THOMSON REUTERS

Westlaw®

# The damage vulnerabilities professionals face in the event of a data breach

**By Edward F. Donohue, Esq., *Hinshaw & Culbertson***

**MAY 18, 2018**

Data breach incidents involving large corporations and government agencies result in immediate media and public attention. However, damage exposure is often limited to mitigation costs, injunctions, regulatory fines and penalties.

Potential data breach targets maintain databases that in some cases include data relating to millions of consumers. However, the private personal information in those databases is often limited. Such data can include credit card numbers, Social Security numbers and driver's license numbers.

The controls on the dissemination of such information was limited before the enactment of the Gramm-Leach-Bliley Act in 1999. In addition, given the frequency with which consumers must disclose this information on the Internet and in commerce to this day and the efforts made to irreversibly pirate and distribute it, as a practical matter it is less "private" and often less sensitive than attorney-client records, physician medical records and the like.

> Even when identity theft victims can show they suffered direct economic loss from breaches leading to identity theft, the economic-loss doctrine has posed a hurdle for recovery.

Certain information, such as credit card numbers and personal passwords, can be cancelled and changed quickly as part of a response plan. In addition, under many state data breach laws, timely response and disclosure requirements serve to cap liability to consumers to certain established liquidated amounts.[1]

As a result, consumers affected by these incidents have been frustrated in their efforts to recover large sums based on the absence of sufficient proof of "injury in fact." Injury-in-fact is damage that either currently exists or is imminent as opposed to injury that is hypothetical or based on conjecture. *Berg v. Obama*, 586 F. 3d 234 (3d Cir. 2009).

However, a data breach and theft of records maintained by a professional potentially poses substantially greater risk for intrusion into personal privacy and proprietary information. This analysis discusses the common damage limitations applicable to businesses generally.

It also discusses the question of whether a professional may face greater damage exposure given the types of records that may be compromised.

## COMMON DAMAGE DEFENSES

The record of disfavor among many courts in allowing consumers to recover based on speculative and future harm is underscored by the fact that the U.S. Supreme Court has disallowed such recoveries based on threshold questions of standing.

In one case, *Clapper v. Amnesty International USA,*[2] against named defendant National Intelligence Director James Clapper, Amnesty International USA and other human rights, labor, legal and media organizations alleged that the National Security Agency engaged in unlawful and unconstitutional electronic surveillance practices that caused Amnesty International and others to undertake costly and burdensome measures to protect the confidentiality of their foreign communications.

The plaintiffs asserted the unlawful surveillance made their highly sensitive communications vulnerable to third-party access such that there was an objectively reasonable likelihood that their confidential communications would be intercepted in the future.

The court found that the plaintiffs had failed even to state a claim raising a genuine case or controversy under Article III of the U.S. Constitution. It held that the claim was predicated on a speculative chain of suppositions that the government would target the plaintiffs' communications and succeed in doing so.

The court held that preventative measures the plaintiffs had undertaken at their own expense to detect such unwanted surveillance did not support actual injury considering the lack of proof of actual or imminent — as opposed to future potential — injury.

*Clapper* has been widely followed for the proposition that the fact of a data breach compromising personally identifying information is not by itself sufficient to support standing without evidence that the compromised information was used to the direct detriment of the plaintiffs.[3] These cases have concluded that victims cannot establish standing "inflicting harm on themselves"[4] by taking proactive measures and incurring costs to reverse the effects of identity theft.

Courts have also rejected the more creative theory that plaintiffs can be harmed by their alleged loss of the "benefit of the bargain" with the company that failed to prevent a privacy breach of their data.[5]

On the other hand, when a significant number of plaintiffs can show that hackers have used pirated information to make fraudulent credit card charges, block access to bank accounts, and cause an inability to pay bills that leads to late payment charges, courts have recognized that these plaintiffs have legally cognizable claims.[6]

## IMPACT OF THE 'ECONOMIC LOSS' DOCTRINE

Even when identity theft victims can show they suffered direct economic loss from breaches leading to identity theft, the economic-loss doctrine has posed a hurdle for recovery.[7]

The economic-loss doctrine prohibits plaintiffs from recovering monetary damages in tort when allegedly a contract or implied contract exists.

The doctrine is important because its application constrains the availability of common law tort remedies for torts such as negligence. The actual injury suffered by the commission of a tort is generally considered foreseeable and thus recoverable. Unless the ultimate injury is so unusual based on intervening causes of loss or other extrinsic factors the courts will only limit liability on specific policy grounds.

A transactional attorney in a law firm may have records containing proprietary information and trade secrets that would be very damaging if publicized by a hacker.

Contract claims normally support only "economic loss" thus a defined out-of-pocket loss directly traceable to and foreseeable from the breach. Compensable injury is measured more liberally and generously under tort law.

Even courts that have allowed recoveries for injury caused directly by the mishandling of data have declined to allow claims for common law negligence based on the economic-loss doctrine.

For example, in *Enslin v. Coca-Cola Co.*[8] the plaintiff, a former Coca-Cola employee, traced the theft of his personally identifiable information and that of thousands of other former Coke employees to the theft of 55 laptops that were not password protected.

After Coca-Cola disclosed the loss to the former employees , the plaintiff was subjected to a broad-based takeover of his private personal information. His credit cards were used to facilitate numerous unauthorized purchases in locations as distant as Ireland.

Enslin also discovered that one identity thief even used his information to obtain a job at United Parcel Service. In short, the plaintiff's personal information had been widely dispersed among criminals, drawing him and other Coca-Cola employees into protracted and expensive efforts to regain control of their identities.

The court decided the plaintiff had established standing to sue and had stated viable claims for, among other things, breach of contract and restitution based on his employment relationship with the defendant. However, it also said the plaintiff had not and could not plausibly allege that he had suffered damage to his person or property. As such, the court dismissed his negligence and negligent misrepresentation claims based on the economic-loss doctrine.

The court explained that Pennsylvania, like most other states, does not impose a general duty of care supporting liability for general negligence in the absence of a "special" relationship such as a fiduciary relationship between the parties.

The court held that the employer-employee relationship did not rise to that of a special relationship generally or under the facts of the case. Thus, it said the plaintiff could not proceed with negligence claims.

## PROFESSIONAL LIABILITY FOR DATA BREACH

Though there may be no special relationship between employer and employee to enable a negligence claim, many professionals are deemed to stand in a special if not a fiduciary relationship with their clients. Thus, a good deal rides on the professional's ability to prove that the breached information was not misused in a way that harmed the client after a breach, as the government was able to do in *Clapper*.

The case of *Stacy v. HRB Tax Group Inc.*[9] is illustrative. There, tax preparation firm H&R Block Tax Services hired a tax preparer without conducting a criminal background check. Had it done so, it would have learned through records readily available from the Michigan Department of Corrections that the prospective employee had multiple convictions for her involvement in identity theft schemes using computers.

After she was hired, the employee used client taxpayer information to file six fraudulent tax returns with the IRS, all for her own personal gain. H&R Block maintained a computer information system that allowed its employees to access clients' information at each H&R Block location. The new employee accessed the clients' personal information through the computer system to file the fraudulent returns.[10]

The U.S District Court for the Eastern District of Michigan dismissed the clients' negligent hiring/supervision suit, holding that Michigan has never recognized any form of negligence, including negligent hiring, in contexts where the only injury suffered is economic in nature.

The 6th U.S. Circuit Court of Appeals reversed, also applying Michigan law.[11] The court, citing *Graves v. Warner Bros.*, 656 N.W.2d 195 (Mich. Ct. App. 2003), stated: "Because criminal activity by its deviant nature is normally unforeseeable, generally, there is no duty to protect another from the criminal acts of a third party in the absence of a special relationship between the defendant and the plaintiff or the defendant and the third party. ... Examples of the 'special relationships' Michigan law recognizes include: landlord-tenant, proprietor-patron, employer-employee, residential invitor-invitee, carrier-passenger, innkeeper-guest and doctor-patient."

In *Stacy*, the 6th Circuit also relied on *Bell v. Michigan Council 25*, No. 246684, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005), in holding that Michigan would find a special relationship exception applied if the tax preparation firm had been entrusted with the type of confidential client information that was misused to commit fraud.

Therefore, as in *Enslin*, the court recognized that the economic-loss doctrine did not bar claims for negligent hiring and negligent supervision by one in a special relationship.

The fiduciary or special relationship exception as applied to professionals is important for several reasons. First, as *Stacy* recognized, criminal conduct is not generally considered reasonably foreseeable, and a duty of care is generally recognized only if a special or fiduciary relationship exists. Thus, cases such as *Stacy* complement and provide the force of tort law to professional ethical mandates that a client's confidences be strictly protected.

Moreover, if the economic-loss doctrine does not insulate professionals from liability in cases involving a failure to foresee and guard against criminal conduct, then other tort theories may also apply.

As previously discussed, a standard data breach generally compromises massive amounts of personal data, such as credit card information, home addresses and telephone numbers. Some of the data is either publicly available or broadly disseminated by consumers to ordinary businesses.

It is difficult to obtain the individual authentication information one would need to cause economic injury. The data may never be exploited at the individual level given the breadth of the breach and the controls vendors can implement to detect and prevent misuse of customer information once the breach is identified.

However, as *Stacy* illustrates, professionals frequently possess much more sensitive information.

A transactional attorney in a law firm may have records containing proprietary information and trade secrets that would be very damaging if publicized by a hacker. Similarly, a litigation attorney's files may have confidential information on the guilt, innocence or culpability of a client that is a criminal or civil defendant.

Again, even if never used to obtain a penal or pecuniary advantage, the damage created by the release of such information is palpable whether or not it can be measured in economic terms.

For this reason, professionals may be vulnerable not merely to damage claims associated with the negligent release of basic private personal information. They may face invasion-of-privacy claims that have generally not been successfully prosecuted in data breach cases because the compromise of even large quantities of consumer information maintained by ordinary businesses involves more general information less susceptible to misuse irrespective of the scale of the breach.[12]

However, standing precedent in the invasion-of-privacy arena has not required proof of special compensatory damages in some situations.[13]

As discussed in the Restatement (2nd) of Torts Section 652H, the torts of defamation and invasion of privacy are closely related in that exposure to these torts results in personal injury violations that do not universally result in specific economic injury, generally defined as "special damages."[14]

Yet genuine personal injury in the form of subjective fear, shame or emotional distress can result. Specific economic injury from such torts is often difficult to establish and to remedy the genuine injury the claimant suffers. The inequity of barring all relief is manifest when highly personal and confidential information maintained by a professional is compromised and disseminated or exploited.

As in the case of defamation, in the future, the economic-loss rule may not serve as a bar to general damage claims against professionals responsible for maintaining the confidentiality of such information.

## CONCLUSION

On the surface, in the event of a data breach, professionals should have the same basic causation and speculative damage defenses that are available to any other business. Most hackers have no genuine interest in deriving anything other than ransom for holding a client's records hostage.

Nevertheless, in some instances, highly sensitive information will either be misused or published by those with no other motive beyond creating mischief. In those situations, the normal damage measures used in data breach cases are likely not reliable.

Certainly, the economic-loss doctrine may be on weak footing. Moreover, remedies borrowed from the analogous tort of defamation could pose liability risks beyond those that can be readily quantified by a client subject to similar reputational harm from an invasion of privacy.

## NOTES

[1] *See, e.g.,* CAL. CIV. CODE §§ 1798.82(d), 1798.83 (establishing "safe harbor" defenses under California's "Shine the Light" law for companies that make good-faith efforts to cure errors in providing notice and information on breach in accordance with the statute).

[2] 568 U.S. 398, 411-12 (2013).

[3] *In re United States OPM Data Sec. Breach Litig.,* 266 F. Supp. 3d 1, 38 (D.D.C. 2017); *Chambliss v. CareFirst Inc.,* 189 F. Supp. 3d 564, 571-72 (D. Md. 2016); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.,* 45 F. Supp. 3d 14, 35-37 (D.D.C. 2014).

[4] *See, e.g., Chambliss,* 189 F. Supp. 3d at 571-72.

[5] *Id.* at 572. *But see Enslin v. Coca-Cola Co.,* 136 F. Supp. 3d 654, 676-77 (E.D. Pa. 2015) (allowing potential restitution claim in context of employee victimized by identity theft).

[6] *Remijas v. Neiman Marcus Group LLC,* 794 F. 3d 688, 692-94 (7th Cir. 2015); *Enslin*, 136 F. Supp. 3d at 655-56; *In re Target Corp. Customer Data Sec. Breach Litig.,* 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014).

[7] *Enslin*, 136 F. Supp. 3d at 672-74.

[8] 136 F. Supp. 3d 654.

[9] 516 F. App'x 588 (6th Cir 2013).

[10] *Stacy v. H&R Block Tax Servs.,* No. 07-cv-13327, 2011 WL 3566384, at *2-3 (E.D. Mich. 2011), *rev'd in part sub nom. Stacy v. HRB Tax Grp. Inc.,* 516 F. App'x 588 (6th Cir. 2013).

[11] 516 F. App'x at 590-91.

[12] *In re OPM,* 266 F. Supp. 3d at 38.

[13] *See* RESTATEMENT (2D) OF TORTS § 652H, Reporter's Notes and citations therein.

[14] *Id. See also, e.g., Fairfield v. American Photocopy Equip. Co.,* 138 Cal. App. 2d 82 (Cal. Ct. App., 2d Dist. 1955).

*This article first appeared in the May 18, 2018, edition of* Westlaw Journal Computer & Internet.

## ABOUT THE AUTHOR

**Edward F. Donohue** is a partner in the San Francisco office of **Hinshaw & Culbertson**, where he focuses on representing professionals, including lawyers, in professional liability and defense matters. He has extensive experience handling directors' and officers' employment, agents and brokers, and financial institution bond liability claims. Donohue can be reached at EDonohue@hinshawlaw.com.