Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Role Of Economics In Data Breach Class Actions

Law360, New York (September 19, 2014, 10:49 AM ET) --

Matthew Milner

Over the past year, there has been a wave of cyberattacks on payment data systems at major U.S. retailers. Nationwide chains such as Target Corp., Neiman Marcus Group LTD Inc. and Michaels Companies Inc. have experienced breaches in which customers' data has been taken or exposed to unauthorized parties. Subsequent to these data breaches, consumer class actions were filed against each retailer on behalf of customers whose data was compromised.[1]

This month, The Home Depot Inc., the fourth largest retailer in the U.S., acknowledged its point-of-sale systems were breached in a widescale cyberattack that may have extended back to April 2014 and covered stores in both U.S. and Canada.[2] Even before Home Depot could confirm its systems had been compromised, a class action was filed in the U.S. District Court in the Northern District of Georgia against the company on behalf of a putative class of customers seeking injunctive relief and damages.[3] Home Depot is continuing its investigation of the breach and is working with the U.S. Secret Service and computer security firms to understand the scope and impact of the attack and the measures used by the hackers.[4]

The recently filed consolidated complaint against Target in the U.S. District Court of Minnesota provides another illustration of the specific types of allegations being made in consumer class actions related to data breaches.[5] The putative class members are residents “whose credit or debit card information and/or personal information was compromised as a result of the data breach first disclosed by Target on Dec. 19, 2013.”[6] The classes include all individuals who potentially had their information stolen from Target systems, regardless of whether the breach caused actual financial harm, including[7]:

- unauthorized charges on their debit and credit card accounts;
- theft of their personal and financial information;
- costs associated with the detection and prevention of identity theft;
- loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts; and
- costs associated with time spent to address issues resulting from the Target data breach.

Courts in data breach class actions will be faced with difficult questions. For example, did all class

members suffer actual injury from the breach and how does one measure and quantify damages? Economic science — particularly the counterfactual paradigm economists use to analyze fact of injury and damages — provides a rigorous framework to analyze the types of complex point-of-sale transactional data that likely underlie such cases. In this paradigm, one compares a plaintiff's financial position in the "actual world" in which the breach occurred with the plaintiff's financial position had the breach not occurred (i.e., the "but-for" world).

For example, in the Target case, to evaluate potential injury resulting from a data breach to consumers in the actual world, certain facts would need to be ascertained, including:

- Did the plaintiff make purchases from the defendant during the window of the breach?
- Was the plaintiff's payment card information subject to the actual breach?
- Did the status of the plaintiff's account change (e.g., was it frozen) subsequent to the breach?
- Were there unauthorized charges on the payment card at issue?
- Were the fraudulent charges reimbursed?

Each of these questions could be determined with an analysis of the underlying datasets, assuming such data was made available in the case. Depending on the organization, this data may be stored in a single data warehouse or maintained across disparate systems on a store-by-store basis, by geographic region or by subsidiary. Given the size and complexity of transactional data in these cases, it is important to understand the relationships between the affected and unaffected databases. This exercise can involve mapping customer lists to data kept in other relational tables, such as actual payments, address information and payment card information. Once the potentially affected data has been identified, it is imperative to understand what information was subject to the breach and the customers that may be affected.

However, merely identifying who was potentially injured from the data does not tell the whole story. For example, the theft of payment card information does not mean all customers who made purchases during the window of the breach were economically injured. Federal laws protect consumers from being responsible for unauthorized charges. The Fair Credit Billing Act limits personal liability for unauthorized credit card charges to $50 in the U.S.[8] For ATM and debit cards, a cardholder's loss is limited to $50 if the person reports the theft to the card issuer within two business days; the cardholder's loss can be up to $500 if the person reports the theft within 60 days after the statement is sent by the card issuer and becomes unlimited after 60 days.[9] Despite federal regulations offering protection to consumers, many credit and debit card companies offer much stronger protections against unauthorized charges. Visa Inc., MasterCard Inc. and American Express Co. often guarantee that credit and debit cardholders will not be held responsible for unauthorized payments.[10]

These circumstances illustrate the critical aspect of class actions of this type: actual economic injury cannot be assumed, it must be measured for each plaintiff. In order to assess economic damages, one must consider a framework that identifies the potential misconduct and financial harm to individual customers associated with the wrongful act(s).

To recreate the but-for world, one must evaluate if any costs incurred by plaintiffs were due to the data breach or to other factors unrelated to the breach. If an individual is found to be worse off in the actual world relative to the but-for world, then they would have suffered economic injury from the data breach. The difference between the plaintiff's financial positions in the two scenarios is the economic damages. In sum, an impact and damages analysis needs to causally link the data breach to the actual

economic harm to consumers that had personal information compromised as a result of the breach.

As illustrative examples, I use the allegations of two class representatives from the Target complaint to show how one might construct the actual and but-for worlds:

- Brystal Keller alleged she had two fraudulent charges amounting to $710 on her debit card and was reimbursed for the charges 12 days later. She claimed, due to these charges, she was locked out of her account and as a result, "missed a rent payment, a car loan and a washer and dryer payment."[11]

Documentary evidence and data can validate Keller's claims about her debit card usage at Target stores, the fraudulent charges, timing of the reimbursement and the availability of her funds. To recreate the but-for world, a factual inquiry is required to assess if the reasons the plaintiff missed certain payments were due to the data breach at Target or if there were contemporaneous factors unrelated to the breach that may have caused the missed payments.

- Aimee King alleged to have seven unauthorized charges totaling $940 on her debit card. As a result of the charges, King claimed she could not make payments for her car insurance, rent, loan, and cellphone. Moreover, she alleged the breach has caused the interest rate on her loan to increase by 125 percent and her credit score to drop nearly 40 points.[12]

Here, detailed evidence and transactional data can also be used to substantiate the allegations of King's purchases at Target stores, the amounts of the unauthorized transactions, her availability of funds subsequent to the fraudulent charges and whether she was reimbursed for the $940. Similarly, one would need to obtain additional information about King's circumstances in order to confirm that these factors were responsible for her adverse financial impacts, rather than other financial circumstances.

In order to estimate damages to plaintiffs resulting from a data security breach, it is important to construct a rigorous economic analysis that models the actual and but-for worlds. The goal of such analysis is to make each plaintiff whole to the extent there was economic harm resulting from the breach itself. That determination, like in the class action brought against Target, may hinge on a number of individualized factors to determine fact of injury and damages.

—By Matthew Milner, Edgeworth Economics LLC

Matthew Milner is a partner in Edgeworth Economics' Washington, D.C., office.

[1] See In Re: Target Corporation Customer Data Security Breach Litigation, Consumer Plaintiffs' Consolidated Class Action Complaint, MDL No. 14-2522 (PAM/JJK), filed Aug. 25, 2014; Lance Duroni, "Neiman Marcus, Michaels Stores Sued Over Data Breaches," Law360, Jan. 28, 2014.

[2] Shelly Banjo and Danny Yardon, "Home Depot Confirms Data Breach, Do-It-Yourself Retailer Says No Evidence Debit PIN Numbers Were Compromised," The Wall Street Journal Online, Sept. 8, 2014.

Retrieved from http://online.wsj.com/articles/home-depot-confirms-data-breach-1410209720

[3] Leon Stafford, “Suit Filed Against Home Depot in Possible Breach,” The Atlanta Journal-Constitution Online, Sept. 5, 2014. Retrieved from http://www.ajc.com/news/business/lawsuit-filed-against-home-depot-in-possible-data-/nhGbb/

[4] Home Depot, “The Home Depot Provides Update on Breach Investigation,” Press Release, Sept. 8, 2014.

[5] Target Data Security Breach Litigation Complaint.

[6] Target Data Security Breach Litigation Complaint at 239-243.

[7] Target Data Security Breach Litigation Complaint at 2.

[8] Federal Trade Commission (August 2012), Consumer Information, Disputing Credit Card Charges, Retrieved from http://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges

[9] Federal Trade Commission (August 2012), Consumer Information, Electronic Banking, Retrieved from http://www.consumer.ftc.gov/articles/0218-electronic-banking

[10] See http://usa.visa.com/personal/security/zero-liability.jsp; http://www.mastercard.us/zero-liability.html; https://www.americanexpress.com/us/content/pay-bills-with-amex/faq.html

[11] Target Data Security Breach Litigation Complaint at 1.

[12] Target Data Security Breach Litigation Complaint at 1.