Legal Backgrounder

WLF Washington Legal Foundation

Advocate for freedom and justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302

Vol. 24 No. 1 January 16, 2009

BUSINESSES' DATA COLLECTION: WHAT LEGAL RISKS EXIST AND WHO CAN SUE IF BREACHES OCCUR?

by

Kenneth K. Dort and Jeremiah J. Posedel

The lengthy list of data breaches occurring over the last few years – involving companies large and small, digital and analog, public and private – raises difficult questions going forward for any business that collects the personal information of its customers and/or employees. In particular, what is (i) the standard of care to be imposed on these companies by which to assess culpability in the event of future breaches, and (ii) the criteria by which a person whose data is compromised acquires standing to pursue an action against those companies?

What Security Is Necessary? The first question is critical because companies need a measure for assessing the appropriate level of resources to allocate to data protection to avoid exposure after-the-fact for any such data breaches/losses. As outlined below, this process will typically consider a variety of factors ranging from the sensitivity of the collected information to the volume of that information to the levels of access needed on a daily basis.

Who Can Sue? The second question is equally critical because it determines to whom companies will be liable and under what circumstances. In this regard, the recent decision in *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126 (N.D. Cal. 2008), raises the stakes considerably for businesses maintaining personal information databases.

Specifically, *Ruiz* arose out of the theft of two laptops containing personal information submitted with job applications to Gap. The plaintiff was an applicant whose data was on one of the stolen laptops. Significantly, there was no evidence that the plaintiff's identity had been stolen or misused following the theft. Nevertheless, in response to Gap's motion to dismiss, the court ruled that he had alleged the requisite "injury in fact" to pursue his claims against Gap due to nothing more than the *increased risk* of identity theft arising from the laptop thefts.

We will explore each of these considerations in turn below and the lessons businesses can draw from them to plan their security strategies.

Standards/Duties of Care. Many states impose (or plan to impose) on companies that maintain records of their customers' and/or employees' personal data a statutory obligation to implement systems by which to protect that data from breach and/or loss. These provisions are found in those statutes mandating public

---

Kenneth K. Dort is a partner with McGuireWoods LLP, a national law firm with international locations in both Europe and Asia. He practices in the firm's Technology & Business, Intellection Property and Complex Commercial Litigation Practice Groups, and based in the firm's Chicago office. **Jeremiah J. Posedel** is an associate with McGuireWoods. He practices in the firm's Technology & Business, Intellection Property and Complex Commercial Litigation Practice Groups, and is also based in Chicago.

notification of data breaches/losses. California's statute is a good example: "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." CAL. CIVIL CODE § 1798.81.5(b).[1]

Similarly, at the federal level, statutes such as the Graham-Leach-Bliley Act, Pub.L. 106-102, 113 Stat. 1338, and the Health Insurance Portability and Accountability Act of 1996, provide that companies coming within their sphere of coverage must implement systems sufficient to protect customers' applicable health or financial information. *See, e.g.*, 15 U.S.C. § 6801–6809 (implementing the so-called "Safeguards Rule" and 45 CFR § 164.312). These federal statutes are all "result-oriented" in that they do not impose specific requirements or characteristics on what types of systems should be utilized. However, they do provide that after a breach has occurred, the company must justify why the system they did implement was appropriate/reasonable at the time of the implementation.

At this point, there are no cases applying these provisions as to systems implementation or data losses. Nevertheless, given the statutes' uniform reference (again, using California's statute as an example) to "reasonable security procedures and practices appropriate to the nature of the information," it is logical that the likely standard of care is one of "reasonability" taking into account the type and importance of the information in question, the circumstances of the data collection, and the amount of information stored.[2]

To the extent that a given jurisdiction does not impose a statutory obligation to implement a security system, an alternate source of such an obligation might be a company's own representations to its customers during the collection process. Absent anything else, it is probable that the courts would impose a generic "reasonability" standard arising from the common law similar to that in question in *Ruiz*.

In any event, the safest bet for a company facing this situation would be to apply prospectively a "reasonability" test – taking into account the type of information collected; the potential harm to the customers should the data be compromised/accessed; the costs of differing levels of security; the harm to the company's own operations should that data be lost or compromised; and finally, the value to the company in avoiding the negative public relations associated with any potential data loss and the public notification thereof. Thus, in balancing these considerations, a company should be able to assess properly the level of security necessary for its particular data situation.

In reviewing this approach, a company might also consider the Federal Trade Commission's decision in *In the Matter of BJ's Wholesale Club, Inc.*, F.T.C. 042 3160, in which the Commission determined that BJ's had committed an unfair trade practice under federal law by not implementing a reasonable privacy/security policy with which to protect its customers' information. The issue arose when BJ's suffered a serious data breach, and contended that because it had no formal privacy policy, it had not violated any obligations to the customers whose data had been compromised. In response, the Commission concluded that the mere fact that it lacked any such privacy policy at all was a violation in itself. While the Commission has not addressed this situation in the context of a security system implementation for a company not otherwise bound under a specific statute or law, the *BJ's Warehouse* decision should provide any such companies with a clear warning of the pro-security direction in which the Commission is likely to go if and when it does consider that particular situation.

Accordingly, even if a company does not encounter a particular statutory or other legal obligation regarding the implementation of a data security system, best business practices would strongly suggest that all companies install and maintain such a system as appropriate to its particular data and business circumstances.

Standing. Having addressed the issue of what a company should consider in implementing a security system, the logical next question is who can pursue a claim against that company when a breach of its system

---

[1] *See also* the applicable state statutes at National Conference of State Legislatures website at http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm. Note that, of the forty-four states mandating notification following a breach, only California and Arkansas now statutorily mandate the implementation of a security system intended to prevent that breach.

[2] Note, however, the recent regulatory action in Massachusetts requiring specifically enumerated technical safeguards such as secure user authentication protocols, secure access control measures, firewall protection, encryption of all personal information stored on laptops. *See* 201 C.M.R. 17.00. These regulations were to take effect on January 1, 2009, but have been deferred to May 1, 2009.

occurs? Specifically, what type of harm must befall a person sufficient to allow him or her to proceed in court, that is, to have "standing"?

Ruiz v. Gap, Inc. As a matter of law, to have standing, a plaintiff must show that he or she has suffered an "injury in fact," that there is a causal connection between the defendant's conduct and the injury, and that the injury can be somehow remedied by a decision favorable to the plaintiff. The court addressed this issue in *Ruiz* in the plaintiff's favor, ruling that, at least at the pleading stage, the plaintiff's increased risk of harm arising from the theft was sufficient to allege an injury in fact.

Similarly, the court in *Ruiz* also ruled that this increased risk of theft constituted sufficient injury to sustain a negligence claim under California law. Most significantly, however, the court did advise the plaintiff that it was not sure what damages he would be able to demonstrate or recover if liability was to be determined at trial.

This latter point is critical – exactly what is the measure of damages under the circumstances at issue in *Ruiz*? Clearly, the victim of a data theft has suffered some degree of harm based on the existence of the increased risk of identity theft resulting from the breach. But is this enough? Consider that everyone at any time faces *some risk* of identity theft simply because their data is stored by third party businesses as part of those businesses' normal day-to-day activities (think banks, credit card companies, and employers). Now, assuming that a breach occurs, and assuming *arguendo* that the risk of identity theft does increase due to that breach, two questions arise: i) How do we measure the increased risk at issue (assuming we could measure the initial risk at all)? and ii) How do we value that increased risk?

Before *Ruiz*, courts in recent years considering this issue uniformly held that the mere risk of identity theft (increased or otherwise) caused by a data breach was insufficient to comprise the "injury in fact" required for legal actions. Thus, even if the breach itself was a violation of some duty owed to the customers or employees whose data was compromised, the absence of "injury" allowed the courts to dismiss the claims without need for additional proceedings. This was the case following the TJX data loss incident, in which the banks issuing credit cards to the affected TJX customers filed suit against TJX to recover their costs to change credit card numbers and to implement other proactive measures. The courts all dismissed these actions on the grounds that such costs were not caused by the breach, but rather were incurred in anticipation of possible future harm to its customers.

In response to these holdings, Minnesota has enacted a statute specifically providing that under such circumstances, the banks could in fact recover their costs from the business causing the breach or data loss. MINN. STAT. § 625E.64. However, these statutes apply to specific situations; they do not apply to the typical fact pattern considered in *Ruiz*.

The importance of *Ruiz* is that for the first time a court has allowed a case to proceed in the data loss arena despite the plaintiff's admitted lack of actual theft or financial harm. However, even the *Ruiz* court noted that it did not see how damages would be calculated at trial – signaling the possible entry of summary judgment short of trial if after the close of discovery the plaintiff could still not quantify his damages arising from the breach.

Thus, we get to our second question – how to value the increased risk of identity theft. While a direct calculation might remain difficult, an indirect means may exist. Note that it has become common for companies incurring a data loss to offer to the persons affected by the loss the opportunity to sign up for credit monitoring services provided by the large credit bureaus – TransUnion, Experian and Equifax. Typically, the companies pay the charges for these services on behalf of the affected persons. Because these charges provide the affected persons with almost real-time notice of changes to their credit reports, it provides them with the means to eliminate the risk of illicit activity affecting any of their accounts by notifying them of such actions and allowing them to react immediately to contravene that activity. In short, the cost of this service can be used as a proxy for the value of the increased risk caused by the data loss.

Using this approach, the *Ruiz* court might be inclined to award as damages whatever reasonable fees the plaintiff incurred to monitor his accounts to avoid greater damage in the future. This, of course, is why most companies readily agree to fund such services out of their own pocket – it is a logical calculation, it is a ready

way to mitigate much larger damages down the road, and it simply makes good business sense from a public policy perspective.

In essence, *Ruiz* appears to parallel the early products liability cases that moved away from negligence theories toward strict liability, reasoning that because sellers were the parties most able to identify and minimize the risks of poor manufacturing, they were thus the parties to incentivize by placing the burden of damage on them. This would appear to be the implicit basis for the *Ruiz* decision – the companies collecting the data are the ones most able to secure the data being collected, they are the ones most able to reduce the risks of data loss, and thus are the ones most able to spread the risk of loss throughout the system.

Garcia v. Lending Tree. This principle appears to be the basis for the case filed against online mortgage referral company Lending Tree in the Southern District of New York. In *Garcia v. Lending Tree, LLC*, Case No. 08 Civ 4551, filed in May 2008, former Lending Tree employees allegedly provided old passwords to mortgage lenders to allow the latter to gain unauthorized access to confidential customer financial information (such as names, addresses, phone numbers, Social Security numbers, and income data) on the Lending Tree system (initially submitted as part of various loan applications) and to access the credit reports for those customers. The lenders then allegedly used the information to market their services to those customers.

The plaintiff alleged that Lending Tree failed to implement adequate security measures to keep customers' information secure, and thus the customers "were, are or may be at risk for identity theft." *Garcia* Complaint at ¶16. As in *Ruiz*, there was no indication that any affected customer had suffered identity theft or any other actual harm. Unlike in *Ruiz*, the *Lending Tree* court never got the chance to rule on the merits of these allegations because on July 31, 2008, the plaintiff voluntarily dismissed the case without prejudice pursuant to FED. R. CIV. PRO. 41(a)(1).

Accordingly, while the *Ruiz* court clearly departed from the traditional notions of standing and actual harm (which the *LendingTree* court never had a chance to do), it may have started down a path on which the states themselves are already beginning to tread (at least in Minnesota, and possibly others).

Conclusions. *Ruiz* has expanded the traditional boundaries of standing and "injury." *Lending Tree* never got the chance. Nevertheless, *Ruiz* will likely incentivize companies to take steps that they are already taking (or should be) – namely, the implementation of comprehensive security systems where appropriate, and the undertaking of loss mitigation expenses to minimize the risk of actual loss arising from situations caused by their own system failures.

The last point is particularly important. The courts remain disposed against the *Ruiz* decision (as the *Ruiz* court may be also when discovery is concluded). However, it remains good business practice (particularly as a matter of public relations) for a company to stand ready to ameliorate that risk necessitated by the failure of its system with credit monitoring services. It is unclear whether *Ruiz* is a mere "frolic and detour" or the initial step in a new direction in the law of remedies, as the legislative action in Minnesota might suggest.

Only time will tell. At this point, the provision of credit monitoring services by companies experiencing a system breach, while not a legal obligation, should be seriously considered as a response to such a breach (apart from the actual notification itself). It would appear that the timely provision of credit monitoring services is an inexpensive means to address proactively both the public relations issues of a breach and the very real risk of harm to the individuals and businesses whose data was compromised.

  ISBN 1056 3059