The US Consumer Financial Protection Bureau's Dwolla consent order

On 2 March 2016, the Consumer Financial Protection Bureau ('CFPB') brought its first ever data security enforcement action against online payment platform Dwolla Inc. The data security 'expectations' communicated by the CFPB's order are consistent with past enforcement actions brought by other federal and state regulators.

This 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 a historical question as to the scope of the CFPB's authority. In this regard, this consent order 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, utilising its unfair, deceptive or abusive acts or practices ('UDAAP') authority. It is possible that the CFPB's order should not be read to indicate that the CFPB is focused on data security specifically. For example, it is possible that the CFPB was attempting to address perceived 'regulatory arbitrage' in the FinTech space or to otherwise police a case involving alleged blatant deception. Nonetheless, much uncertainty remains, including whether the CFPB is a new cop on the now crowded data security beat.

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. Dwolla operates a payment application that allows its customers to transfer funds to third parties from funds stored in a Dwolla account or transferred from a linked bank account. In order to provide this service, Dwolla allegedly collects a variety of information from its customers, including name, contact 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 the CFPB concluded that the company did not. 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 made by Dwolla seemingly go on and on. For example, Dwolla allegedly also 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.'

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, were not limited to administrative failings. 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 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 monetary penalty of $100,000 and take 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 programme, conduct semi-annual risk assessments and conduct regular, mandatory employee training. Dwolla is also required to patch identified security vulnerabilities in its applications, implement an appropriate method of customer identity authentication at registration and before 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 as a financial institution under the Gramm-Leach-Bliley Act ('GLBA') data security rules and state safeguards laws.

The implications

While the civil money penalty assessed in this case is quite small given recent CFPB actions, this consent order is nevertheless noteworthy. In particular, the CFPB has placed a very firm stake in the ground that it believes its UDAAP authority extends to data security. This is an issue that is 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. Congress, however, specifically carved out pre-existing data security standards of federal consumer financial laws from the scope of the CFPB's authority, such as the GLBA data security requirements.

Despite this 'carve out,' the CFPA authorises 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 its powerful UDAAP authority to expand its supervisory and enforcement efforts beyond the 'enumerated' laws transferred to the agency. With this consent order, the CFPB has continued that trend, bringing an enforcement action focused broadly on alleged misrepresentations about data security. While the CFPB, in drafting the order, appears cognisant of the GLBA and other data security standards, the order itself is not based on the GLBA standards or a failure by Dwolla to comply with such standards. Although 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 general 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.

It is possible that this order simply represents the CFPB sending a signal to the market that financial institutions must "deliver on [their] promises" to consumers about security, as indicated by Director Cordray discussing the Dwolla order in April before the Senate Banking Committee. While it is common for financial institutions to make public statements about their security in, for example, their GLBA privacy notices and privacy policies, financial institutions generally make only limited statements about the extent of that security, such as "we use security measures to protect data that comply with applicable law." Dwolla, however, seemingly was tripping over itself to tout its data security practices and to distinguish those practices as cutting edge. In fact, the CFPB may have believed not only that Dwolla misrepresented its security, but also that Dwolla intended to deceive consumers. Regardless, the extent and scope of Dwolla's alleged representations are so dramatic that Dwolla raised the bar for itself to a level that virtually no company could meet.

It is also possible that the CFPB pursued this action not because it has a focus on data security, but because the CFPB is trying to rein in the emerging 'FinTech' area. As the FinTech area has continued to evolve and more non-traditional entrants to the financial and payments space have emerged, one question that arises is whether the CFPB has authority over the practices of such companies. 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 signals that the CFPB is taking an active oversight role in this developing area. In fact, Director Cordray's testimony before the Senate Banking Committee supports this view. Director Cordray highlighted that if a company tells consumers that it will handle data security in a specific way, consumers will gain confidence from these statements and want to do business with the company. Director Corday pointed out that if such a company is actually deceiving consumers, it is getting an "unfair advantage" over its competitors. Quite succinctly, Director Cordray indicated that the CFPB believes it is not appropriate for "FinTech start-ups" to get an advantage in the marketplace because they are "arbitraging the regulatory system."

Even though the Dwolla order can be characterised as a deception case or as having a FinTech focus, uncertainty abounds. Regardless of the CFPB's rationale for the order or the extent of the signal that it intended to send to the FinTech or broader marketplace, it seems unlikely that the CFPB will put the data security 'genie' back in the bottle. That is, it is hard to imagine that the CFPB will not pursue similar enforcement actions in the future. It is not clear, however, whether the CFPB would bring an action against a company with a mature and well-established information security programme and that uses discretion when making public statements about its data security. It seems unlikely in the short term that the CFPB would bring a more nuanced case that is not focused on deception, but that takes the position that a failure to implement specific security controls is unfair to consumers. Nonetheless, it is important to be cognisant of the possibility that as the CFPB matures it will invest resources in developing security and information technology expertise, similar to, for example, the federal banking agencies. As a result, regardless of one's view of the CFPB's rationale for the order, banks and other 'traditional' financial institutions should closely follow CFPB developments in the data security space and be mindful of the fact that a new regulator may soon scrutinise their data security practices.

Nathan D. Taylor Partner
Morrison & Foerster LLP, Washington DC
ndtaylor@mofo.com