PaymentsCompliance

What Does The First CFPB Order On Data Security Compliance Signal?

16TH MAR 2016 | WRITTEN BY: MARK TAYLOR

Payments and fintech firms must consider very carefully how they furnish privacy policies and build in early compliance protections, legal experts have warned, following a ground-breaking consent order issued by a forceful U.S. regulator. PaymentsCompliance explores the issue.

The Consumer Financial Protection Bureau (CFPB) entered the field of cybersecurity enforcement for the first time recently when it issued a consent order against online payment processor Dwolla.

The U.S. company was accused of misrepresenting safety claims, telling consumers it was PCI-DSS compliant, and had features exceeding the expected industry standards.

Despite the comparatively small $100,000 fine, legal experts have stressed the importance of understanding why the CFPB has, some believe, trod on the toes of the Federal Trade Commission (FTC) in pursuing this case.

Actions Are Louder Than Words On Safeguards

Payments attorney Jane Shea, who leads the data privacy team in the Ohio office of Frost Brown Todd, said: "Up to this point enforcement actions against businesses for not doing what they promised in their published privacy policies has been the domain of and sole effort by the FTC, but when the Dodd Frank Act was enacted the CFPB was granted the ability to police the behavior of businesses and hold them accountable if they violate or run afoul by acting in an unfair or deceptive or abusive manner."

Shea told PaymentsCompliance: "The message is be very careful about what representations you make, in the area of information security.

"When we draft privacy policies for clients, we always recommend the inclusion of a statement such as 'we cannot guarantee absolutely that your information will never be subject to a breach' but I think at a minimum for a business to be taken seriously they must represent that they employ industry standard security procedures.

"Maybe don't say they are the best available but you want to make the effort to do what your peers are doing in this space, and want to put that forward to the public."

The basis of the claim was the CFPB's "unfair, deceptive or abusive acts or practices" (UDAAP) authority to declare practices "unfair, deceptive, or abusive" under 12 U.S.C. § 5531(a), despite no evidence of any consumer harm or breach.

This approach shadows enforcement actions brought by the FTC under Section 5 of the FTC Act.

Former CFPB examiner Kimberly G. Monty, an attorney in the bank regulatory group in the New York office of Schulte Roth & Zabel LLP (SRZ), also noted the similarity in approach to FTC enforcements.

"In those actions, the FTC has used its 'unfair' authority to criticize companies' inadequate cybersecurity practices," she told PaymentsCompliance.

"Here, the CFPB did not allege that Dwolla's practices were unfair.

"What is interesting about the CFPB's determinations is that the regulator appointed itself as an arbiter of PCI compliance, which is another area the CFPB doesn't traditionally deal with and has not in the past."

Requesting companies do more than the expected, as part of the punishment, is a favored education tool of the CFPB, which has been belligerently pursuing cases in the payment space.

Andrew L. Sandler, chairman, executive partner and co-founder of BuckleySandler law firm, said it was clear that the regulatory community was not satisfied with the industry's response to high profile breaches and with regard to adequate protections then put in place.

"I don't know if the CFPB will pursue the data protection angle in an overly heavy manner as it's not really their core focus but we expect them to do some; however we'll see the New York Department of Financial Services and other state regulators do more," he said.

"State attorneys general will do a lot in this area, and the prudential bank regulators are very much focused on data security, along with the FTC."

No Hiding Place In CFPB Exam Procedure

Sandler, a financial services expert, told PaymentsCompliance that the industry must wise up to how the CPFB will check the training and certifications of those involved in the operations of financial services.

"No-one should be surprised at how thorough and detailed the CFPB enforcement examiners will go to uncover any issue, and anyone who has been tested will confirm it is akin to a proctological exam," he said.

"This is a lesson the industry really must heed in dealing with the CPFB.

"The message of this order and other current examinations is insure that representations are consistent with policies and procedures, and elevate the compliance and legal focus on cybersecurity.

"The subtext is cybersecurity issues should not be delegated exclusively to the IT department."

Monty agreed, explaining how the CFPB's examination procedures include a review of a company's

compliance management system.

"Two central components of that review are an examination of employee training, and an examination of the company's corrective actions taken in response to any adverse findings, either from an internal audit, external audit, or an administrative examination finding or order," she said.

"The CFPB may expect financial institutions to have independent oversight of cybersecurity practices, and other compliance matters, and the board is ultimately responsible for overseeing compliance."

The order states the requirement of a centralized compliance program with a direct reporting line to the board of directors.

Get Smart, Early On

This point was picked up by e-payments expert Joshua Rosenblatt, an attorney in the Nashville office of Frost Brown Todd.

He told PaymentsCompliance: "Having the right people on the board is critical. Getting started, its important that the ground work be set, or at least thought out: whether its data privacy or know your customer, these are areas both things the CFPB is highly focused on.

"There are a lot of different areas that if especially for emerging companies, if handled correctly out of the gate, can make their life a lot easier later on.

"If they adopt bad practices early they can get in trouble later."

Rosenblatt also noted the significance of the fine.

"The penalty, to me, is large enough to get people's attention, but not so large that it puts Dwolla out of business," he said.

"It sends a very clear message to the industry, especially start-ups, that privacy is something to be taken seriously."

The Dwolla case is likely to be just the beginning for payment processors handling sensitive data.

SRZ's Monty added: "The more technology merges with financial products, the more the CFPB wants to get ahead of that innovation, and set the tone for what it expects from the industry in terms of consumer protection.

"Innovative financial technology is often released by smaller companies that don't necessarily know the ropes of the financial industry and the rules that go along with it.

"The CFPB is now trying to make sure these emerging payment systems are built from the ground up with consumer protection in mind."

1. HOW DOES THE FTC COMPARE?

With a new cop on the beat, payments companies now have two regulators monitoring their data practices. Given the similarities between this action and the workings of the FTC, did Dwolla escape lightly?

In December, the FTC fined LifeLock, an identity theft protection service that can aid credit card safety ar eye-watering $100m for violating an order requiring the company to secure consumers' personal information.

Among the accusations were claims that from at least October 2012 through March 2014, LifeLock failed to establish and maintain a comprehensive information security program to protect users' sensitive personal information, including social security, credit card and bank account numbers.

LifeLock also allegedly falsely advertised that it protected consumers' sensitive data with the same high-level safeguards used by financial institutions.

2. A YEAR IN THE LIFE OF THE CFPB

PaymentsCompliance has been closely tracking the consumer watchdog over the last 12 months:

March 2015: CFPB is one of several agencies putting its voice towards how the future of American payment systems should be regulated and subject to oversight .

April 2015: Four payment processors caught in a federal dragnet aimed at debt collectors are sanctioned despite not knowing they were part of the scam.

May 2015: PayPal hit with $25m fine for "illegal credit and billing practices".

May 2015: Payment processor fined $30m for its part in a boiler room telemarketing scam.

July 2015: A Western Union subsidiary is fined for "deceiving" consumers.

July 2015: Citibank is fined $700m for "illegal" credit card billing practices.

August 2015: Publicly available consumer complaint database has more than 55,000 entries against credit and pre-paid cards.

September 2015: Fifth Third Bank fined $3m for credit card add-on malpractices.

December 2015: CFPB says it has saved consumers $16bn in fees.

January 2016: CFPB says it is to increase focus on the credit card market.

March 2016: CFPB says non-banks should be subject to same regulation as banks .

Topics: FRAUD & SECURITY | DATA PROTECTION

Geography: UNITED STATES

Sectors: FINTECH | PAYMENT PROCESSING

Content: NEWS & ANALYSIS