SQUIRE PATTON BOGGS

Another Cop on the Data Privacy Enforcement Beat – The Consumer Financial Protection Bureau Issues Its First Data Security and Privacy Enforcement Action

On March 2, 2016, the Consumer Financial Protection Bureau (CFPB) assessed a US$100,000 penalty against Dwolla, Inc. (Dwolla), in the CFPB's first data security enforcement action. The CFPB thus became the latest Federal agency to take action against a company for inadequate protection of sensitive personal information gathered online. The Dwolla Consent Order addresses both advertising and representations made to the public, as well as internal protection and training relating to data security.

This CFPB action sends a clear message that a company's claims about its data security measures must be accurate, and that any company handling personal consumer data needs to have reasonable and adequate data security measures. The fact that no data breach or other public incident precipitated this action is a reminder that data security measures, and staff training, need to be periodically tested and evaluated. Entities subject to CFPB supervision should take careful note of the broad implications of this Order, which appears to open a significant additional area of inquiry in CFPB examinations.

Dwolla is an online payment processing company that competes with PayPal and other online payment networks. As of May 2015, Dwolla had approximately 653,000 members and transferred as much as US$5 million per day. The CFPB found that Dwolla violated Sections 1031(a) and 1036(a)(1) of the Consumer Financial Protection Act of 2010 (CFPA), which prohibit "unfair, deceptive, or abusive" practices. Among the actions cited as deceptive: claims on the Dwolla website and to consumers that its data security practices "exceed" or "surpass" industry standards, that "100% of [consumer] info is encrypted and stored securely," and that Dwolla's data security measures comply with Payment Card Industry Security Standards.

The Consent Order, without citing any data breach or consumer complaint, asserted that Dwolla's claims misrepresented the company's actual practices and contradicted its privacy policies. As a result, the Consent Order asserts, the company's actions were "likely to mislead a reasonable consumer into believing that Dwolla had incorporated reasonable and appropriate data-security practices when it had not." The CFPB further asserted that the "representations were material because they were likely to affect a consumer's choice or conduct regarding whether to become a member of Dwolla's network." The Consent Order also cited Dwolla for lacking sufficient training of its staff, and for not ensuring that privacy and data security measures were adequately incorporated in mobile applications offered to consumers.

In a blog posting following the CFPB order, Dwolla claimed that it "has not detected any evidence or indicators of a data breach [or] received a notification or complaint of such an event." While Dwolla no doubt argued that point to the CFPB, the CFPB's legal standard – like the Federal Trade Commission's – does not require a showing of actual harm to any consumer; rather the standard is whether the acts and practices are "likely" to mislead or deceive a consumer.

Interestingly, the Consent Order does not just enjoin Dwolla from future misrepresentations, but goes beyond that to affirmatively require that the company: (1) "adopt and implement reasonable and appropriate data-security measures to protect consumers' personal information on its computer networks and applications;" (2) "establish, implement, and maintain a written, comprehensive data-security plan;" (3) "designate a qualified person to coordinate and be accountable for the data-security program;" (4) "conduct data-security risk assessments twice annually of each area of relevant operation to identify internal and external risks to the security, confidentiality, and integrity of Respondent's network, systems, or apps;" and (5) "conduct regular, mandatory employee training," to name a few.

The massive amounts of data collected online, coupled with a litany of high visibility data breaches, have made data privacy and security a focus of regulatory attention. Although the Federal Trade Commission (FTC) has long been a prime watchdog over company online privacy and data security practices, the CFPB is not the first federal agency to flex its enforcement muscles in such matters. For example, the Federal Communications Commission (FCC) issued its first data security enforcement action in 2014, when it departed from agency precedent and applied a longstanding statute previously focused on protecting a consumer's telephone calling details to encompass a broader array of sensitive personal information. In that action, the FCC proposed a US$10 million penalty against TerrCom and YourTel for "collect[ing] names, addresses, Social Security numbers, [and] driver's licenses . . . and stor[ing] them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation." The FCC later resolved the apparent violations in a US$3.5 million settlement.

The Takeaways

First, this action shows that the CFPB is willing to take action against service providers and online platforms, as well as against traditional financial institutions. Second, as the CFPB notes in its press release, this first action "builds off advances made by several other agencies." More than ever before, companies must understand that multiple agencies watch over data protection practices – including the FCC, FTC, Securities and Exchange Commission, state Attorneys General and, now, the CFPB. Inadequate security measures have also led to liability claims against companies, as well as their officers and directors. Based on the conduct described in the Consent Order, Dwolla could have just as easily been forced to answer to the FTC or another law enforcement agency. Third, companies may be subject to varying legal standards when under investigation for data security and privacy protection. In fact, the "unfair, deceptive or abusive acts or practices" standard employed by the CFPB is even broader than that of the FTC.

At the March 3 Privacy & Data Security Symposium co-presented by the Federal Communications Bar Association and the American Bar Association Forum on communications, officials from the FTC and the FCC reaffirmed their collaboration and shared mission in protecting the privacy and security of consumer personal data. Multiple federal and state agencies have overlapping jurisdiction when it comes to privacy and data security. As the Dwolla case illustrates, these agencies are taking expansive views of their mandates.

The FTC, FCC and other government officials at the Symposium made it clear that companies handling consumer data need to make sure that: (1) they have adequate privacy and data security measures in place; (2) they have considered what data they really need, what they should jettison, and what level of protection is needed in light of the nature of the data being collected and maintained; (3) they have trained their personnel on these issues; (4) they have data breach response plans just in case something happens; and (5) a company's privacy policy and other statements about their data protection and handling should be truthful and correct. As the Dwolla case shows, the CFPB concurs with these other agencies and will make its mark as another cop on this data security beat.

Contacts

Paul Besozzi
Partner, Washington DC
T +1 202 457 5292
E paul.besozzi@squirepb.com

Deborah Lodge
Partner, Washington DC
T +1 202 257 8019
E deborah.lodge@squirepb.com

Phil Zender
Partner, San Francisco
+1 415 393 9827
philip.zender@squirepb.com

Koy Miller
Associate, Washington DC
T +1 202 457 5321
E koyulyn.miller@squirepb.com

Zach Luck
Associate, Columbus
T +1 614 365 2794
E zachary.luck@squirepb.com