March 11, 2016

Consumer Financial Protection Bureau Brings Its First Data Security Enforcement Action

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
David T. Cohen

On March 2, the Consumer Financial Protection Bureau ("CFPB") issued its first ever consent order in a data security matter. According to the order, Dwolla, Inc. settled allegations that it misrepresented that the company had reasonable and appropriate data security practices when, according to the CFPB, its practices failed to employ reasonable and appropriate measures to protect user data from unauthorized access. While Dwolla did not admit or deny any allegation, the consent order requires Dwolla to pay a $100,000 civil penalty and take other specified actions for a five-year period, such as conducting semi-annual data security risk assessments and developing, with direct input from the board of directors, a compliance plan.

The CFPB began operating in 2011 after the Dodd–Frank Wall Street Reform and Consumer Protection Act gave the agency authority to regulate consumer financial products and services under the federal consumer financial laws. The action against Dwolla demonstrates that this relatively new agency is going to take a strong position in the cybersecurity realm and pursue companies within its jurisdiction for allegedly making deceptive statements about data security, even without an actual compromise of consumer information. The agency's decision to proceed against a start-up payment processor also underscores the wide variety of consumer financial companies that could face an enforcement action by the CFPB.

According to the consent order, Dwolla is a payment processing company that transfers as much as $5 million per day for its 650,000 members. Members transfer money from either a Dwolla account or a personal bank account linked to the member's Dwolla account. The consent order states that, when a customer establishes a Dwolla account, Dwolla stores the customer's name, address, date of birth, telephone number, and social security number, and if the customer links the account to a personal bank account, Dwolla also stores a bank account number, routing number, and a username, password, and pin.

The CFPB alleges that Dwolla made representations that its data security practices "exceed[ed]" and "surpass[ed]" industry standards, allegedly claiming, for example, that the company "sets a new precedent for the industry for safety and security." Dwolla also allegedly made multiple statements related to its encryption technology, including stating that the company encrypts "all sensitive information that exists on its servers" and is compliant with Payment Card Industry ("PCI") standards.

The CFPB concluded that these statements constituted deceptive acts or practices in violation of the Consumer Financial Protection Act ("CFPA"). According to the CFPB, these statements were false or misleading because Dwolla "failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access." In particular, the order asserts that Dwolla:

- stored, transmitted, or caused to be transmitted personal information such as names, social security numbers, and bank account information without encrypting that data;
- was not PCI compliant;
- did not have reasonable and appropriate data security policies and procedures;

- until 2014, did not conduct comprehensive risk assessments and inadequately trained its employees;
- had an inadequate software development operation; and
- stored sensitive customer information on applications that were not tested for security before being released to the public.

Notably, however, the CFPB does not allege that any third parties gained unauthorized access (or even attempted to gain unauthorized access) to any of the personal information that it claims Dwolla failed to adequately protect.

The negotiated consent order, which will be effective for five years, requires that Dwolla refrain from further misrepresentations regarding data security, adopt a comprehensive data security plan, and implement related policies and procedures, including designating an employee to be accountable for the data security program. These requirements resemble those typically imposed by consent orders entered into by the Federal Trade Commission ("FTC"), which has thus far been the federal agency most active in the data security space. But the CFPB order also imposes several requirements that go above and beyond what the FTC typically imposes. For example, while the FTC frequently requires companies to conduct data security risk assessments, the CFPB order requires that Dwolla conduct such assessments twice annually. Likewise, while the FTC frequently requires third-party data security audits, it typically requires only that they be conducted biennially; the CFPB order requires that such audits be completed once per year. Even more notably, the CFPB order imposes specific requirements on Dwolla's board of directors. It requires that the report generated by the third-party data security audit be provided to the board of directors, that the board of directors develop a compliance plan to correct identified deficiencies and implement recommendations, and that the audit report and the board's plan be submitted to the CFPB. It further provides that the CFPB can accept or revise the plan. Additionally, pursuant to the consent order, the board must review and assume ultimate responsibility for all submissions made to the CFPB. Finally, as noted above, the order requires Dwolla to pay a $100,000 civil penalty.

While many of the requirements imposed under the consent order will require significant attention by Dwolla and its board of directors, it is important to note that, unlike FTC consent orders, which are typically for a period of twenty years, this order will be in force for only five years. Whether the CFPB believes that immediate, intense data security measures are the best remedy for alleged data security violations remains to be seen. But what is clear is that this relatively new agency believes it need not wait for a data security incident to occur before bringing an enforcement action against a company within its jurisdiction – even a start-up – that it believes is making deceptive, material representations about its data security practices.

For more information regarding the settlement between the CFPB and Dwolla or to discuss data security practices generally, please feel free to contact Heather Egan Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.