KPMG

CLIENT ALERT

CFPB Enforcement Action - Data Security Practices and Protection of Consumer Personal Information

The Consumer Financial Protection Bureau (CFPB or Bureau) recently announced that it had settled an enforcement action against an online payment system (the Respondent) to address the CFPB's findings the Respondent deceived customers about its data security practices and the safety of its payment network (Consent Order).[1] The CFPB did not allege that any breach to the Respondent's network had occurred or that any consumer had suffered financial harm. The Respondent agreed to pay a civil money penalty of $100,000 and to take steps to strengthen its data security practices.

Things to Consider. **This action is the CFPB's first with regard to data security**, and made all the more notable because the "enumerated consumer laws" for which the CFPB has enforcement authority do not include the data security provisions of the *Gramm-Leach-Bliley Act* (GLBA). To date, the Federal Trade Commission (FTC) has taken the primary enforcement role on data security issues, commonly citing violations of the *FTC Act* provisions prohibiting unfair and deceptive acts or practices (UDAP). The CFPB states that its current action "builds off advances made by several other agencies" but relies on its own broad authority to protect consumers from financial harm resulting from financial companies' unfair, deceptive, or abusive acts or practices (UDAAP). However, **the requirements of the enforcement action are similar to steps outlined in previous FTC actions,** including requirements to establish a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of consumer information, and to conduct annual information security audits that conform to the Payment Card Industry (PCI) Data Security Standards (as established by the PCI Security Standards Council).

The Respondent is part of the growing number of digital payment companies and other nonbank, non-traditional financial services firms that operate under **the "FinTech" umbrella**. As a nonbank provider of consumer financial products and services, the CFPB deems it to be a **"covered person"** subject to the Bureau's authority. To this point, the CFPB's UDAAP authority has proven to be a formidable tool for reaching into existing and emerging nonbank financial services firms that generally have not been subject to supervision at the federal level. In announcing the Consent Order, the CFPB quoted Director Richard Cordray as stating, "With data breaches becoming commonplace and more consumers using these online payment systems, the risk to consumers is growing. It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices."

Bank and nonbank financial services firms that handle sensitive consumer personal information, including large banks under the supervision of the CFPB and new start-up financial technology firms, **should anticipate that the Bureau will continue to look closely at data security surrounding consumer personal information**, as well as other GLBA-related provisions, such as privacy, even when there may be no evidence of consumer harm. In the absence of specific guidance, firms are encouraged to consider the required actions outlined in the Consent Order as a proxy for "best practices" and incorporate them, as appropriate, into their own data security programs. Such an approach is consistent with the CFPB's intent in publicly releasing orders, as suggested by Director Cordray in prepared remarks before the Consumer Bankers Association on March 9, 2016, where he said: "These orders provide detailed guidance for compliance officers across the marketplace about how they should regard similar practices at their own institutions. If the same problems exist in their day-to-day operations, they should look closely at their processes and clean up whatever is not being handled appropriately. Indeed, it would be 'compliance malpractice' for executives not to take

[1] See CFPB press statement March 2, 2016, available at: http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/

careful bearings from the contents of these orders about how to comply with the law and treat consumers fairly." In simple terms, this is a "fair warning."

The Consent Order in summary: The Respondent operates an online payment network that allows consumers to register, and set up, an account with the Respondent (Registered Account) and to use that account to transfer funds to another consumer's Registered Account. The transferred funds may be sourced from a consumer's Registered Account or from a personal bank account linked to the Registered Account. Consumers must provide the Respondent with information that the Respondent collects and stores, including: name, address, date of birth, telephone number, Social Security Number (SSN), bank account number, bank routing number, user name, password, and unique four-digit PIN.

The CFPB alleges the Respondent represented to consumers that it employed reasonable and appropriate measures to protect consumer information from unauthorized access and that its network and transactions were "safe" and "secure." Further, on its Web site and in direct communication with consumers, the Respondent made representations that its data security practices "met or exceeded industry standards," including statements that it stored consumer information "in a bank-level hosting and security environment;" was compliant with the security standards of the PCI Security Standards Council; and that it encrypted "all sensitive information that is on its servers," including "data in transit and at rest." The CFPB alleges that, in fact, these were misrepresentations and that, in practice, the Respondent failed to: adopt and implement reasonable and appropriate data-security policies and procedures; conduct regular risk assessments; or ensure that employees received adequate training about security risks. In addition, the CFPB alleges the Respondent did not use encryption technologies to properly safeguard sensitive consumer information or practice secure software development.

The CFPB alleges the Respondent's misrepresentations would likely mislead a reasonable consumer into believing that it had reasonable and appropriate data security practices, and further, would likely affect a consumer's choice or conduct regarding whether to create a Registered Account with the Respondent. Accordingly, the CFPB found the Respondent's actions to constitute deceptive acts or practices in violation of the *Consumer Financial Protection Act*. The CFPB did not allege that any breach to the Respondent's network had occurred or that any consumer had suffered financial harm. As of May 2015, the Respondent had more than 650,000 Registered Account holders and had transferred as much as $5 million per day.

The Respondent agreed to the Consent Order without admitting or denying any of the CFPB's findings of fact or conclusions of law. In so doing, it agreed to pay a civil money penalty of $100,000 and to take steps to strengthen its data security practices, including:

- Establishing, implementing, and maintaining a written, comprehensive data security plan;
- Designating a qualified person to coordinate and be accountable for the data security program;
- Conducting data security risk assessments twice annually;
- Conducting regular, mandatory employee training about security risks;
- Developing and implementing security patches to fix security vulnerabilities;
- Developing, implementing, and maintaining reasonable procedures to select and retain service providers capable of maintaining securities practices consistent with the Consent Order and to require such practices by contract; and
- Obtaining an annual data security audit from an independent, qualified third-party.

Industry Updates. As noted earlier, the FTC has enforcement authority for the data security provisions of the GLBA and could have brought a similar case against the Respondent, alleging violations of the GLBA or its UDAP authority under Section 5 of the FTC Act. The FTC has been active with regard to data security for quite a while, citing organizations for failing to design or to implement an appropriately comprehensive privacy or data security program in at least 47 cases

since 2002.[2] Most recently, the FTC announced that it reached a settlement with a corporate entity regarding allegations that the company's poor data security practices unfairly led to the exposure of its customers' payment card information in multiple data breaches.[3] The FTC is expected to remain active with regard to data security practices, and nonbank firms should anticipate that the FTC and CFPB could coordinate their efforts in much the same way they have done for debt collection. On March 7, 2016, the FTC announced that it intends to study the policies, practices, and procedures of companies that audit the compliance of others with the PCI Data Security Standards, and the role such audits play in protecting consumers' information and privacy.[4] The FTC states that it issued orders to nine companies requesting information on how they conduct assessments to measure a company's compliance with the PCI Data Security Standards, examples of such assessments, and information on additional services they provide, including forensic audits.

Finally, U.S. banks are beginning to enter the developing FinTech payments markets. On March 9, 2016, new reports indicated that several large U.S. banks are poised to jointly launch and participate in a payment system that will permit member bank customers to transfer funds in real time through mobile applications to customers of other member banks participating in that payment system.[5] The banks reportedly expect this new system, currently called "clearXchange," to have an advantage over other nonbank payment systems, such as the Respondent, because of the speed at which the banks will be able to transfer funds to one another, while the nonbank payment providers are dependent on the banks to transfer funds. This imbalance may change, however, as the U.S. moves toward "faster payments" initiatives through the Automated Clearing House Network. Financial institutions should take note that as the speed of payments transactions increases, so too will the CFPB's interest in protecting consumers and the security of their personal information. In addition, other regulators are interested in the development of the FinTech sector and, like the CFPB, have been watching closely. In particular, the Office of the Comptroller of the Currency (OCC) recently indicated it will soon release a report that looks at relationships between banks and FinTech firms and also identifies risks and opportunities for innovation in the federal banking system. Though not specifically stated, data security practices and consumer privacy will likely factor into the OCC's perspective.

For additional information, please contact:

Amy Matsuo
Principal and National Lead
Financial Services Regulatory Risk Practice
T: 919-380-1509
E: amatsuo@kpmg.com

Carolyn Greathouse
Principal
Financial Services Regulatory Risk
Enterprise and Consumer Compliance
T: 314-244-4096
E: cgreathouse@kpmg.com

Author: Karen Staines, Director, Americas Financial Services Regulatory Center of Excellence, kstaines@kpmg.com

The Americas Financial Services Regulatory CoE is based in Washington, DC and comprised of key industry practitioners and regulatory advisers from across KPMG's global network.

[2] Bailin, Patricia, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, available at https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf.
[3] See FTC press statement December 9, 2015, available at: https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment.
[4] See FTC press statement March 7, 2016, available at: https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing
[5] Henry, David. *Big U.S. banks to take one tech rivals with instant payments*, March 9, 2016, Reuters.