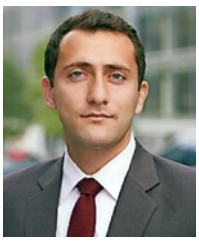
Bloomberg Law

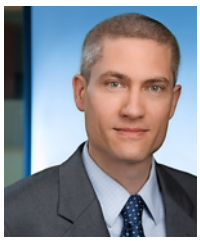
Privacy and Security Law Report®

Data Breach Litigation

The changing consumer data breach plaintiff standing legal landscape means that companies must understand the importance of rigorous economic analysis to assess the plausibility of class-wide impact and damages in data breach class actions within the context of harms plaintiffs typically claim in these cases, the authors write.

A Rigorous Analysis of Class Certification Issues in Consumer Data Breach Litigation



By Michael Kheyfets, Michelle Visser, David Cohen and Adam Winship

Earlier this year, the economist among the present co-authors wrote an article about economic analysis of claims in data breach class actions that focused on financial institution (FI) cases. (Michael Kheyfets et al., *Economic Analysis of Financial Institution Claims in Data Breach Class Actions*, Information L.J., Winter 2016, at 2). That article focused on FI rather than consumer class actions because, at the time, consumer class actions were routinely dismissed as lacking Article III standing. Since that time, however, the U.S. Courts of Appeal for the Sixth and Seventh Circuits have reversed district court rulings that consumer data breach plaintiffs lacked standing to sue. The U.S. Supreme Court has also since handed down two opinions that will affect the analysis of consumer data breach class actions: *Spokeo Inc. v. Robins* rejected plaintiffs' reliance on a statutory right of action to establish standing, while *Tyson Foods Inc. v. Bouaphakeo* voiced a qualified acceptance of the use of ''representative evidence'' to establish class-wide damages.

Given these changes in the legal landscape, we revisit the framework of the previous FI article, this time to discuss economic analysis of class claims in consumer data breach matters. Specifically, we discuss the importance of rigorous economic analysis to assess the plausibility of class-wide impact and damages in data breach class actions within the context of harms plaintiffs typically claim in these cases.

I. The Legal Landscape

A. Recent Standing Cases

A fundamental hurdle plaintiffs face in consumer data breach cases is the demonstration of cognizable injury. Even in cases where plaintiffs have suffered direct losses from identity theft or fraud, it can be difficult, if not impossible, to establish that the fraudulent losses at issue were caused by the breach. Moreover, where the breach is of payment card data, consumers tend to be fully reimbursed for fraudulent charges, due to the card brands' zero liability policies. This difficulty in establishing direct loss to consumers has led to a rapid evo-

 ISSN 1538-3423

lution in plaintiffs' legal theories. Some theories—such as harm through loss of privacy or emotional harm—have been almost universally rejected by courts. Similarly, arguments that a breach has led consumers to lose the value of their personal information have been widely rejected by courts, which have pointed to the fact that consumers generally do not (and cannot) sell their personal information. Theories relating to consumers not getting the benefit of the bargain—i.e., that in making a purchase from defendants, plaintiffs paid a premium for the security of their personal information—have also generally failed.

At the current stage in the evolution of legal theories, a primary battleground over cognizability of harm lies in injury related to future harm—either the increased risk of future harm itself, or harm stemming from present expenditures meant to mitigate the risk of future harm. Defendants have had a great deal of success in arguing that such harms are not cognizable—and thus insufficient to warrant Article III standing—under the holding of the 2013 Supreme Court case *Clapper v. Amnesty International*. *Clapper* rejected allegations of ''possible future injury'' where the threatened injury was not ''certainly impending,'' and of mitigation costs incurred in reaction to future injury that is itself not cognizable: Plaintiffs ''cannot manufacture standing by incurring costs in anticipation of non-imminent harm.'' (It bears noting that even in cases where standing is conferred, plaintiffs' alleged injuries may not satisfy the damages elements of the causes of action they bring. This issue is beyond the scope of this article.)

Despite a string of successes in invoking *Clapper*, data breach defendants face uncertainty in the wake of recent Sixth and Seventh Circuit cases that found that alleged risks to consumer data breach plaintiffs of future harm, when coupled with efforts by consumers to mitigate that risk, satisfied the *Clapper* standard. The first of these opinions—the 2015 Seventh Circuit opinion *Remijas v. Neiman Marcus Group LLC*—arose out of a 2013 cyberattack on Neiman Marcus Group, Inc. stores, with approximately 350,000 payment cards allegedly affected. Reversing the district court, the Seventh Circuit held that the plaintiffs—not just certain consumers who had allegedly already experienced credit-card fraud but also some consumers with potentially affected payment cards—had Article III standing. The Court reasoned that given allegations that ''hackers deliberately targeted'' Neiman Marcus to obtain payment-card data, stole the data, and then misused 9,200 of the stolen card numbers, ''it is plausible to infer that the plaintiffs have shown a substantial risk of harm.'' Ultimately, the *Neiman Marcus* Court held that because there was an ''objectively reasonable likelihood'' that future injury would occur, plaintiffs ''should not have to wait until hackers commit identity theft or credit-card fraud'' to gain standing. In 2016 the Sixth Circuit in *Galaria v. Nationwide Mutual Insurance Co.* and the Seventh Circuit in *Lewert v. P.F. Chang's China Bistro Inc.* and found the risk of future harm and mitigation costs to satisfy injury-in-fact in decisions that mirrored the *Neiman Marcus* reasoning, but arguably went even further to find standing: *Nationwide* made no mention of already-incurred fraud, and *P.F. Chang's* made no mention of it except to note that one of two named plaintiff experienced fraudulent charges.

At the same time that these Sixth and Seventh Circuit cases may have made it easier for plaintiffs to establish standing based on a risk of harm and mitigation measures, the Supreme Court may have cut off an alternative approach to the actual injury requirement in *Spokeo*. Prior to *Spokeo*, some—but not all—circuits had reasoned that federal statutes, such as the Fair Credit Reporting Act (FCRA), created a legally cognizable interest that Congress had created through the statute's private right of action, such that an individual could suffer injury sufficient for standing by the mere violation of a statute. The FCRA, for example, creates a private right of action for individuals affected by a credit reporting agency's failure to ''assure maximum accuracy'' of consumer reports. By the reasoning of some circuits, then, the FCRA created a private right to have an accurate consumer report, and thus an individual with an inaccurate report would have standing by virtue of being deprived of the statutorily created right to accuracy. Data breach plaintiffs relied upon this reasoning to circumvent standing requirements by alleging violations of statutes that provide a private right of action such as the FCRA, the Stored Communications Act and other federal and state statutes. However, this reasoning was rejected by *Spokeo*.

Spokeo operates a website that allows users, including prospective employers, to access profiles of any given individual. The named plaintiff Robins alleged a violation of the FCRA—that his Spokeo profile falsely ascribed to him positive characteristics he did not have: employed, married with children, affluent and possessing a graduate degree. The Ninth Circuit held that Robins had standing because the alleged violation was of *his* statutory rights in the accuracy of his consumer report, ''not just the statutory rights of other people,'' and that his interest in this statutory right to accuracy was ''individualized rather than collective.''

In reversing the Ninth Circuit, the Supreme Court noted that to have standing, a plaintiff must allege injury that is both ''concrete *and* particularized,'' and faulted the Ninth Circuit for addressing only whether alleged injury was ''particularized.'' In remanding the case for consideration of concreteness, the Court acknowledged that ''intangible'' injuries, including a ''risk of real harm'' could be ''concrete.'' Importantly, though, the Court confirmed that—even in the presence of a statutory right—not just any risk of harm is sufficient to confer standing. A court must consider whether the ''degree of risk is sufficient to meet the concreteness requirement.''

B. Tyson Foods v. Bouaphakeo

At the same time that the above decisions were grappling with issues of standing, the Supreme Court issued a decision that will affect the analysis of class certification in consumer class actions that reach this stage. In *Tyson*, the Court affirmed the certification of a class based on the ''representative evidence'' of a statistical sample used to establish liability and damages. The Court, however, declined to adopt ''general rules'' regarding the use of statistical evidence in class action cases, stating that ''[w]hether and when statistical evidence can be used to establish class-wide liability will depend on the purpose for which the evidence is being introduced.''

Plaintiffs had alleged that Tyson's failure to fully compensate employees for time spent donning and doffing protective gear before and after shifts at a pork processing plant resulted in unpaid overtime in viola-

  PVLR ISSN 1538-3423

tion of the Fair Labor Standards Act (FLSA). Because Tyson kept no records the actual time spent donning and doffing by class members, Plaintiffs sought to establish damages through a study that measured the average time spent donning and doffing for a sample of 53 employees. Plaintiffs then assumed that individual employees spent this average amount of time and combined the average with employee time sheets to estimate overtime pay wrongly withheld. The jury found for plaintiffs, and the Eighth Circuit affirmed.

Tyson's primary argument before the Supreme Court was that a class cannot be properly certified where liability and damages are determined using an average obtained through a sample of the proposed class. Tyson relied on *Wal-Mart Stores Inc. v. Dukes*, in which the Supreme Court found that a Title VII class was improperly certified where the employer had no common policy of sex discrimination and plaintiffs attempted to infer discrimination toward any given class member through a sampling of employees which revealed an estimated ''percentage of claims determined to be valid.'' The *Wal-Mart* Court found this ''Trial by Formula'' impermissible because it enlarged the class's substantive rights, allowing the class to recover where individual plaintiffs could not.

The *Tyson* Court rejected Tyson's argument, reconciling its holding with *Wal-Mart* with the explanation that inference from sampling was improper in *Wal-Mart* because without a common policy of sex discrimination, the class members were not ''similarly situated.'' Class members in *Tyson*, on the other hand, were deemed to have been similarly situated because each member ''worked in the same facility, did similar work, and was paid under the same policy.'' The underlying question both in *Wal-Mart* and in *Tyson* was ''whether the sample at issue could have been used to establish liability in an individual action.'' Given the statistical evidence in *Tyson* was properly admitted, then, the jury was entitled to rely on statistical evidence to establish damages just as it would if such evidence were brought in individual suits.

While *Tyson* was a victory for plaintiffs in some contexts, there are likely to be significant issues with its application in consumer data breach class actions. First, *Tyson* was an incomplete victory even within that litigation. The court delayed ruling on whether a class can be properly certified where plaintiffs have not established a means of insuring that uninjured members will not share in the damages award because damages had not yet been disbursed. The Court recognized, however, the importance of the question, and Chief Justice Roberts' concurring opinion expressed doubt that the district court would be able to infer which class members the jury determined had unpaid overtime: ''Given this difficulty, it remains to be seen whether the jury verdict can stand.''

The economic framework for assessing class certification issues in consumer breach cases mirrors what has been previously outlined for financial institution cases.

Second, the *Tyson* holding was limited to its circumstances, which are distinguishable from the typical data breach case. In consumer data breach cases, class members are not nearly so ''similarly situated'' as the class members in *Tyson*. For instance, proposed classes of consumers vary both in whether the consumers experienced post-breach misuse of their personal information (and, if so, to what extent) and in whether they purchased credit monitoring or took other preventative measures as a result of the breach. Proposed consumer classes are arguably more like the proposed class in *Wal-Mart*, where no common discriminatory policy bound them together—impact, if any, is far from uniform when personal information is misused in the wake of a data breach and individual consumers each have their own idiosyncratic reactions to a data breach and have nothing akin to the common workplace, work tasks, and payment policy that were deemed to bind the class together in *Tyson*. Given the variability within proposed classes in data breach suits, it seems unlikely that statistical, ''representative'' evidence would suffice to establish liability and damages if a data breach class action were brought as individual actions, and thus it would not suffice to establish class-wide damages under *Tyson*. The economic analysis below highlights these and other challenges consumer data breach plaintiffs may face in attempting to certify a class.

II. Economic Analysis of Class Certification and Damages Issues in Consumer Cases

A. Relevant Economic Framework

The economic framework for assessing class certification issues in consumer breach cases mirrors that which we have previously outlined for financial institution cases. (See *Economic Analysis of Financial Institution Claims in Data Breach Class Actions*.) The key elements of this framework include:

- Construction of an appropriate ''but-for world,'' i.e., one where the breach did not occur, for the purpose of comparing it to the ''actual world,'' where it did.
- Testing (and ''falsifiability'') of assumptions on which the but-for world is constructed.
- Rigorous assessment of the evidence to determine whether injury can be established using evidence common to the class, or if individualized inquiries would be necessary.

This third element follows standards prescribed by the Supreme Court in other class action matters, such as *Comcast Corp. v. Behrend* and *Wal-Mart v. Dukes*, among others.

As we discussed above, the Court's more recent *Tyson* decision may have superficial appeal to plaintiffs as a shortcut to rigorous economic analysis that relies solely on ''representative evidence.'' However, as we explain in more detail below, the Court's refusal to adopt a ''broad categorical rule [. . .] governing the use of representative and statistical evidence in class actions'' is critical in the context of the damages theories frequently put forth in data breach cases. The circumscribed nature of the ruling is important because the use of ''*Tyson*-style'' statistical evidence—a small sample intended to represent the ''average'' experience of all class members—is likely to be problematic in a data breach case. Given consumers' idiosyncratic reactions to a data breach, extrapolating from a small sample of consumers to thousands (or millions) of other purported class members whose data was (or may have been) compromised risks reaching the wrong conclusions.

B. Economic Analysis of Claims in Consumer Cases

The appropriateness of the class action mechanism for adjudicating a consumer data breach litigation rests crucially on the plaintiffs' ability to present an analysis capable of determining whether all—or, in some cases, virtually all—class members could have suffered injury from the alleged data breach. That is, the plaintiffs' burden is to propose a method that would be able to assess whether a particular type of claimed harm can be evaluated on a class-wide basis. However, even reliance on ''representative evidence''—rather than that spanning the entire proposed class—may be problematic for the purpose of establishing that class members were ''similarly situated'' as a result of the breach at issue.

In this section, we discuss three theories of economic harm often presented by plaintiffs in these matters, including the cost of (i) fraudulent misuse of stolen information, (ii) time spent mitigating the potential effects of a breach, and (iii) data security, which plaintiffs claim they did not receive. (Although we focus on these three theories here, a number of others have also been put forth in data breach cases, including among others (i) diminution in value of personal information, (ii) loss or delay of tax refunds as a result of fraudulently filed tax returns, and (iii) damages caused by Defendants' failure to notify affected individuals.)

1. Valuation of Harm from Misuse of Stolen Personal Information

A prevalent theory of harm in consumer data breach cases is that of direct harm from the misuse of stolen personal information. In the payment card context, for example, this would be harm to consumers from fraudulent charges—either by the hackers themselves, or by third parties who purchased the stolen information—which would not have taken place but for the breach. For example, the *In re Target Corp. Customer Data Sec. Breach Litig.* plaintiffs claimed the following fraudulent charges stemmed from that breach:

- Plaintiff Brystal Keller believed that her prepaid Walmart GE Capital Visa debit card was compromised after fraudulent charges of $434.15 and $276 appeared on her card.

- Plaintiff Aimee King believed that her Meta Bank Visa debit card was compromised because she incurred seven unauthorized charges totaling approximately $940.

- Plaintiff Christie Oliver believed that her Bank of America Visa debit card was compromised after she discovered unauthorized charges totaling $1,506.98.

- Plaintiff Deborah Rhodes believed that her GE Capital Visa debit card was compromised after she incurred a fraudulent charge of $3,900.

- Plaintiff Michelle Mannion believed that her Lorain National Bank MasterCard debit card was compromised because of four unauthorized charges amounting to about $222.

- Plaintiff Frederick Smart presumed that his Chase Bank Visa debit card and Target REDcard debit card were compromised after he incurred fraudulent charges totaling roughly $101 on his Target REDcard debit card and $277 on his Visa debit card.

- Plaintiff Martha Reynoso believed that her EPPICard debit card was compromised after her account balance was depleted by $3,637.67.

Claims of a similar nature were made by plaintiffs in *In re The Home Depot Inc., Customer Data Breach Security Litigation*, *Whalen v. Michaels Stores Inc.*, *Neiman Marcus*, and *P.F.Chang's*.

To measure this direct harm, any analysis must distinguish the effect of the claimed conduct (i.e., data breach specific to the litigation) from all other contemporaneous factors. That is, it is necessary to examine the *causal link* between the breach and specific fraudulent charges. For example, a given payment card may be subject to multiple data breaches (some of which may have been disclosed publicly, while others may not have been). Any analysis purporting to calculate damages from a given breach would need to distinguish fraudulent charges resulting specifically from *that* breach, as opposed to any other breach involving that card. The timing of charges is critical here. For example, a card that incurred fraudulent charges *prior* to the initial point of the breach at issue may raise questions about whether the unauthorized transactions incurred *after* the incident are tied to the relevant breach or to another one. Thus, for example, if a number of retailers are breached in quick succession, determining proximate causation becomes difficult.

Some courts have indicated the issue of causality as meriting rigorous analysis at the class certification stage. For example, the District of Maine in *In re: Hannaford Brothers Co. Customer Data Security Breach Litigation*, deemed ''fatal'' the plaintiffs' failure to present expert opinion on ''what proportion of the fees incurred are attributable to the Hannaford intrusion, as distinguished from other causes.'' However, there have been other instances where courts have found the mere suggestion of the absence of causality unconvincing. For example, in *In re Adobe Systems Inc. Privacy Litigation*, the Northern District of California rejected the defendant's argument that a named plaintiff may have been a victim of contemporaneous data breaches involving Target and Neiman Marcus, as there was ''no factual basis for Adobe's speculation that [named plaintiff] Halpain was a customer of either Target or Neiman Marcus, let alone that Halpain's personal data was compromised in data breaches involving these companies.'' (Notably, that case settled before the Court had oppor-

  PVLR ISSN 1538-3423

tunity to consider causation issues at the class certification stage.)

Some courts have indicated the issue of causality as meriting rigorous analysis at the class certification stage.

If consumers clear the causation hurdle, the proposed damages analysis must apply to all (or substantially all) class members. For example, the eight named plaintiffs in *Target* claimed a wide range of fraudulent charges, where the alleged fraudulent charges ranged from several hundred to several thousand dollars. Even assuming that all these charges did stem from the Target breach (which we understand was not factually established), it would still be necessary to perform an analysis to determine whether all individuals in the class were affected similarly. Any aggregate or average estimate based on the named plaintiffs' claims—or on some source of information not specific to the proposed class—would inaccurately measure fraudulent charges experienced by any individual class member. An average of approximately $1,400 calculated from the eight named Target plaintiffs would overestimate the fraudulent charges experienced by some of the 40 million members of that proposed class, while underestimating the fraudulent charges experienced by others. Moreover, an estimate of average *fraudulent charges* would not reflect the average *damages* actually incurred because consumers with ''zero liability'' credit cards—which we understand are prevalent among consumers—would have likely had fraudulent charges refunded. For example, in *Target*, only one of eight named plaintiffs alleged that fraudulent charges were not fully reimbursed.

A critical weakness of the ''average harm'' model is the possibility that some—or even many—class members may not have incurred any losses associated with fraudulent charges. The avoidance of all losses might occur not only with an individual plaintiff's reimbursement for fraudulent charges, but also, to name just one example, with plaintiffs who replaced their payment cards (or whose financial institutions did so on their behalf) and thus incurred no charges at all. These issues, as well as additional ones presented by the named *Target* plaintiffs—e.g., overdraft fees, lowered credit scores, missed bill payments, etc.—are inherently individualized. It would be inappropriate to *assume* that each member of the proposed class suffered some *average* amount of harm related to fraudulent charges tied to the breach, when in fact it is likely that many did not.

A variation of this theory states that in addition to (or in lieu of) *actual* harm resulting from the disclosure and misuse of personal information, consumers are at a greater risk of suffering harm in the *future*—a risk that *Neiman Marcus*, *PF Chang's* and *Nationwide* held was sufficient for Article III standing under the circumstances of those cases. That is, even if—for example—fraudulent charges have not been incurred at the time that the case is filed, consumers are nonetheless more likely to suffer this type of harm than they would have been absent the specific breach. The analysis of this theory often boils down to the claim that plaintiffs have incurred and will continue to incur expenses to mitigate the risk of fraud—e.g., for credit monitoring products—and that the nature of these expenses is ''common'' because any consumer affected by the breach would have seen an increase in their exposure to risk of misuse.

A critical weakness of the ''average harm'' model is the possibility that some—or even many—class members may not have incurred any losses associated with fraudulent charges.

This type of argument, however, merits the same level of analysis as that of ''actual harm.'' For example, once a consumer's credit card is reissued, the ''future harm'' from the exposure of the old card is reduced to zero. Other types of information—e.g., e-mail addresses, passwords, etc.—can also become ''stale'' over time and may require diminishing monitoring and protection. The valuation of such harm—as well as any potential assessment of it across any proposed class of consumers—should take into account the (i) types of data disclosed for any given consumer, (ii) ''useful life'' of those types of data, as well as (iii) the remedies necessary for any given consumer to mitigate risk of future harm.

2. Valuation of Time Spent Mitigating Effects of the Breach in a Class Action Context

Another often-proposed theory is that consumers incur harm through lost time spent mitigating the effects (or perceived effects) of a data breach. These time-expending activities include placing freezes on accounts, setting up alerts with credit reporting agencies, closing or modifying accounts, and monitoring credit reports for unusual activity. For example, plaintiffs in *P. F. Chang's* claimed ''damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Security Breach.''

The core of this claim is that but for the breach, consumers would not have needed to spend that time mitigating effects of the data breach. Even assuming that plaintiffs could establish that the alleged activities were, in fact, necessitated by the data breach at issue (which is outside the scope of this article), and even if that time has some financial value, the precise amount—as measured by opportunity cost—varies by individual. For example, if one class member had to displace work time in order to deal with the consequences of the breach, while another did so in lieu of watching TV, the value lost by the two class members would vary. Additionally, the value of a class member's time is inherently individualized. For example, if ''opportunity cost'' is defined on the basis of income, a class member earning minimum wage would be affected differently under this theory than a highly paid executive.

It is also difficult (if not impossible) to ascertain the amounts of time actually spent on activities directly relating to the data breach. For example, if a class member had a single credit card number disclosed as part of

the breach, but then spent time cancelling, reissuing, and monitoring all of his payment cards and accounts, it may be difficult to determine what portion of the time spent should be compensable by the breached entity. Moreover, it may be the case that some plaintiffs spent no time on mitigating activities—either by choice or because they were unaware that their information had been compromised. It would be inaccurate to assume that all (or substantially all) class members are owed ''opportunity cost'' damages without an analysis of how much time, if any, individuals spent on relevant tasks.

It is our understanding that in the *Target* settlement, class members were deemed eligible for reimbursement of two hours of lost time at $10 per hour for each type of documented loss they incurred, and that this kind of compensation structure has been used in other breach case settlements. It is worth noting that while this type of simplified approach is potentially useful for the purposes of setting the size of a settlement fund, it would be insufficient as an analysis of class certification. This is because this type of ''average harm'' approach *assumes* that the single compensation amount is appropriate, without *testing* whether it actually is for any consumer or group of consumers.

3. Valuation of The ''Benefit of the Bargain'' in a Class Action Context

Damages theories relating to the ''benefit of the bargain,'' which have been proposed in a number of data breach cases, are predicated on the notion that either (i) there is a ''data security premium'' built into prices of products sold by the breached entity—and consumers paid that premium under false pretense—or (ii) customers would have avoided firms (e.g., retailers, insurers, etc.) with vulnerable information technology systems altogether. For example, plaintiffs in *P.F. Chang's* claimed that ''the cost of their meals is an injury because they would not have dined at P.F. Chang's had they known of its poor data security.'' Similarly, plaintiffs in *Neiman Marcus* argued that ''they overpaid for the products in Neiman Marcus because the store failed to invest in an adequate security system.''

As with the economic analysis of opportunity cost of time, the nature of this type of claim makes certifying a class problematic. Difficulties estimating the premium individual class members place on data security is the issue here. For example, one customer may place a high value on data security, while another may place little or no value. Although two customers purchasing the same product at a restaurant or retailer (e.g., a meal at P.F. Chang's or a garment at Neiman Marcus) would generally pay the same or similar prices, no single ''risk premium'' amount may be identifiable on a class-wide basis. (For example, retailers generally do not charge different prices to customers paying with cash, even though those customers do not provide any information as part of the transaction that requires a ''security premium.'')

Moreover, individual customer preferences would dictate whether any given customer would have avoided a retailer altogether if the IT vulnerability was known. That is, some would have still chosen to eat at P.F. Chang's, while others may not have. This is an inherently individualized inquiry, meaning that damages resulting from this type of harm are also likely to be unique and not amenable to a ''class-wide'' method. For example, a CreditCards.com survey conducted in October 2014 found that 52 percent of responders ''probably'' or ''definitely'' would shop at a store that had a data breach, indicating that consumer response to breaches—as well as any purported premium an individual consumer places on payment card data security—varies.

   ISSN 1538-3423

  PVLR ISSN 1538-3423