB), June 2016	Following a cyber breach involving customer data, the SEC penalized MSSB for failing to adopt written policies and procedures reasonably designed to protect customer records and information under the Safeguards Rule of Regulation S-P. https://www.sec.gov/litigation/admin/2016/34-78021.pdf