PROACTIVE PROTECTION OF CONSUMERS OR PREMATURE PENALTY? CONSUMER FINANCIAL PROTECTION BUREAU BUCKS THE TREND IN DATA SECURITY BREACH CASES

Date: 15 March 2016

Consumer Financial Services Alert

By: Ryan M. Tosi, Lindsay Sampson Bishop, R. Bruce Allensworth

Data breaches and cybersecurity attacks appear to be growing in frequency. Despite the increase in the number of such attacks, plaintiffs have found it difficult to establish a legal foothold for data breach claims, as federal courts across the country have routinely dismissed data breach claims brought by private litigants where no cognizable harm has been alleged. The Consumer Financial Protection Bureau ("CFPB"), however, now appears poised to enforce regulations regarding the protection of private consumer information, including holding companies accountable -- even without any data breach or misuse of private consumer information.

DATA SECURITY LITIGATION

In recent months, there has been a flurry of dismissals of data security breach class actions and multidistrict litigation for lack of Article III standing -- the constitutional right to bring lawsuits in federal court -- because the plaintiffs failed to allege any actual harm caused by the misappropriation and purported misuse of data purportedly obtained from the breach. For example, in *Whalen v. Michael Stores Inc.*, --- F. Supp. 3d ---, 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015) and *In Re: SuperValu, Inc., Customer Data Security Breach Litigation*, 14-MD-2586 ADM/TNL, (D. Minn. Jan. 7, 2016), the Eastern District of New York and the District of Minnesota each dismissed class actions where the named plaintiffs, whose credit card information had been accessed through the use of malware after shopping at the defendants' retail stores, failed to allege they sustained any actual harm following the purported unauthorized use of their data. Moreover, the alleged instances of unauthorized use of data was limited to two occasions in *Whalen* and only one occasion in *SuperValu*, and plaintiffs did not allege any further fraudulent activity after cancelling their credit cards following the breaches. Both courts thus noted that the alleged risk of future harm stemming from the data breaches was speculative and insufficient to constitute injury in fact.

These cases, among many others,[1] reflect a growing trend among federal courts to require plaintiffs to allege actual, cognizable harm arising from a data security breach in order to establish legal standing to bring a lawsuit.

THE CFPB'S DATA SECURITY CONSENT ORDER

Against this backdrop, the timing of the CFPB's first-ever data security enforcement action is significant. Using its authority to regulate unfair, deceptive, or abusive acts or practices ("UDAAP"), the CFPB recently entered into a Consent Order with Dwolla, Inc. ("Dwolla"), an online payment platform, for alleged misrepresentations regarding

Dwolla's data security practices. Notably, the CFPB obtained the Consent Order in the absence of *any* actual data breach or evidence of harm to consumers.

Dwolla permits consumers to direct funds to their own accounts or to other consumers or merchants. In order to open a Dwolla account and effectuate fund transfers, consumers must submit, and Dwolla then stores, their personal identifying information, including names, dates of birth, social security numbers, and bank account numbers. Dwolla also stores digital images of driver's licenses, social security cards, and utility bills, along with usernames, passwords, and four-digit pins. According to the CFPB, Dwolla represented, expressly or by implication, that it had robust data security practices to safeguard such personal information. Dwolla claimed that its network and transactions were "safe" and "secure," and "safer [than credit cards]," that its data security practices "exceed industry standards," and "set a new precedent for the industry for safety and security," that "all information is securely encrypted and stored," and that it encrypts data "utilizing the same standards required by the federal government."

Dwolla agreed to the issuance of the Consent Order, but did not admit or deny any of the CFPB's findings of fact. In the Consent Order, the CFPB focused on the UDAAP deception prong and alleged that Dwolla's data security practices for the collection, maintenance and storage of consumers' personal information did not exceed industry standards. The CFPB alleged that Dwolla, among other things, failed to employ reasonable and appropriate security measures to protect consumers, including data encryption and compliance with the standards set forth by the Payment Card Industry Security Standards Council. Further, the CFPB contended that Dwolla did not encrypt all sensitive consumer information in its possession, did not use appropriate measures to identify foreseeable security risks, and did not implement reasonable data security policies and procedures. Consequently, the CFPB asserted that Dwolla's representations regarding its consumer data protection measures and the safety and security of its network and its transactions, including the representation that its practices "exceeded" industry standards, were likely to mislead a reasonable consumer into believing that Dwolla had appropriate data security measures and were therefore deceptive.

The Consent Order required Dwolla to pay a civil penalty of $100,000, to take numerous steps to augment its data security practices, and prohibited Dwolla from misrepresenting its data security practices. The CFPB did not specifically identify what it believed would constitute "reasonable and appropriate" data security measures, but did require Dwolla to:

- Establish and maintain a written data security plan reasonably designed to protect the confidentiality of sensitive consumer information;
- Identify and designate a qualified individual to coordinate the data security program;
- Develop an "appropriate method" of customer identity authentication when consumers register for services and before effectuating a transfer of funds;
- Adopt "reasonable and appropriate" data security policies and procedures;
- Conduct biannual data security risk assessments for both internal and external vulnerabilities, and adjust the data security program in light of the risk assessments;
- Conduct employee training on the data security policies and procedures; and

- Involve the board of directors in developing a compliance plan to correct deficiencies identified in the data security audit, to ensure adherence to the Consent Order, and to require timely and appropriate corrective action to remediate any failure to comply with the Consent Order.

In announcing the Consent Order, CFPB Director Richard Cordray stated that "[w]ith data breaches becoming commonplace and more consumers using these online payment systems, the risk to consumers is growing. It is crucial that companies put systems in place to protect this information and accurately inform consumers about their data security practices." Further, in prepared remarks to the Consumer Bankers Association on March 9, 2016, Director Cordray acknowledged that the CFPB's public enforcement actions could apply industry-wide and are "intended as guides to all participants in the marketplace to avoid similar violations and make an immediate effort to correct any such improper practices." Specifically, Director Cordray stated that the consent orders "provide detailed guidance for compliance officers across the marketplace about how they should regard similar practices at their own institutions. If the same problems exist in their day-to-day operations, they should look closely at their processes and clean up whatever is not being handled appropriately." Director Cordray remarked that "it would be '*compliance malpractice*' for executives not to take careful bearings from the contents of these orders about how to comply with the law and treat consumers fairly."[2]

CONCLUSION

Although the CFPB focuses on the deceptive representations Dwolla made to consumers in light of its existing data security practices and encryption techniques, the question remains whether the CFPB would have taken action against Dwolla in the absence of any misrepresentations to consumers solely because Dwolla's data security protections were inadequate. While many federal courts continue to require that consumers allege actual harm in order to proceed with a data security breach suit in private litigation, the CFPB, through the use of its UDAAP authority, may be poised to subject financial institutions within the CFPB's enforcement jurisdiction to liability for data security issues in the absence of discernable harm to consumers, and appears to have found a mechanism to impose penalties on companies even if those companies are unlikely to be successfully targeted in federal civil suits. We will continue to monitor developments on these issues and provide further analysis on cybersecurity and data privacy news as it arises.

Notes:

[1] *In re Zappos.com, Inc. Customer Data Sec. Breach Litig.*, --- F. Supp. 3d ---, No. 12-00325, 2015 WL 3466943, at *5 (D. Nev. June 1, 2015) ("The majority of courts dealing with [recent] data-breach cases … have held that absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing."); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 366 (M.D. Penn. Mar. 13, 2015) (no standing where plaintiffs did not allege that they actually suffered any form of identity theft following data breach); *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 853–54 (S.D. Tex. 2015) (even where plaintiff alleged possibility "that fraudulent use of her personal information could go undetected for long periods of time," court found no standing where plaintiff did not allege actual identity theft or fraud).

[2] Director Cordray's full remarks can be viewed at: http://www.consumerfinance.gov/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-consumer-bankers-association/

KEY CONTACTS

R. BRUCE ALLENSWORTH
SENIOR OF COUNSEL

BOSTON
+1.617.261.3119
BRUCE.ALLENSWORTH@KLGATES.COM

RYAN M. TOSI
PARTNER

BOSTON
+1.617.261.3257
RYAN.TOSI@KLGATES.COM

LINDSAY SAMPSON BISHOP
PARTNER

BOSTON
+1.617.951.9198
LINDSAY.BISHOP@KLGATES.COM