Legal Analysis

Data Breach Class Action Litigation – A Tough Road for Plaintiffs

By Timothy H. Madden

Introduction

With the increased prevalence of e-commerce, e-banking and other forms of electronic communication, and the attendant need to transmit or store sensitive personally identifiable information such as names, birth dates, social security numbers, financial account numbers and other similar data, the protection of this sensitive information has come under serious scrutiny. Many organizations, ranging from financial institutions to health care organizations to universities and retailers have suffered embarrassing occasions in which their customers', employees', students' or patients' personally identifiable information has either been accidentally lost or intentionally stolen. Naturally, the loss or theft of personally identifiable information — a "data breach" — has increasingly resulted in litigation, often brought as a class action on behalf of all of the hundreds, thousands or even tens of thousands of individuals whose personally identifiable information has been compromised.

An examination of the growing body of data breach-related case law reveals that unless plaintiffs can demonstrate that they have suffered actual harm, such as the fraudulent use of their financial

Timothy H. Madden is a Counsel at Bingham McCutchen LLP. Tim has guided clients through data breach situations, and has obtained the dismissal of resulting class action litigation.

information, courts have been reluctant to allow such litigation to proceed past the earliest stages, let alone to certify classes of plaintiffs or award damages. Massachusetts courts are no exception. This article will survey how courts in Massachusetts and elsewhere have treated these cases, assess why plaintiffs have had such difficulty finding success in this arena, and discuss an alternative enforcement mechanism that may cause businesses to pay greater attention to securing the confidential information they maintain.

Background

We all have heard of the biggest data breaches – TJX, Hannaford, Sony Playstation and others – with new ones seemingly reported every day. Literally thousands of organizations have suffered publicly reported data breaches in the years since the electronic transmission and storage of personally identifiable information has become increasingly widespread. Since 2005, there have been at least 2,600 known data breach incidents, affecting over 535 million records.[1] That pace breaks down to several new data breaches being reported each week.

Data breaches generally take one of two forms: the accidental loss of electronic records containing personally identifiable information (for example, a lost laptop, the accidental e-mailing of records, or the accidental loss of back-up tapes in transit); or the intentional and unauthorized intrusion into an organization's computer network and subsequent theft of information, often called "hacking." Because of the recent proliferation of state laws and regulations requiring prompt notice to individuals whose personal information is affected by a data breach, these incidents often result in public disclosure, and can lead to national media attention.[2] As a result of this public disclosure and media scrutiny, class action litigation is often filed virtually immediately upon disclosure of the existence of a data breach incident.

Arguably, the immediate filing of the claims may explain the lack of fraud or identity theft in some cases; in some, though, it may be that the data is never exploited, either because it doesn't wind up in the hands of criminals or because of advanced fraud controls now employed by financial and other

institutions. In those cases where the data breach has resulted in actual fraudulent use of personal information, plaintiffs have seen some success recovering their economic losses, whether it be in the courtroom or at the negotiation table. Where there is no demonstrable use of the compromised information, however, class action plaintiffs are forced to seek to recover damages related to the aggravation and emotional distress incurred, and time and money spent closing accounts, monitoring their credit, or worrying about and taking measures to guard against the potential for future fraud or identity theft. Plaintiffs have brought these claims under myriad legal theories, including negligence, breach of contract, breach of fiduciary duty, negligent misrepresentation, violation of state consumer protection laws such as Mass. General Laws ch. 93A, and others. Sometimes, class action plaintiffs also seek to invoke the protections of the various state data breach notification laws.[3] All of these types of claims, however, have faired poorly, in Massachusetts and elsewhere.

The Typical Data Breach Class Action Litigation: Case Dismissed

Courts across the country, including in Massachusetts, have not been receptive to data breach class actions absent the existence of actual, demonstrable economic harm to the plaintiff class. These cases have generally been dismissed, often on a Rule 12 but sometimes on Rule 56 motions, under one of two rationales: courts have generally held either that plaintiffs lack standing under Article III of the United States Constitution because with no harm there is no injury-in-fact and no case or controversy; or, that plaintiffs fail to make out the essential elements of their claims because they have suffered no recoverable damage.

Lack of Article III Standing

For a plaintiff to have Article III standing, three elements must be established:

First, the plaintiff must have suffered injury in fact – an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of…. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992). Where, as is the case in the vast majority of data breach class actions, the plaintiff merely alleges an increased risk of harm in the form of future fraud or identity theft, but no actual, present harm, courts have frequently held that such plaintiffs lack Article III standing.[4]

Failure to State a Claim

While the majority of data breach cases are decided on standing grounds, factually similar cases have been dismissed on the basis that plaintiffs failed to make out the essential elements of their claims, often because they have suffered no actual harm. In these cases, just like in the standing cases, plaintiffs usually allege that they have suffered emotional and/or financial harm related to their need to guard against future fraud or identity theft. Courts, however, have held that claims for potential future harm are too speculative to support a claim for damages. Some plaintiffs have even argued by analogy that data breach cases are similar to circumstances in which plaintiffs have been awarded damages related to their need to monitor for future occurrences of serious medical conditions, however courts have generally distinguished these cases on their facts and have not been inclined to accept this analogy.[5]

An example of a data breach case that was dismissed for failure to state a claim is *Belle Chasse Automotive Care, Inc. v. Advance Auto Parts, Inc.*, No. 08-1568, 2009 WL 799760 (E.D. La. March 24, 2009). There, the court granted the defendant's Rule 12(b)(6) motion to dismiss the plaintiffs' negligence claim stemming from an intrusion into the company's computer network. The court held that the plaintiffs failed to state a claim because they did "not allege that any third party accessed their information and stole their identities, or that any other concrete financial loss resulted from the alleged negligence." *Id*. at *4. *See also Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629 (7th Cir. 2007) (affirming dismissal of negligence claim related to data breach because expenses incurred monitoring credit not compensable harm). Courts have come to the same conclusion not just on negligence claims, but

also on data breach related claims alleging breach of contract, breach of fiduciary duty, negligent misrepresentation, alleged violations of state consumer protection laws and other tort claims.[6]

Have Data Breach Class Actions Fared Any Better in Massachusetts?

Simply put, no. While there have been only a few data-breach related cases resolved by Massachusetts courts, the outcomes of those cases have fit the above patterns. Where there is actual, demonstrable harm to the plaintiff class, claims have seen some success. But, where there is no demonstrable use of compromised personal information, Massachusetts courts have been no more receptive than other courts across the country.

In the case stemming from the data breach suffered by the TJX Companies, *In re TJX Comp. Ret. Sec. Breach*, 564 F.3d 489 (1st Cir. 2009), certain claims brought by banks that had issued credit cards compromised in the breach survived a motion to dismiss, at least in part because those banks could demonstrate that they had been required to reimburse cardholders for fraudulent transactions following the incident, and thus had suffered actual economic harm.

On the flip side, in a recent District of Massachusetts case, the plaintiff class pressed claims arising from the defendant's alleged failure to adequately protect class members' personally identifiable information in a manner consistent with the requirements of Massachusetts law and the defendants' marketing materials, and permitted unsecured (and unnecessary) access to employees (and thus, reasoned the plaintiffs, acted in an unfair and deceptive manner). *See Katz v. Pershing, LLC*, No. 10-1227, 2011 WL 1113198 (D. Mass. March 28, 2011). There, Judge Stearns granted the defendant's Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction, ruling that because the plaintiff did "not allege that any of her [personal information] has been lost, stolen, disclosed, or accessed by an unauthorized person[,]" "any potential injury that Katz might suffer at some point in the future because of a misappropriation of her [personal information] is far too speculative to satisfy standing requirements; therefore, she has failed to satisfy the injury-in-fact requirement." *Id*. at * 1.[7] While *Katz*

did not involve the theft or loss of personally identifiable information, and seems to leave the door slightly ajar for plaintiffs whose personal information is actually "lost, stolen, disclosed or accessed," the principles at issue translate and the *Katz* court relied upon and cited to more traditional data breach cases. When viewed in combination with established Massachusetts case law rejecting claims for damages related to solely future harm, *see, e.g., Urman v. South Boston Sav. Bank*, 424 Mass 165 (1997) (threat of future harm not recoverable as tort damages), it becomes clear that even in a more typical data breach case, absent allegations of actual harm suffered, Massachusetts courts are unlikely to allow plaintiffs to proceed past the earliest stages of litigation.

Is There Any Hope for Plaintiffs?

Given the near universal dismissal of data breach related class action litigation absent present, identifiable harm, is there any hope for plaintiffs in Massachusetts or elsewhere? The answer may be "not directly," but through enforcement actions brought by the Office of the Attorney General.

The Massachusetts Attorney General has, in at least one instance, brought claims under M.G.L. ch. 93A against a business that suffered a data breach. The Attorney General's claim related to the defendant's failure to comply with industry standards for the protection of personally identifiable information, and resulted in a settlement payment in the amount of $110,000. Notably, this claim was brought by the Attorney General prior to the effective date of 201 C.M.R. 17.00, the stringent regulations defining the "Standards for the Protection of Personal Information of Residents of the Commonwealth," yet the settlement requires compliance with those regulations and other industry standard protections.[8] For example, the settlement of this matter requires the defendant to implement, maintain and adhere to a written information security program, review its information security program annually, adhere to payment card industry compliance standards and implement increased security measures on its computer systems.

While this case could be seen as a precedent for private plaintiffs to bring suit under ch. 93A for an organization's unfair and deceptive failure to comply with industry standards and/or the stringent data security requirements found in 201 C.M.R. 17.00, it is doubtful that such a claim would survive a motion to dismiss absent allegations of actual loss. Even though the Attorney General need not prove actual harm as a basis for an enforcement action under ch. 93A, § 4, private plaintiffs do need to prove actual harm to state a claim for damages under ch. 93A, *see Hershenow v. Enterprise Rent-A-Car Company of Boston, Inc.*, 445 Mass. 790 (2006) (clarifying that actual loss caused by the defendant's conduct is an essential element under ch. 93A). This actual harm requirement, combined with the case law discussed in this article, makes it unlikely that a data breach plaintiff who could not prove demonstrable harm would survive under such a theory.

Conclusion

Any person affected by the loss of their confidential, sensitive personal information – which, by now, almost certainly includes you or someone you know – naturally feels violated and harmed by the experience. Nevertheless, unless there is an unlikely sea change in how courts deal with data breach litigation, it would appear to be the case that unless affected individuals have either suffered actual identity theft or been the victims of actual fraud – and can overcome the high hurdle of establishing a causal connection between that harm and the defendant's loss of their personal information – class action plaintiffs will likely remain unable to recover on claims resulting from a data breach.[9] ■

Endnotes

1. *See* http://www.privacyrights.org/data-breach (last visited August 9, 2011) (listing publicly available details of data breaches since 2005).

2. State data breach laws generally require that individual notice be provided as soon as practical to each person whose personally identifiable information has been compromised. Often, state laws also allow for alternative notice in the form of e-mails to affected individuals, a press release and/or publication of a notice in local media, where it is unduly costly or unfeasible to provide individual notice. *See, e.g.*, M.G.L. ch. 93H. For a full list of state data breach notification laws, *see*

http://www.ncsl.org/IssuesResearch/TelecommunicationsInformation Technology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (last visited August 9, 2011). Recently proposed federal legislation may soon preempt many of these state laws, in whole or in part. Among other discrete federal laws, the HITECH Act, 42 U.S.C. § 13001, *et seq*., requires notice by covered entities in cases where HIPAA-protected health information is compromised, and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, *et seq*., imposes similar obligations on covered financial institutions.

3. State data breach notification laws, however, generally do not provide for a private right of action, but instead require notice to regulators and affected individuals in the event of a covered data breach. *See, e.g.*, M.G.L. ch. 93H.

4 *See, e.g.*, *Hammond v. The Bank of New York Mellon Corp.*, No. 08-Civ-6060, 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) (claims stemming from accidental loss of back-up computer tapes containing personal information, no allegations of loss or actual damages); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046 (E.D. Mo. 2009) (claims arising from hacking incident, but no allegations of actual harm); *Randolph v. ING Life Ins. & Annuity Co*., 486 F. Supp. 2d 1 (D.D.C. 2007) (claims arising from stolen laptop, but no allegations of actual harm).

5 In *Donovan v. Philip Morris USA, Inc.*, 455 Mass. 215, 223-27 (2009), the Supreme Judicial Court held that cigarette smoker plaintiffs who had sustained some observable lung tissue damage could recover for expenses associated with monitoring for future development of lung cancer. However, it does not appear that any Massachusetts data breach plaintiffs have successfully argued that such a theory should equally apply to future harm related to financial fraud or identity theft resulting from a data breach incident.

6 A helpful fact (from a defense perspective) in many of these cases is that upon learning of the data breach, many of the defendants provided affected individuals with credit monitoring free of charge for some defined period of time, thus undermining any argument that plaintiffs incurred damage because they had no reasonable choice but to pay for such a service in order to protect against future loss.

7 *Citing Sea Shore Corp. v. Sullivan*, 158 F.2d 51, 56 (1st Cir. 1998) (“[f]uture injury must be imminent to qualify as injury-in fact” to ensure that the “alleged injury is not too speculative”).

8 See press release, “Major Boston Restaurant Group That Failed to Secure Personal Data to Pay $110,000 Under Settlement With AG Coakley” available at http://www.mass.gov/?pageID=cago pressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2011_03_28_briar_group_settlement&csid=Cago (last visited August 9, 2011).

9 It should be noted that while the vast majority of data breach cases are dismissed for the reasons described in this article, there are outlier cases in which claims have survived. *See, e.g., Rowe v. Unicare Life and Health Ins. Co.,* No. 09-2286, 2010 WL 86391 (N.D.Ill. Jan. 5, 2010) (denying Rule 12(b)(6) motion and permitting claim to proceed under Illinois law based on allegations of emotional distress and risk of future harm resulting from data breach in which personally identifiable information was temporarily available to the public via the internet).