Tousley Brain Stephens PLLC

Attorneys

1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101-4416
Telephone (206) 682-5600
Facsimile (206) 682-2992

American Association for Justice
October 8, 2015, Webinar

Highlights and Strategies in Data Breach Litigation

THEORIES OF RECOVERY

Kim D. Stephens
Tousley Brain Stephens PLLC

1. Article III Standing

a. In the context of putative data breach class action cases, the named plaintiff has the same burden of showing Article III standing as he or she would in a non-class case.

b. That is, she must allege and show that the defendant caused her personal injury—not that other, unidentified members of the class suffered an injury. In other words, a plaintiff cannot maintain a class action as a class representative if she could not bring an individual cause of action against the defendant. *See, e.g., Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871 (1990); *Lewis v. Casey*, 518 U.S. 343 (1996); *Haas v. Pittsburgh Nat'l Bank*, 526 F.2d 1083 (3d Cir. 1975). A class representative who raises multiple causes of action must show such standing for each claim. *In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235 (3d Cir. 2012) (quoting *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006)).

c. Recent Cases:

i. For instance, the plaintiffs in *In re Target Corp. Data Security Breach Litigation* alleged unlawful charges, restricted access to bank accounts, late payment charges, and other injuries that were "fairly traceable" to Target's conduct. The court found that, at least at the motion to dismiss stage, these allegations were sufficient to confer standing. 2014 WL 7192478 (2014).

ii. Similarly, in *In re Adobe Systems, Inc. Privacy Litigation*, No. 5:13-cv-05226 (N.D. Cal. Sept. 4, 2014) the court found that the plaintiffs, whose personal data was stolen by hackers who breached Adobe's servers, were at "immediate and very real" risk of having that data misused. Specifically, the court noted that because the hackers specifically targeted Adobe's systems and some of the stolen data had already appeared on the internet, the risk of misuse was "certainly impending… to require plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact."

iii. In *In re LinkedIn User Privacy Litigation*, the court once dismissed the plaintiff's complaint for lack of Article III standing, finding that the "promise of industry standard security had not been part of Plaintiff's bargain for premium services [from LinkedIn]." No. 5:12-cv-03088 (N.D. Cal. March 28, 2014). In her second amended complaint, the plaintiff alleged that she bought her premium LinkedIn subscription "in reliance on LinkedIn's misrepresentation and would not have done so but for the

misrepresentation." The court noted that "importantly," the plaintiff also alleged that she read and relied on LinkedIn's statement in its privacy policy that it utilized

"industry standard security." As a result, the court found the plaintiff's allegations sufficient to establish Article III standing.

iv. Another recent case, *Spokeo v. Robins*, is currently on appeal from the 9th Circuit. In *Spokeo*, the plaintiff claimed that the information about him that Spokeo displayed on its website was inaccurate, but has not alleged any concrete harm flowing from that inaccuracy. The Supreme Court will ostensibly decide whether Congress may confer Article III standing to a class of plaintiffs that suffered no concrete harm. In other words, the Court will determine whether Congress authorized a plaintiff, who could not otherwise invoke federal court jurisdiction, to bring a private action based on a bare violation of a federal statute.

v. In *Remijas v. Neiman Marcus Group*, No. 14-3122 (7th Cir. July 20, 2015), the plaintiffs alleged damages resulting from hackers stealing approximately 350,000 credit card numbers from Neiman Marcus, with approximately 9,200 cards experiencing fraudulent charges at the time of the complaint. The district court dismissed the suit without prejudice, however, ruling that both the individual plaintiffs and the class lacked Article III standing as their alleged injuries were insufficiently concrete. However, on appeal, the Seventh Circuit reviewed the plaintiffs' damage allegations and overturned the district court's ruling, citing *Adobe* with approval. Specifically, the court found that because the hackers specifically targeted Neiman Marcus and actually stole the plaintiffs' credit card numbers, "there is no need to speculate as to whether [their] information has been stolen" and that waiting "for the threatened harm to materialize in order to sue" would only create more problems for the plaintiffs.

2. Substantive Claims

a. Federal Claims

i. *Claims Based on the Fair Credit Reporting Act (FCRA)*

1. In the context of data breach cases, bringing a FCRA claim requires a plaintiff to show that the defendant was a consumer reporting agency, such that the FCRA regulated the defendant's activities. Consumer reporting agencies must, under the FCRA, adopt procedures with regard to "confidentiality, accuracy, relevancy, and proper utilization" of the consumers' information. 15 U.S.C. § 1681(b) (emphasis supplied). Liability under the FCRA would exist only when the defendant "furnished" that information, in the form of consumer reports, in an unauthorized manner.

2. Recent data breach cases show a reluctance on the part of the courts to find either that the hacked entity was a reporting agency under the FCRA or that the data breach was an act of "furnishing" subject to the FCRA. *See, e.g., Willingham v. Global Payments, Inc.*, U.S. Dist. LEXIS 27764 (N.D. Ga. 2013) (hacked electronic transaction processor defendant not a "consumer reporting agency" and, even if it was, it did not furnish the plaintiffs' data to hackers—it was stolen).

3. Similarly, the Seventh Circuit rejected the plaintiff's argument that Advocate Health and Hospitals Corp. was such an agency. *Tierney v. Advocate Health & Hospitals Corp*. The court in that case found that the private information at issue, which the plaintiff alleged Advocate released to third parties as the result of insufficient securities procedures, were not "consumer reports" under the FCRA.

    a. Specifically, the court noted that the FCRA excludes reports that only contain information about a customer's experiences or transactions with the defendant entity, like those at issue in *Tierney*.

    b. The court also noted that Advocate was not a consumer reporting agency subject to the FCRA: it did not compile information about consumers for the purpose of furnishing consumer reports to third parties, either for fees or on a non-profit basis. Instead, it collected and transmitted information to obtain payment for its health care providers.

ii. *Claims Based on Employment Benefit Plans (ERISA)*

1. ERISA contains "expansive pre-emption provisions" to ensure that only federal courts regulate employment benefit plan claims. *Aetna Health Inc. v. Davila*, 542 U.S. 200, 208 (2004). As a result, for some benefit plan-related claims—those subject to so-called "complete preemption"—courts will not permit state-law causes of action that duplicate, supplant, or supplement ERISA's civil enforcement remedy. *Id.*

    a. This type of preemption thus functions as a jurisdictional doctrine, as it confers exclusive jurisdiction to federal courts for these claims, even those that, on their face, allege state law causes of action.

    b. Under *Davila*, courts use a two-pronged test to determine whether the plaintiff must bring her claim in federal court:

        i. If the plaintiff could, at some point in time, have brought the claim under ERISA § 502(a)(1)(B), and

        ii. The defendant's actions do not implicate any other independent legal duty.

2. Judge Koh, in the Northern District of California, utilized this test in refusing to remand plaintiffs' breach of contract claims to state court, finding that both prongs were satisfied. *See In re Anthem, Inc. Data Breach Litigation*, No. 5:15-cv-02874-LHK (N.D. Cal. Sept. 8, 2015).

    a. First, Judge Koh found that two of the named plaintiffs "could have brought their breach of contract claims under [ERISA]" because those plaintiffs "received health benefits during the relevant time period pursuant to employer-sponsored ERISA plans administered by Defendants." *Id.*

    b. Second, as the plaintiffs did not allege any other independent legal duty implicated by Anthem's conduct as it related to the breach of contract claim, the second prong was similarly satisfied. *Id.* Although the plaintiffs

did argue that the HIPAA notice provided to them by Anthem—and which they alleged Anthem breached—created an independent legal duty, the court disagreed, finding that the HIPAA notice was part of the agreement covered by ERISA, not a separate agreement.

c. However, in contrast to the *Anthem* decision, courts have found that simply asserting a claim that relates generally to an ERISA plan is insufficient to confer federal jurisdiction. For instance, in *Wickens v. Blue Cross of Cal., Inc.*, 2015 WL 4255129 (S.D. Cal. July 14, 2015), the court noted that an independent legal duty does not exist when the plaintiff's claim requires the court to interpret the terms of the ERISA-regulated benefits plan. That is, the benefits plan is an "essential part" of the plaintiff's claim and the defendant's liability exists *only* due to its administration of the plan. In *Wickens*, however, the court found that "Plaintiff's breach of contract claim is not based on the interpretation of the plan for benefits but based on an independent duty of an entity to protect the personal information of individuals if such information is required to be provided to the entity." *Id.* at *3.

3. Similarly, in *Rose v. Healthcomp, Inc.*, 2015 WL 4730173 *8 (E.D. Cal. Aug. 10, 2015), the court found "that Plaintiff's state law cause of action in this action could be brought if the ERISA plan did not exist. Therefore, the second prong is not met and Plaintiff's state law cause of action in this action arises independently of ERISA or the plan terms."

iii. *Consumer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030*

1. The CFAA is primarily a criminal statute, but provides a civil remedy of somewhat limited utility in the class data breach context. As the result of required predicate damages and limitations on who a plaintiff can sue, a plaintiff can only bring a cause of action under the CFAA against a corporation if the plaintiff suffered at least $5,000 in damages as the result of the defendant corporation unlawfully accessing the plaintiff's personal information. Note that this latter requirement means that only the entity which accessed the plaintiff's personal information may be sued under CFAA.

2. Several recent cases demonstrate the weight of the plaintiffs' burden when bringing CFAA claims: in one case, the court stated that a mere invasion of a statutory or constitutional right did not satisfy the damage requirement. *In re Google Android Consumer Priv. Litig.*, 2013 WL 1283236 (N.D. Cal. Mar. 26, 2013). In another, the court stated that not only did the plaintiffs similarly fail to satisfy the damage requirement, they also failed to show that the defendant accessed their data without authorization (and thus unlawfully) because they voluntarily installed the software at issue. *In re iPhone Application Litig.*, 844 F.Supp.2d 1040 (N.D. Cal. 2012).

iv. *Stored Communications Act (SCA), 18 U.S.C. § 2702*

1. Like data breach cases brought under CFAA, SCA claims present problems for plaintiffs due to specific statutory requirements.

2. In the case of the SCA, plaintiffs must show that the hacked defendant "knowingly" released the plaintiffs' confidential information. In other words, mere negligence is insufficient to constitute a SCA violation. Other requirements, such that the defendant provide a service "to the public," may present similar difficulties for plaintiffs. *See, e.g., Willingham v. Global Payments, Inc.*, U.S. Dist. LEXIS 27764 (N.D. Ga. 2013) (dismissing SCA claim because defendant's provision of electronic transaction processing services to merchants not a service "to the public," defendant did not "knowingly" divulge plaintiffs' information in hack, and plaintiffs failed to allege affirmative act on part of defendant).

b. State Law Claims

i. *Express/Implied Contracts*

1. Class plaintiffs seeking damages from a data breach must carefully research and plead a claim based on an implied contract.

a. For instance, in *Krottner v. Starbucks*, 406 Fed. Appx. 129 (9th Cir. 2010), hackers stole the plaintiffs' personal information in a breach of Starbucks' systems. Among other claims, the plaintiffs alleged that Starbucks breached an implied contract to encrypt and safeguard their personal information. In dismissing that claim, the court noted that although the plaintiffs pointed to three specific documents they claimed created the implied contract, they failed to allege offer and acceptance: the plaintiffs did "not allege that they read or even saw the documents, or that they understood them as an offer. Nor do they allege that they accepted the purported offer on its terms." The court further noted that the three documents did not include any terms requiring Starbucks to encrypt or safeguard the plaintiffs' data.

b. Plaintiffs must also be wary of the inherent tension between a defendant's affirmative representations in forming a contract and reliance issues. For instance, in *LinkedIn* (cited above), the court noted that the "crucial distinction" in that plaintiff's theory of economic injury was she alleged "her payment or overpayment was caused by LinkedIn's alleged misrepresentations, which she alleges she read and relied on in making her decision" to purchase the product.

2. If an express contract exists, choice of law provisions may prove helpful in obtaining certification of a class, although some courts (including the Washington Supreme Court) have noted that choice of law provisions resulting in the application of multiple states' laws in the same suit could result in the lack of predominance of common legal and factual issues. *See, e.g., Schnall v. AT&T Wireless Services, Inc.*, 171 Wn.2d 260 (2010).

ii. *Unjust Enrichment*

1. Allegations of unjust enrichment may create problems for plaintiffs at the class certification stage, particularly when the plaintiffs seek to certify a nationwide personal injury class.

2. For instance, in *In re ConAgra Peanut Butter* (cited above), the plaintiffs claimed that ConAgra had been unjustly enriched by selling tainted peanut butter (which, by virtue of its adulteration, was valueless). In examining this claim, the court noted the significant variations in all 50 states' unjust enrichment laws, with some states' tests including three elements, while other states' tests include two or even six elements. Many states even include a scienter requirement under which the defendant must have "awareness" of the benefit received. As a result, the court found that "the combination of significant individualized questions going to liability and the need for individualized assessments of damages precludes Rule 23(b)(3) certification."

iii. *Negligence* – beware of the economic loss rule

iv. *Fiduciary Duty*

1. Court have cast a skeptical eye at claims that a hacked retail defendant had—or breached—a fiduciary duty to safeguard a plaintiff's confidential data. For instance, in *Lovell v. P.F. Chang's China Bistro*, 2015 WL 4940371 (W.D. Wash. March 27, 2015), in which hackers obtained customer credit card information from the defendant restaurant, the court found that a restauranteur has no fiduciary duty to a patron. In dismissing the plaintiff's breach of fiduciary duty claim, the court noted that a fiduciary duty only arises when a party "has a duty, compelled by his undertaking, to act primarily for the benefit of another in all matters related to the undertaking."

2. By contrast, in healthcare data breach cases, insurers do stand in at least a quasi-fiduciary relationship with respect to their insureds. The use of confidential information provided by the insured to the insurer is a necessary component of the insurers undertaking with respect to its insured, and therefore the quasi-fiduciary relationship may extend to the protection of that information. The insurer is an integral (indeed, now legally mandated) party to the doctor patient relationship. Doctors *do* stand in a fiduciary relationship to their patients, and the providing of confidential information to the doctor by the patient is a key component of that relationship. Patients naturally and reasonably provide confidential information to doctors with the expectation that, as a fiduciary, that information will be kept confidential. Whether such a claim would survive and provide a basis for relief remains an open question.

3. However, in *Resnick v. Avmed, Inc.*, 693 F.3d 1317 (2012), the 11th Circuit reversed the district court's dismissal of the plaintiffs' breach of fiduciary duty claim. The court found that the plaintiffs—whose personal information was contained, unencrypted, on the defendant healthcare plan provider's stolen laptops—had, in fact, stated a claim for breach of fiduciary duty. In that case, the court examined the causation element of the plaintiffs' fiduciary duty

claim in the context of Florida law, which requires "damages flowing from the breach" of fiduciary duty. (The court did not address, and appeared to assume, the existence of AvMed's fiduciary duty.) The plaintiffs' allegation that thieves used the *same* stolen duty to steal their identities proved crucial for showing causation: the 11th Circuit suggested that, absent this causal connection, the plaintiffs' fiduciary duty claim (as well as other claims) likely would not have survived a motion to dismiss.

iv. *Bailment*

1. Although plaintiffs have alleged bailment in the context of data breach cases, the theory has yet to show much promise. In more than one case, courts have declined to find that property or personalty encompasses the personal information at issue in data breach cases.

2. For instance, *Enslin v. The Coca-Cola Company*, No. 2:14-cv-06476 (E.D. Penn. Sept. 9, 2015), the court stated that personal information "lost by a party holding that information was not 'property' or 'personalty' for the purposes of the law bailment." Courts examining the same claim in other data breach cases (notably *Ruiz v. Gap, Inc.*, *In re Sony*, and *In re Target*) reached similar conclusions.

v. *Fraud*

1. Although plaintiffs have brought fraud claims—which, in some cases, survived a motion to dismiss (*see, e.g.*, *In re Adobe Systems*)—based on failure to disclose lax data security practices, plaintiffs may also allege that a subsequent cover-up of the breach was also fraudulent.

2. For instance, under California's unfair competition law, an actionable fraudulent omission is one that is "contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose." *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835 (2006); *see also Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th 1544, 1557 (2007). In California, four circumstances exist in which a duty to disclose may arise: "(1) when the defendant is the plaintiff's fiduciary; (2) when the defendant has exclusive knowledge of material facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; [or] (4) when the defendant makes partial representations that are misleading because some other material fact has not been disclosed." *Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 255 (2011). "[A] fact is deemed 'material,' and obligates an exclusively knowledgeable defendant to disclose it, if a 'reasonable [consumer]' would deem it important in determining how to act in the transaction at issue." *Id.* at 256.

3. Thus, a hacked defendant would need to state affirmatively, for instance, that it had not been hacked, or that the hackers had not stolen any data. A defendant's failure to disclose a data breach—that is, fraud by omission—may

also support such a claim, particularly when many state statutes require such a disclosure.

c. State Statutory Claims

i. *California Confidentiality of Medical Information Act ("CMIA")*

1. The CMIA, Cal. Civ. Code § 56, *et seq*., broadly prohibits covered persons or entities from disclosing or releasing medical information without consent. An individual may recover actual damages or $1,000 in nominal damages for negligent disclosure of medical information. *See* Cal. Civil Code § 56.101. The CMIA applies to "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor " that deals with medical information. *Id.*

2. Although the CMIA's broad definitions and statutory damages provision would suggest the viability of a medical data breach claim with a concomitantly substantial damages award, recent court decisions significantly limit its utility in the class data breach context.

a. For instance, California appellate courts narrow construe the scope of the CMIA, including by requiring that the disclosed information be both individually identifiable and reveal something about the patient's medical history. *See Eisenhower Medical Center v. Superior Court*, 226 Cal. App. 4th 430, 435 (2014) (holding no release of medical information where the records in question included PII and a hospital medical record number).

b. The courts also require that plaintiffs plead, and ultimately prove, "that the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence." *Regents of Univ. of Cal. v. Sup. Ct.*, 220 Cal. App. 4th 549, 570 (2013); *see also Sutter Health v. Sup. Ct.*, 227 Cal. App. 4th 1546, 1556 (2014) (quoting *Regents*). In other words, the plaintiff must show that the "stolen medical information was actually viewed by an unauthorized person." *Sutter Health*, 227 Cal. App. 4th at 1.

ii. *Washington Unfair Business Practices Act (Wash. Rev. Code 19.86 et seq.)*

1. Washington's Consumer Protection Act, like other CPA statutes (see below), may prove useful in data breach cases in which the plaintiffs suffered less-obvious injuries. The CPA permits plaintiffs to recover based on the hacked defendant's deceptive acts and omissions, which, in the context of data breach cases, could include failing to maintain adequate data security practices, failing to disclose those inadequacies, and even failing to disclose the fact of the breach itself in a timely manner. Washington's statute also carries the possibility of treble damages.

a. The Third Circuit recently upheld the FTC's ability to bring an enforcement action based on a similar claim of an unfair practice—rather than a violation of a specific rule—under the unfairness prong of the FTC Act, 15 U.S.C. § 45(a). *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015)

b. In that case, the court held that Wyndham had fair notice that its data security practices fell short of the FTC Act's prohibition of unfair practices.

2. In data breach cases, plaintiffs may also seek to recover the difference between the amount they paid for the hacked company's services and the amount the product they received was actually worth, either under the auspices of a state CPA claim or under another theory—provided it does not run afoul of the economic loss rule.

3. Washington, like several other states, requires that entities disclose data breaches within a certain timeframe. Wash. Rev. Code. 19.255 *et seq.* In Washington, the entity suffering the breach must provide notice to affected residents and the state Attorney General in the most expedient time possible and without unreasonable delay, which the statute defines as no more than 45 days from the date of discovery. However, the statute allows longer notification delays when requested by law enforcement or if necessary to determine the scope of the breach and secure data systems.

iii. *Other States* - see attached state CPA laws appendix. These laws can vary widely in their applicability to class cases, as, for instance, some require pre-claim notice, while others explicitly prohibit class treatment of state CPA claims.

d. Conflict of Law/Choice of Law

i. *Class Cases*

1. In the context of class cases, courts look to whether the state statute at issue—typically a CPA statute or similar—is substantive or procedural, which in turn "governs whether the state law can trump Rule 23's federal class action mechanism." *Target*, 2014 WL 7192478 at *9. That is, "when a state legislature creates a private right of action to enforce a state statute's requirements, the state's definition of that private right of action to prohibit class actions defines the scope of the state-created right and is therefore substantive." *Id.* As a result, in states with prohibitions on class actions based in consumer protections statutes—ten states[1], as of this writing—plaintiffs cannot maintain class actions for consumer protection statutory violations.

2. Although Fed. R. Civ. P. 23(b)(3) requires that common questions of law predominate, courts applying the "most significant relationship" test examine a number of factors in determining which state's (or states') law or laws apply. Those factors are the location of the injury; the location of the conduct causing injury; the domicile of the parties; and the place where the parties' relationship is centered. *See Restatement (Second) of Conflict of Laws* (1971).

[1] Those states are Alabama, Georgia, Kentucky, Louisiana, Mississippi, Montana, South Carolina, and Tennessee, with Ohio and Utah prohibiting unless a final court judgment or state attorney general already declared the challenged act deceptive. *See Target* at *7.

a. In nationwide class cases, the domiciles of the class members may be the least important of the four factors, particularly because the choice of law inquiry is qualitative, not quantitative.

b. And, while the location of the plaintiffs' injuries may be their domicile state, "certain economic interests may be held—and may be injured—out of state," supporting application of the non-domicile state's law. Bobbitt v. Milberg LLP, No. 13-15812 (9th Cir. 2015).

ii *MDL Cases*

1. Generally, when state law governs, a "transferee district court must be obliged to apply the state law that would have been applied if there had been no change of venue." *Van Dusen v. Barrack*, 376 U.S. 612 (1964). In MDL cases, as in other diversity cases, courts will engage in the two-part inquiry, first evaluating whether state or federal law governs under *Erie*, then if state law applies, determining which state's law applies by using the choice of law principles of the forum state. *In re Volkswagen & Audi Warranty Extension Litig.*, 692 F.3d 4, 14 (1st Cir. 2012)
2. When a plaintiff files a case directly to the MDL, most courts will apply the choice of law principles of the originating jurisdiction, as otherwise the choice of law principles of the MDL's jurisdiction would govern every such case. *See, e.g., was Wahl v. Gen. Elec. Co.*, 786 F.3d 491, 496 (6th Cir. 2015) (collecting cases).
3. For cases that the MDL panel ordered transferred for consolidated proceedings, at least one circuit has found that the transferee court's application of the transferor court's jurisdiction's choice of law principles was proper. *See McKay v. Novartis Pharm. Corp.*, 751 F.3d 694, 697 (5th Cir. 2014). Note, however, that this does not necessarily mean that the law of the transferor court's own jurisdiction will apply; instead, it means that that the transferee court applies the state law that the transferor court would have applied. *See In re ConAgra Peanut Butter Prods. Liab. Litig.*, 251 F.R.D. 689, 693 (2008) (noting that "multidistrict judge[s] asked to apply divergent state positions on a point of law would face a coherent, if sometimes difficult, task").

iii. *State Law Example: Washington State*

1. Federal courts sitting in diversity jurisdiction must apply the forum state's choice of law principles to determine the controlling law.
2. In Washington, courts perform a two-step choice of law inquiry.
    a. First, they must find an actual conflict of laws.
    b. Assuming an actual conflict exists, the courts then apply the "most significant relationship" test to the particular issue.
    c. Washington follows the rule of dépeçage, under which the court may apply different forums' laws to different issues in the same

case, depending on which jurisdiction has the most significant relationship to the specific issue.

3. Conclusion

As these cases demonstrate, class data breach cases represent a rapidly developing area of law. As courts replace their initial hostility to these cases with a recognition of their role in providing data breach victims with recourse, data breaches will no longer occur without consequence for those with lax data security procedures.

For example, in retail data breaches, the current risk of loss for the lax-security retailer is minimal, provided if it complied with bank processing interchange rules in accepting debit and credit card transactions. As a result, class action claims by affected consumers against those retailers provide crucial accountability and, hopefully, result in retailers devoting more attention and resources to strengthening security procedures.

Until that happens, the plaintiffs' bar must pursue these cases with vigilance and creativity to provide remedies to injured consumers.