PUBLICATION

Someone Needs to Take the Lead on Data Security for Financial Services Industry

May 13, 2016

Cybersecurity and data protection – or more specifically, the lack of it – in the financial services industry present risks for both an institution's consumers and the institution's safety and soundness. The presence of both of these risks has led to multiple regulators attempting to address the problem by testing and bringing enforcement actions. But the question of who has primary supervisory and enforcement authority over these issues remains unanswered. With the increase of data protection complaints and the ever-growing occurrence of data breaches, it is obvious that the financial industry needs clear direction. Without a primary regulator promulgating a new rule or setting a standard for compliance, institutions must look towards multiple agencies to identify their best practices – meaning it's only a matter of time before opposing guidance will be issued as each agency settles into their own approach.

Who should lead the effort, then?

To start, there's the Federal Financial Institutions Examination Council (FFIEC), a formal interagency body already empowered to prescribe uniform principles for the federal examination of financial institutions. Council members include federal regulators from the Federal Reserve, FDIC, CFPB, NCUA and the OCC. The FFIEC has stated that an institution should take a "comprehensive approach to maintain the security and resilience of its technology infrastructure including the establishment of a robust cybersecurity framework," and they recommend establishing "robust governance policies and risk management strategies" along with a recommendation to "commit sufficient resources including expertise and training," and to establish "an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation." This is all great information for financial institutions to adhere to, but we need something more concrete, more direct. Something putting forth necessary, specific controls and processes that an institution can rely on to know they are compliant in managing both consumer and prudential risk adequately, in a manner that will be deemed compliant upon exam by either regulator.

Last December the FFEIC published a notice and request for comment on a proposed cybersecurity tool they described as an assessment tool that "allows a financial institution to identify its inherent cyber risk profile based on the financial institution's technologies and connection types, delivery channels, online/mobile products and technology services that it offers to its customers, its organizational characteristics, and the cyber threats it is likely to face." Again, this is a great start to standardization for consumer and fiduciary regulators, but if you look closely you will see that only the OCC, FDIC, NCUA and Federal Reserve are listed as the involved agencies. Where is the CFPB? It is also worth noting that all the risk defined in this notice uses language such as, "Absent immediate attention to these rapidly increasing threats, financial institutions and the financial sector as a whole are at risk." Which may mean that the CFPB will take a different approach and not utilize this same tool, as the language seems directed at the safety and soundness of an institution.

Not surprisingly, the CFPB entered the data protection space with an enforcement action. In a press release announcing the action, the CFPB cited its authority under UDAAP to bring a claim against an entity called Dwolla, Inc., explaining, "rather than setting 'a new precedent for the payments industry' as asserted, Dwolla's data security practices in fact fell far short of its claims. Such ***deception*** about security and security practices is illegal." One would think that it was the *statements* that were illegal, not the *practices*, but read through the

consent order and it's obvious that the CFPB was focused on Dwolla's policies and procedures – not their marketing material. The consent order quickly disposes of the marketing violations by mentioning that Dwolla is enjoined from "misrepresenting, or assisting others in misrepresenting, expressly or by implication, the data-security practices implemented," then immediately moves onto a lengthy discussion on how they must change their data protection *procedures*. The order fined Dwolla a mere $100,000, but went on to require the company to (1) adopt and implement reasonable and appropriate data-security measures to protect consumers' personal information; (2) establish, implement and maintain a written, comprehensive data security plan that is reasonably designed to protect the confidentiality, integrity and availability of sensitive consumer information; (3) adopt and implement reasonable and appropriate data-security policies and procedures; (4) designate a qualified person to coordinate and be accountable for the data-security program; (5) conduct data-security risk assessments twice annually and evaluate and adjust the data security program as needed; (6) conduct regular, mandatory employee training; (7) develop, implement and update, as required, security patches to fix any security vulnerabilities identified in any web or mobile application; and (8) develop, implement and maintain an appropriate method of customer identity authentication. One has to wonder what might happen if the Bureau tries this on a larger scale, attempting to levy a fine in the millions – will an institution challenge the CFPB's authority in the space? And is this order the CFPB's attempt to position itself as a primary authority on data protection and cybersecurity?

This type of uncertainty will increase risks and compliance costs for the financial services industry and needs to be addressed as soon as possible. For now, institutions must monitor the activity across all regulators of their particular segment of the industry to ensure compliance. If you have any questions or concerns about your cybersecurity protocols or data privacy policies, please reach out to a member of Baker Donelson's Privacy and Information Security team.