Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 20 / MARCH 11, 2016

EXPERT ANALYSIS

Is the CFPB the New Cop on the Data Security Beat?

By Nathan D. Taylor, Esq., and Angela E. Kleine, Esq.
Morrison & Foerster

On March 2, 2016, the Consumer Financial Protection Bureau ("CFPB") broke new ground (at least for the CFPB) when it released a consent order against Dwolla, Inc. ("Dwolla"), an online payment platform, regarding data security. While in many respects the data security "message" sent by the CFPB is not a new one (e.g., companies must live up to their data security promises), the consent order is particularly noteworthy because it represents the CFPB's first formal foray into the data security area, an area where there has been some question as to the scope of the CFPB's authority.

This consent order clearly indicates the CFPB's belief that the Consumer Financial Protection Act ("CFPA") provides the agency with the authority to police data security practices in the financial space, utilizing its unfair, deceptive or abusive acts or practices ("UDAAP") authority.

THE CONSENT ORDER

In the consent order, the CFPB alleges that Dwolla made false representations to consumers regarding its data security practices, in violation of the CFPA. In this regard, Dwolla operates a payment application that allows its customers to transfer funds to third parties from funds stored in a Dwolla account or in a linked bank account. In order to provide this service, Dwolla allegedly collects a variety of information from its customers, including name, contact information, Social Security number and bank account information.

At the heart of the matter, the CFPB alleges that Dwolla represented to consumers that Dwolla maintained "reasonable and appropriate" data security safeguards, when in fact the company did not.

In this regard, the consent order lists a litany of alleged misrepresentations by Dwolla. For example, the CFPB alleges that Dwolla represented that its network and transactions were "safe" and "secure," its data security practices "exceed" or "surpass" industry standards and the company "sets a new precedent for the industry for safety and security."

Dwolla allegedly also stated that its data hosting and security environment were "bank-level" and that it encrypted consumer data using federal standards for encryption. The alleged representations do not end there.

Dwolla allegedly told consumers that "100% of [their] info is encrypted and stored securely" and that the company encrypted all "sensitive information that exists on its servers."

If accurate, Dwolla raised the bar for itself to a level that no company likely could meet. In fact, these representations are not only aggressive in scope, but also not typical for most companies (particularly since state Attorneys General frequently bring deception claims regarding representations made by companies about their data security practices).

Dwolla is required to pay a civil money penalty of $100,000 and take a wide variety of steps to improve its security practices.

The CFPB alleges a number of ways in which Dwolla failed to live up to these promises. For example, the CFPB alleges that Dwolla did not adopt and implement reasonable data security policies and procedures, conduct risk assessments or train its employees regarding security.

The CFPB's allegations, however, are not limited to administrative failings. For example, the CFPB alleges that Dwolla did not in fact use encryption to safeguard sensitive information and did not "practice secure software development."

Putting the various allegations together, the CFPB concludes that Dwolla deceived its customers because the representations that the company made regarding its data security practices (which the CFPB found to be material) were "likely to mislead a reasonable consumer into believing that Dwolla had incorporated reasonable and appropriate data-security practices when it had not."

As part of the order, Dwolla is required to pay a civil money penalty of $100,000 and take a wide variety of steps to improve its security practices, in addition to being prohibited from making misrepresentations regarding its security practices. For example, Dwolla will be required to maintain a written information security program, conduct semi-annual risk assessments and conduct regular and mandatory employee training.

Dwolla also will be required to patch identified security vulnerabilities in its applications, implement an appropriate method of customer identity authentication at registration and before effecting a funds transfer, implement reasonable procedures for the selection and retention of service providers and obtain an independent annual data security audit.

Many of these provisions represent existing obligations that likely apply to Dwolla under the Gramm-Leach-Bliley Act ("GLBA") data security rules and state safeguards laws.

TAKEAWAYS

While the civil money penalty assessed in this case is quite small given recent CFPB actions, this consent order is noteworthy for a number of reasons.

First and foremost is the fact that the CFPB has placed a very firm stake in the ground that it believes its UDAAP authority extends to data security. As noted above, this is an issue that was not entirely free from doubt.

Under the CFPA, rulewriting, supervision and enforcement of a wide variety of federal consumer financial laws were transferred from various agencies to the CFPB. These "enumerated consumer laws" include, for example, the privacy provisions of the GLBA and the Fair Credit Reporting Act ("FCRA").

Congress, however, specifically did not transfer to the CFPB the GLBA data security requirements, nor the red flags and credit report information disposal requirements of the FCRA. That is, Congress specifically carved out pre-existing data security standards of federal consumer financial laws from the scope of the CFPB's authority.

Despite this "carveout" (and its implied Congressional intent), the CFPA authorizes the CFPB to prevent a covered person from "committing or engaging in an unfair, deceptive, or abusive act or practice ... in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service."

From the start, the CFPB has used this powerful new UDAAP authority to expand its enforcement efforts beyond the "enumerated" laws transferred to the agency. With this consent order, the CFPB has continued the trend, bringing an enforcement action focused broadly on alleged misrepresentations about data security and avoiding any reference to the GLBA.

While the CFPB, in drafting the order, appears cognizant of the GLBA and other data security standards, the order itself is not based on the GLBA data security standards or a failure by Dwolla to comply with such standards.

While it is not clear whether the CFPB brought this action after consultation or coordination with the Federal Trade Commission ("FTC"), the FTC could have brought the same action alleging that

Dwolla's security practices failed to comply with the FTC's GLBA safeguards rule or that Dwolla's representations regarding its security were deceptive, in violation of the prohibition on unfair or deceptive acts or practices in interstate commerce under Section 5 of the FTC Act. However, the CFPB apparently beat the FTC to the punch.

As the "FinTech" area has continued to evolve and more non-traditional entrants to the financial and payments space have emerged, one question that invariably arises is whether the CFPB has authority over the practices of such companies (or the extent of that authority).

In the consent order, the CFPB finds that Dwolla is a "covered person" under the CFPA and subject to the CFPB's broad enforcement authority. As a result, the consent order may be a signal that the CFPB is a new cop on the beat not only for data security, but also with respect to emerging and new financial activities conducted by non-traditional financial institutions.

For example, in the CFPB's press release, Director Richard Cordray highlighted that "[c]onsumers entrust digital payment companies with significant amounts of sensitive personal information," and as risks to consumers continue to grow, "[i]t is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices."

In addition, while the consent order does not require Dwolla to encrypt specific data elements, the order could be read to imply that the CFPB believes that Dwolla should have encrypted data elements that are not typically considered sensitive.

For example, in its findings, the CFPB concludes that Dwolla stored and transmitted the following data without encrypting the data: first and last names, mailing addresses, Dwolla 4-digit PINS, Social Security numbers, bank account information and digital images of driver's licenses, Social Security cards and utility bills.

Leaving aside best practices, there are only limited encryption requirements under U.S. law. For example, the Massachusetts data security regulations and the Nevada safeguards laws require the encryption of a consumer's name and, for example, Social Security number, driver's license number and financial account number in certain contexts.

Nonetheless, there are no U.S. laws (or even best practices) that require the encryption of, for example, name and contact information. It is possible that the CFPB included this finding to support the proposition that Dwolla's statement that it encrypted "100%" of consumer information was deceptive because Dwolla did not encrypt many types of data, such as the listed data elements.

However, if the CFPB continues down this data security path, future orders should be closely scrutinized for signals regarding the CFPB's expectations regarding encryption.

The CFPB has placed a very firm stake in the ground that it believes its UDAAP authority extends to data security.

Nathan D. Taylor (L) is a partner in the Washington office of **Morrison & Foerster**, where he provides practical advice to help companies enhance their cybersecurity posture. His practice has a special emphasis on federal and state privacy laws and regulations impacting financial institutions. He can be reached at ndtaylor@mofo.com. **Angela E. Kleine** (R) is a partner in the firm's San Francisco office, where she is a member of the financial services litigation group. She focuses on complex civil litigation and enforcement. She can be reached at akleine@mofo.com.