Do your company's cybersecurity practices deceive consumers?

March 3, 2016

Direct guidance on cybersecurity by the CFPB

Not a day goes by without breaking news of a cybersecurity breach. Indeed, thoughts of a system hack keep many executives up at night. Small- and medium-sized businesses often fear that they do not have the robust resources or staff to adequately handle these threats.

The Consumer Financial Protection Bureau (CFPB) has now weighed in: See, Consent Order, In the Matter of Dwolla, Inc., 2016 CFPB-0007 (March 2, 2016). This consent order makes two things clear: first, if you provide a product or service to consumers that involves money or private information, or you are an affiliate or vendor for such a business, there is no excuse for not having a functional data security plan; and second, such a plan need only be reasonable and appropriate for the business' size and complexity, which is good news for many.

Of particular importance is the fact that the CFPB has now used its ultimate weapon — Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) — as a tool to ensure that consumer-facing companies will adopt effective security protocols. This should cause companies to take a very close look at security precautions and what they are representing to consumers about the protection of non-public information.

False representations of data security measures amount to deceptive activity and are subject to sanction. In Dwolla, Inc., the company represented to consumers that their information and money would be protected by security precautions that met or exceeded industry standards — a statement that was not true. The ensuing consent order resulted in a $100,000 fine, consumer refunds, and the imposition of onerous compliance, monitoring and recordkeeping requirements.

The corollary to this proposition may be the same. The failure to disclose that your organization does not adequately maintain appropriate security precautions may also be considered deceptive or abusive conduct, given that consumers are often invited to share information through electronic means and a reasonable consumer could assume that he or she is protected by appropriate safeguards as mandated by other areas of law. Bottom line: if a reasonable consumer is unaware that sensitive information is not protected, the consumer probably has not been informed of such by the organization. That failure may amount to deceptive or abusive inaction.

Some of Dwolla's consumer representations may have sounded like simple puffery, but the effect was a reasonable presumption that its platform was secure. The company promised consumers that it employed reasonable and appropriate measures to protect consumer data from unauthorized access. Dwolla represented that the company's transactions were "safer [than credit cards] and less of a liability for both consumers and merchants," its data-security practices exceeded industry standards, it stored consumer information "in a bank-level hosting and security environment," it encrypted data "utilizing the same standards required by the federal government" through "industry standard encryption technology," its website and mobile applications used the latest encryption and secure connections, and it was "PCI compliant."

As alleged in the consent order, these representations were not true. Consumers had been deceived. (Score a large fine for the CFPB and refunds to affected consumers.) By using UDAAP as a tool to enforce data security, the bureau has sent a clear

message: if a company falsely advertises that it protects non-public information or financial transactions, such representations are considered deceptive acts and constitute a violation of the Consumer Financial Protection Act.

CFPB's cybersecurity guidelines

The CFPB is often accused of creating rules through enforcement actions. The Dwolla consent order is no exception and teaches us plenty about cybersecurity guidelines. The CFPB expects any business that offers or provides consumer financial products or services to consumers to do the following:

1. Adopt and implement data-security policies and procedures reasonable and appropriate for the organization.
2. Implement appropriate measures to identify reasonably foreseeable security risks.
3. Ensure that employees who have access to or handle consumer information receive adequate training and guidance about security risks.
4. Use encryption technologies to properly safeguard sensitive consumer information.
5. Practice secure software development, particularly with regard to consumer-facing applications.

Based on the requirements imposed on Dwolla in the consent order, comprehensive data-security policies and procedures should include the following:

- Reasonable and appropriate measures governing the collection, maintenance or storage of consumers' personal information.
- A written data-security plan to govern the collection, maintenance or storage of consumers' personal information. This plan must contain administrative, technical and physical safeguards appropriate to a business' size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected about consumers, as well as adequate and regular risk assessments to identify reasonably foreseeable internal and external risks to consumers' personal information or to assess the safeguards in place to control those risks.
- Data-security training for staff on their responsibilities for handling and protecting the security of consumers' personal information, including education about the dangers of phishing.
- Protections against storing or transmitting consumers' personal information (names, addresses, SSNs, PINS, bank information, and other non-public documents or data) without encrypting that data.
- Regular data-security risk assessments of each area of relevant operation to identify internal and external risks to the security, confidentiality and integrity of a network, systems or apps; of sensitive consumer information stored by a company; and of the sufficiency of any safeguards in place to control these risks. (Dwolla is required to conduct this assessment twice annually.)
- Develop, implement and update, as required, security patches to fix any security vulnerabilities that may become identified.
- Develop, implement and maintain an appropriate method of customer identity authentication prior to the transaction of business or use of sensitive information.
- Develop, implement and maintain reasonable procedures for the selection and retention of service providers capable of maintaining security practices and require those providers, by contract, to implement and maintain appropriate safeguards.
- Designation of a qualified person to coordinate and be accountable for the data-security program.
- Obtain an annual data-security audit from an independent, qualified third-party using procedures and standards generally accepted in the applicable industry.

From Dwolla, we learn the following:

1. All consumer-facing businesses providing or offering to provide consumer financial products or services, along with affiliates and vendors for such businesses, need a comprehensive data-security plan that is tested and assessed often and updated as needed.

2. Consumers need to be put on notice as to whether appropriate data-security safeguards are employed by a business or if there are weaknesses.
3. An effective system must be employed to ensure appropriate customer identification procedures are used.
4. Consumer-facing businesses must employ data encryption when storing or transmitting non-public consumer information.
5. Third-party vendors must adopt appropriate measures as well, and vendor agreements must create oversight to ensure this obligation is met.
6. Employee education and training is paramount, including specific policy awareness and general security precautions to prevent breaches, such as phishing attacks.
7. Failure may not just be a breach of federal and state privacy regulations ,but may amount to deception and abuse of consumers.

As previously noted, there is good news within this guidance. This is not a "one size fits all" proposition. The scope and cost of a plan will vary by the size and complexity of an affected business. "[T]he plan must contain administrative, technical, and physical safeguards appropriate to [a company's] size and complexity, the nature and scope of [its] activities, and the sensitivity of the personal information collected about consumers" (emphasis added). Fortunately, a small independent organization will not be held to the same standards and complexity as that of a large multi-national institution.

Authors