



by Carolyn A. Deverich, Brian R. Strange, and David A. Holop

# Into the BREACH

Plaintiffs have been increasingly  
successful in gaining injunctive relief  
for online security breaches

AS OUR INCREASINGLY digital world encompasses everything from banking to birthdays, the personal information available on Web sites and stored in electronic databases continues to grow exponentially. Many of us have the intimate details of our lives stored in online databases, including our addresses, phone numbers, birth dates, Social Security numbers, credit card and bank account information, and Web site user names and passwords. All this data is vulnerable to theft, through means as simple as stealing the hardware on which the data is stored or through complex, remote cyber-theft by sophisticated hackers.

In the past few years, the frequency of data security breaches has skyrocketed. One estimate puts the number of records breached

since 2005 at over 500 million.<sup>1</sup> Some of the largest security breaches occurred at:

- TJX Company, with an exposure of 45 million customer credit and debit card account numbers.
- TD Ameritrade, involving 6 million files of customer contact information.
- The Gap, unveiling the private information of over 750,000 job applicants.
- Starbucks, revealing the private information of over 97,000 Starbucks employees.
- Citibank, involving the potential exposure of names, account numbers, and contact information for 360,000 credit card customers.
- Sony, with a potential compromise of the confidential account and financial information of 144 million Sony PlayStation, Qriocity,

and Sony Online Entertainment Network users, including over 1 million unencrypted credit card numbers.<sup>2</sup>

When consumers' personal information is breached, they face an immediate and immeasurable injury involving the loss of security,

---

**Carolyn A. Deverich, an associate at Strange & Carpenter, specializes in class action and data breach litigation. Brian R. Strange, the founding partner of Strange & Carpenter, focuses his practice on class action and complex business litigation, with a specialty in Internet privacy and antitrust class actions. He is currently serving on the plaintiffs' steering committee in *In re Sony Gaming Networks and Customer Data Security Breach Litigation*. David A. Holop, an associate at Strange & Carpenter, specializes in class action litigation.**

increased risk of identity theft, and potential invasion of privacy. With the loss of security, consumers may suffer emotional distress worrying about lost privacy and identity risks. They may spend money and time to forestall these dangers by purchasing credit monitoring services, monitoring credit and bank accounts, and seeking to cancel current debit and credit cards. They also may lose opportunities due to unavailable credit or a decline in their credit ratings. Businesses, too, suffer enormous losses whenever sensitive and confidential company data has been breached. Damages arising from the exposure of confidential corporate financial and business information can be enormous, not to mention the potential liability that arises when confidential consumer or employee information maintained on a company's system is breached.

Courts have tried to apply traditional damage models in assessing these damages, with mixed results. A number of courts have turned to the economic loss doctrine in analyzing injuries from potential identity theft, finding that plaintiffs are barred from recovery for alleged breach of tort duties when a contractual relationship exists between the plaintiff and the defendant and the losses are purely economic. Other courts are finding that the dangers and risks associated with exposing a plaintiff's private and personal information to hackers may be cause to expand the parameters of online security breach liability. Courts appear increasingly willing to offer at-risk plaintiffs what they really seek—security.

This trend first emerged when courts analyzed the reach of Article III of the U.S. Constitution to cases involving a breach of online security. Federal courts have an independent obligation at the outset of every case to ensure the plaintiff has standing.<sup>3</sup> Along with causation and redressability, one of the key elements of standing is injury-in-fact. A plaintiff must show that he or she “has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical.”<sup>4</sup> This requirement is an important issue in data breach cases when the plaintiff alleges harm based on the increased risk of identity theft that arises from the breach.

The courts that have addressed the standing issue are split. Some find the risk of future harm to be enough to meet the injury-in-fact test, while others do not. The Seventh Circuit first recognized standing based on this type of alleged injury in 2007 in *Pisciotta v. Old National Bancorp.*<sup>5</sup> with the Ninth Circuit following suit in 2010 in *Krottner v. Starbucks Corporation.*<sup>6</sup> Both the courts in *Pisciotta* and *Krottner* found that an act that harms the plaintiff only by increasing the risk of future

harm to the plaintiff is enough to confer standing.

The courts reached this result by relying on a line of cases finding injury-in-fact in analogous situations in which the defendant's actions had increased the plaintiff's risk of future harm, including exposure to toxic substances,<sup>7</sup> the use of a defective medical implant,<sup>8</sup> environmental harms,<sup>9</sup> and even an increase in discretion given to an ERISA plan administrator.<sup>10</sup> The Ninth Circuit also cited to *Doe v. Chao*,<sup>11</sup> in which the Supreme Court found Article III standing based on the plaintiff's allegation that he “was ‘torn...

**The fact that a plaintiff has suffered a breach of his or her data security but has not experienced actual identity theft should not bar recovery. Courts have long held that the risk of injury is compensable when there is an adequate remedy for the risk.**

all to pieces’ and ‘greatly concerned and worried’ because of the disclosure of his Social Security number and its potentially ‘devastating’ consequences.”<sup>12</sup>

However, the Sixth Circuit in *Lambert v. Hartman*<sup>13</sup> was more skeptical of the injury from the increased risk of identity theft, calling it “somewhat ‘hypothetical’ and ‘conjectural.’”<sup>14</sup> Some district courts have similarly held they lack subject matter jurisdiction because plaintiffs whose data has been breached, but not yet misused, have not suffered a sufficient injury-in-fact.<sup>15</sup> But most of these cases were decided before the trend started by the Seventh Circuit in *Pisciotta*, and cases decided since have typically found the increased risk of identity theft to be sufficient for standing.<sup>16</sup> Yet even assuming the trend to find injury-in-fact continues, plaintiffs will still need to prove the merits of their claims for damages—a completely separate issue from standing.

Claims for injury due to the increased risk of identity theft have included:

- Tort claims, such as negligence and strict liability.
- Contractual claims, such as breach of express or implied contract or warranty.
- Statutory claims, such as state unfair consumer practices acts or privacy acts.

For recovery under any of these claims, plaintiffs generally must suffer actual injury or damage. When consumers have suffered actual identity theft that has led to fraudulent charges or some other present financial harm,

courts have generally allowed these claims to go forward to the extent the plaintiff can show actual damage.<sup>17</sup> The issue is less clear when plaintiffs have not suffered identity theft but rather face an increased risk of identity theft and the accompanying burden of dealing with this threat.

### Tort Damages

The classic negligence claim requires proof of harm to the plaintiff: “Negligent conduct in itself is not such an interference with the interests of the world at large that there is any right to complain of it, or to be free from it,

except in the case of some individual whose interests have suffered.”<sup>18</sup> Negligence does not compensate individuals for the general nuisances of life but ordinarily requires proof of some personal injury or property damage.

Some argue that the loss of time and effort expended dealing with a potential security breach (including the need to request new credit and debit cards, monitor accounts for fraudulent charges, and convince banks and credit card companies that any fraudulent charges should be reversed) and the heightened risk of identity theft constitute a nuisance and nothing more. Indeed, some courts examining the issue of damages resulting from the exposure of private and sensitive consumer data have found that when there is no actual theft of identity, mere economic losses caused by the heightened risk of theft are not compensable.<sup>19</sup>

These courts have attributed their findings to state common law damage requirements and to the oft-misapplied economic loss doctrine.<sup>20</sup> While state common law differs from federal law in the definition of the level of necessary harm,<sup>21</sup> the general principle expressed by these courts is that the harm suffered by those whose personally identifiable information is compromised may be enough to meet the standing requirement, but the traditional negligence requirements of actual, present, and cognizable injury are not sufficiently present to state a claim.<sup>22</sup>

Nevertheless, this automatic bar from tort recovery seems inconsistent with other author-

# MCLE Test No. 211

The Los Angeles County Bar Association certifies that this activity has been approved for Minimum Continuing Legal Education credit by the State Bar of California in the amount of 1 hour.

1. Over the past five years, the frequency of data security breaches has decreased.  
True.  
False.
2. Pursuant to Article III of the U.S. Constitution, a plaintiff has standing in federal court if the plaintiff has suffered an "injury in fact" that is "concrete and particularized" and "actual or imminent."  
True.  
False.
3. The Seventh Circuit was the first circuit to recognize Article III injury-in-fact based upon risk of future harm caused by a data breach.  
True.  
False.
4. All circuits have followed the Seventh Circuit finding that a data breach that harms a plaintiff only by increasing the risk of future harm is enough to confer Article III standing.  
True.  
False.
5. Plaintiffs have brought claims for increased risk of identity theft due to data breach under various theories except:  
A. Negligence.  
B. Defamation.  
C. Unfair consumer practices.  
D. Breach of contract.
6. The Sixth Circuit has stated that waiting for a plaintiff to suffer injury before allowing any legal recourse may be harsh and economically inefficient.  
True.  
False.
7. Courts have held that plaintiffs who have been exposed to health or medical risks are entitled to medical monitoring, even when the plaintiffs have not yet shown physical harm.  
True.  
False.
8. The Ninth Circuit considered—but did not grant—monitoring relief to data breach plaintiffs in *Stollenwerk v. Tri-West Health Care Alliance*.  
True.  
False.
9. Emotional distress damages are typically not available in contract cases even when actual harm is proved.  
True.  
False.
10. More than 40 states have passed laws that create a civil cause of action for failure to secure data.  
True.  
False.
11. Texas enacted the first data breach security law.  
True.  
False.
12. The California Security Breach Information Act does not require businesses to notify consumers when their data has been breached.  
True.  
False.
13. Illinois expressly allows for recovery of economic losses in data breach cases by deeming a violation of the state's data breach statute to also be a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act.  
True.  
False.
14. Which state recently considered a bill that would authorize "any person who is affected by a security breach that creates a risk of harm of identity theft" to sue for actual or statutory damages?  
A. Montana.  
B. New York.  
C. California.  
D. Hawaii.
15. California recently passed a bill that requires restitution payments from criminal defendants to their identity theft victims.  
True.  
False.
16. The American Recovery and Reinvestment Act of 2009 includes a nationwide data breach notification law.  
True.  
False.
17. The HITECH Act allows covered entities to wait up to a year before notifying individuals whose "protected health information" has been breached.  
True.  
False.
18. The Veterans Benefits, Health Care, and Information Technology Act of 2006 requires the Department of Veterans Affairs to provide free credit monitoring to parties affected by a data breach if there is a "reasonable risk" for misuse of the information.  
True.  
False.
19. In data breach settlements approved by courts over the past few years, the relief includes free credit monitoring services to at-risk parties and identity theft funds to reimburse losses and related expenses stemming from the security breach.  
True.  
False.
20. In *Claridge v. RockYou, Inc.*, the district court judge ruled that claims for breach of contract and negligence based on potential identity theft could proceed.  
True.  
False.

## MCLE Answer Sheet #211



### INTO THE BREACH

Name \_\_\_\_\_

Law Firm/Organization \_\_\_\_\_

Address \_\_\_\_\_

City \_\_\_\_\_

State/Zip \_\_\_\_\_

E-mail \_\_\_\_\_

Phone \_\_\_\_\_

State Bar # \_\_\_\_\_

### INSTRUCTIONS FOR OBTAINING MCLE CREDITS

1. Study the MCLE article in this issue.
2. Answer the test questions opposite by marking the appropriate boxes below. Each question has only one answer. Photocopies of this answer sheet may be submitted; however, this form should not be enlarged or reduced.
3. Mail the answer sheet and the \$20 testing fee (\$25 for non-LACBA members) to:

Los Angeles Lawyer  
MCLE Test  
P.O. Box 55020  
Los Angeles, CA 90055

Make checks payable to Los Angeles Lawyer.

4. Within six weeks, Los Angeles Lawyer will return your test with the correct answers, a rationale for the correct answers, and a certificate verifying the MCLE credit you earned through this self-assessment activity.
5. For future reference, please retain the MCLE test materials returned to you.

### ANSWERS

Mark your answers to the test by checking the appropriate boxes below. Each question has only one answer.

- |     |                               |  |
|-----|-------------------------------|--|
| 1.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 2.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 3.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 4.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 5.  | <input type="checkbox"/> A    | <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D |
| 6.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 7.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 8.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 9.  | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 10. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 11. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 12. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 13. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 14. | <input type="checkbox"/> A    | <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D |
| 15. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 16. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 17. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 18. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 19. | <input type="checkbox"/> True | <input type="checkbox"/> False   |
| 20. | <input type="checkbox"/> True | <input type="checkbox"/> False   |

ity. The *Restatement (Second) of Torts* states that one “whose legally protected interests have been endangered by the tortious conduct of another is entitled to recover for expenditures reasonably made or harm suffered in a reasonable effort to avert the harm threatened.”<sup>23</sup> The Sixth Circuit has noted that “there is something to be said for...prevention, as opposed to...treatment. Waiting for a plaintiff to suffer physical injury before allowing any redress whatsoever is both overly harsh and economically inefficient.”<sup>24</sup> At least one court has held that a plaintiff who alleged “that she spent considerable time, as well as money, making long distance calls, contacting the various credit rating agencies in order to get the fraudulent accounts closed and prevent future fraudulent activity under her name” stated a claim,<sup>25</sup> though the court did not indicate how her damages were to be calculated.

The fact that a plaintiff has suffered a breach of his or her data security but has not experienced actual identity theft should not bar recovery. Courts have long held that the risk of injury is compensable when there is an adequate remedy for the risk.<sup>26</sup> For example, the Southern District of Ohio found in *Day v. NLO* that when the plaintiffs had been exposed to excessive radiation due to the defendants’ negligence, the plaintiffs were entitled to medical monitoring—even though the plaintiffs had not shown any physical harm but were merely at risk from the exposure.<sup>27</sup> The court explained:

From a certain perspective this remedy seems to violate the courts['] traditional reluctance to allow recovery for “risk of injury.” However, the courts['] concerns over damages which are uncertain, speculative, or conjectural are overcome by the reasonableness of compensation for diagnostic tests in cases where liability has been established. The safeguard against speculative recovery is the reasonableness of the procedures ordered in light of the tortious act.<sup>28</sup>

Other courts, including some in California, have held the same: At-risk plaintiffs who have been exposed to harm but have not yet exhibited injury may recover the costs of monitoring the potential injury to ensure that if the injury does occur, it will be properly treated.<sup>29</sup>

This principle fits perfectly within the circumstances of security breaches. Plaintiffs are not exposed to harm in the form of physical injury but instead to harm in the risk to the injury of their personal identities. The relief for this risk of injury is analogous too. Instead of medical monitoring, the remedy for the risk is credit monitoring to ensure the customer’s economic health.

The Ninth Circuit has considered this type of monitoring relief.<sup>30</sup> In *Stollenwerk v. Tri-West Health Care Alliance*, the plaintiffs alleged that the defendant failed to secure their personal information when burglars broke into the defendant’s headquarters and stole equipment and hardware, including computers on which the plaintiffs’ personal information was stored.<sup>31</sup> The court noted that “one [might] appl[y] a similar [medical monitoring] standard to determine the availability of damages for the cost of credit monitoring in instances of exposure of personal information.”<sup>32</sup> However, under the particular facts of that case—the only proof of personal data exposure was the burglary, which involved “a range of hardware...not just the servers containing customers’ personal information,” and there was “no evidence the thieves had any interest in their personal information, rather than just the hardware”—the court held that “the risk [of identity theft]...was low,” so the plaintiffs could not recover.<sup>33</sup>

In contrast, a number of the more recent security breaches involve intrusion directly into the databases containing users’ personal data, so the risk of identity theft or other misuse is high. Credit monitoring is the ideal relief in these situations.

### Contract Damages

Contract-based claims have faced a similar dilemma. Like the requirements for tort claims, some courts have held that plaintiffs must prove actual damages resulting from the alleged breach.<sup>34</sup> Contract damages are typically even more limited than tort damages. The usual relief is to give the aggrieved party the benefit of his or her bargain. Emotional distress damages are generally not available in contract cases even when actual harm is proved.<sup>35</sup> Some courts analyzing contract claims have found that, as with negligence claims, the increased risk of identity theft does not give rise to compensable damages.<sup>36</sup>

Nevertheless, contract claims have not been completely barred in security breach cases. In a suit against AOL for the disclosure of users’ search histories, a federal district court upheld a number of California statutory claims on a motion for judgment on the pleadings.<sup>37</sup> The court found that the plaintiff’s purchase of AOL’s services, coupled with AOL’s failure to provide what was bargained for—keeping the plaintiffs’ information private—proved sufficient to sustain the claims.<sup>38</sup> In another case involving UniCare Life and Health Insurance’s breach of its customers’ private information, numerous claims, including breach of implied contract, survived a motion to dismiss.<sup>39</sup> The plaintiffs’ injuries involving severe emotional distress,

increased risk of future harm, credit monitoring, and harm to their possessory interest in their personal health information met the federal pleading standard.<sup>40</sup>

Last year, U.S. District Court Judge Phyllis J. Hamilton in the Northern District of California allowed claims for breach of contract and negligence based on the potential for identity theft to proceed in *Claridge v. RockYou, Inc.*<sup>41</sup> Defendant RockYou, a developer of online services, allegedly failed to secure and protect its users’ sensitive personally identifiable information, including e-mail addresses, passwords, and login credentials. The plaintiffs brought a number of claims. The state statutory claims were struck down, but the breach of contract, breach of implied contract, and negligence claims were not. Specifically, the court held that the “plaintiff has sufficiently alleged a general basis for harm by alleging that the breach of his [personally identifiable information] has caused him to lose some ascertainable but unidentified ‘value’ and/or property right inherent in the [personal information].”<sup>42</sup> Judge Hamilton’s decision opens the door for other judges to follow suit.

### Statutory Damages

Statutory-based claims generally require lost money or property damages or some other tangible form of injury.<sup>43</sup> However, many statutes do not require a showing of actual damages.<sup>44</sup> No state has yet passed a statute giving rise to statutory damages based specifically on the increased risk of identity theft from a data breach, but this type of law may be enacted in the future.

Legislation is beginning to play a role in the area of damages for data breaches. Many states have passed laws that create a civil cause of action for failure to secure data. The first law of this kind, which served as a model for many other state laws, was California’s Security Breach Information Act (California SBIA). Passed in 2003, the California SBIA imposes on businesses a duty of notification to those who suffer an unauthorized intrusion into their personal data.<sup>45</sup> At last count, there are 46 states—as well as Washington, D.C.; Puerto Rico; the U.S. Virgin Islands; and New York City—that impose a duty of notification when a security breach has occurred. The California SBIA also contains a data protection obligation and expressly authorizes the maintenance of a suit for damages for breach of that duty<sup>46</sup>—another trend followed by other states in their laws. However, these laws provide no guidance on what damages are available. Moreover, other states with notification statutes do not provide for private causes of action,<sup>47</sup> while others only assess civil penalties.<sup>48</sup>

PRIVATE CLUB  
545 SOUTH FIGUEROA STREET, LOS ANGELES, CA 90071

THURSDAY  
MARCH 8, 2012

# USC LAW REAL ESTATE 12

USC GOULD SCHOOL OF LAW 2012 REAL ESTATE LAW AND BUSINESS FORUM

**learn about new directions and how  
to play them to your advantage**

**Register Now  
Early Bird  
Rates End  
February 17**

## AGENDA

### MORNING

Commercial Real Estate Markets in the U.S.: Value Trends, Capital Markets, and Managing Risk  
• The California Economy and Future Trends in Real Estate Investment • Using Available Land Use Tools to Thrive in Uncertain Times • Office and Retail Lease Protections for Landlords and Tenants • The Peaks and Valleys in the Investment Landscape of California • Bonus Breakfast Session: Career Options After Ten Years of Practice

### AFTERNOON

Luncheon Keynote by USC Law Professor Edward McCaffery • What's Going on in Redevelopment  
• Practical Tips for Maximizing the Benefits of a CMBS Financing • Is Chapter 11 a Viable Option for Real Estate Companies? • CEQA Reform in 2011 and the Future • Opportunities for Hotels in a Volatile Market  
• Outlook for Investments in Distressed Debt • Quick Hits on Hot Topics

### CLOSING

"Meet the Speakers and Network" Annual Wine and Cheese Reception

### NATIONALLY KNOWN SPEAKERS INCLUDE:

William Anderson • Kelly Broughton • Mark Fluent • Paul Fuhrman • Mayor Bill Fulton (ret.)  
• Sally Gordon • Scott Grossman • Emile Haddad • Hugh Hilton • Professor George Lefcoe  
• Michael Lehrman • Jeff Lugosi • Steven Marcussen • Judge Bruce Markell (Nev. Dist.)  
• Kelly Martin • Christopher Meany • Hessam Nadji • Cynthia Nelson • Senator Alex Padilla  
• Eric Paulsen • Chip Sellers • Troy Senik • Kevin Shannon • Sabeth Siddique • Patricia Sinclair  
• Glenn Sonnenberg • Lawrence Souza • John Tamny • Jason Thomas • Christopher Thornberg  
• Thomas Whitesell • Homer Williams • William Witte • plus dozens of other real estate stars!

Earn CLE/CPE/DRE credits

**Special discount for co-sponsors and local bar association members**

Register online now at <http://law.usc.edu/cle/realestate>



At least one state, Illinois, allows for recovery of economic losses in data security cases by expressly providing that a violation of the state's data breach statute is deemed to also be a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act.<sup>49</sup> The Illinois Deceptive Trade Practices Act permits a "person who suffers actual damage...[to recover] actual economic damages or any other relief which the court deems proper," including "reasonable attorney's fees and costs."<sup>50</sup> This still requires actual damages but allows for recovery upon merely a showing of economic loss.

No state to date has passed a law providing for statutory damages without a showing of actual damages from identity theft. Early in 2011 Hawaii considered a bill that would authorize "any person who is affected by a security breach that creates a risk of harm of identity theft" to sue for actual or statutory damages.<sup>51</sup> Nevertheless, its future is unclear. A bill was passed in 2011 in California that requires restitution payments from criminal defendants to their identity theft victims, including credit report monitoring and credit repair costs.<sup>52</sup> These bills may indicate a trend toward potential statutory relief for victims of the increased risk of identity theft.

Federal security breach laws are not far behind. The American Recovery and Reinvestment Act of 2009 includes a nationwide data breach notification law as part of its Health Information Technology for Economic and Clinical Health Act (the HITECH Act).<sup>53</sup> The HITECH Act requires entities covered by the statute to immediately notify individuals whose "protected health information," including medical records and other individually identifiable health information, has been breached.<sup>54</sup> Both the Department of Health and Human Services and the Federal Trade Commission have issued rules or regulations designed to implement the notification requirements of HITECH.<sup>55</sup>

The Veterans Benefits, Health Care, and Information Technology Act of 2006 requires the Department of Veterans Affairs to provide notice to veterans of a breach of their personal data. Moreover, the department also must 1) notify law enforcement and certain congressional committees when a data breach occurs, 2) perform a risk analysis if unauthorized access to sensitive personal information occurs, and 3) notify and provide free credit monitoring to those affected if there is a "reasonable risk" for misuse of the information.<sup>56</sup>

A number of other bills have been introduced in Congress that would require companies to safeguard sensitive personal data and notify consumers about data security breaches.<sup>57</sup> Consistent federal legislation pro-

viding statutory relief for victims of increased risk of identity theft may be following soon.

### Injunctive Relief

Presuming that courts and statutory law continue to move toward remedying injured data breach victims, what is the proper form of relief? When plaintiffs' private information has been exposed, putting them at risk of identity theft, the primary relief that plaintiffs seek is

**The *RockYou* holding may be the beginning of a move toward an expanded understanding of damages in these cases. In addition, the security monitoring injunctive relief approved by multiple courts in settlements suggests that the threat of identity theft is a remediable injury with concrete available relief.**

security. In the handful of data breach settlements approved by courts over the past few years, the parties and the courts (in approving the settlements) have consistently found that the best way to remedy the risk of identity theft is to provide injunctive relief. This involves free credit monitoring services to at-risk parties along with identity theft insurance or funds to reimburse identity theft losses and related expenses that stem from the security breach. These remedies rectify immediate damages to plaintiffs who have already suffered identity theft from the breach as well as provide protection to plaintiffs who are at risk for identity theft. In some cases, the relief also will cover future damages to plaintiffs who experience identity theft after the settlement.<sup>58</sup>

For example, in the Countrywide breach litigation settlement, class members were offered two years of credit monitoring and identity theft insurance, as well as reimbursements of out-of-pocket expenses resulting from the theft of their private information (such as costs for replacement checks, driver's licenses, and the like) and reimbursement for losses from identity theft. This relief was contingent on the loss being actual and not already reimbursed and more likely than not a result of the alleged theft of private information through Countrywide's breach.<sup>59</sup> The court approved this settlement, noting that it "offers a reasonable resolution that properly addresses the tricky issues presented by data breaches."<sup>60</sup>

The court approved similar relief in the TJX breach case.<sup>61</sup> In the TD Ameritrade litigation, the court rejected two settlements

but has approved a third settlement that sets up a fund to pay for identity theft claims.<sup>62</sup> Courts in these settled cases have viewed the provision of credit monitoring services and funds for payment of future losses to be adequate forms of security to ensure that the harmed plaintiffs can recover for their losses. These settlements illustrate the type of injunctive relief judges should consider in security breach cases moving forward.

Plaintiffs seeking to recover money damages based solely on the increased threat of future identity theft and their accompanying expenses incurred in increased monitoring have faced a tough battle in the courts. The damage requirements of tort and contract law, as well as many statutes, have prevented a number of claims from proceeding. At the same time, no clear consensus and no authoritative decision preclude these cases, and some courts have shown a willingness to move away from traditional damage models to remedy untraditional security breach injuries.

The *RockYou* holding may be the beginning of a move toward an expanded understanding of damages in these cases. In addition, the security monitoring injunctive relief approved by multiple courts in settlements suggests that the threat of identity theft is a remediable injury with concrete available relief. This is a burgeoning area of law that will play out in courtrooms and legislatures in the years to come. ■

<sup>1</sup> See Privacy Rights Clearinghouse, <http://www.privacyrights.org/data-breach#CP> (last visited Dec. 30, 2011) (542,967,619 records exposed from 2,835 data breaches in the United States since 2005).

<sup>2</sup> *Id.*; In re Sony Gaming Networks & Customer Data Sec. Breach Litig., MDL No. 11-2258 (S.D. Cal. 2011); Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2009).

<sup>3</sup> *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 95 (1998); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

<sup>4</sup> *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

<sup>5</sup> *Pisciotta v. Old Nat'l Bancorp.*, 499 F.3d 629, 633-

34 (7th Cir. 2007).

<sup>6</sup> Krottnier v. Starbucks Corp., 628 F. 3d 1139, 1141-43 (9th Cir. 2010); *see also* Ruiz v. Gap, Inc., 380 Fed. Appx. 689, 690-91 (9th Cir. 2010) (unpublished).

<sup>7</sup> *See* Denney v. Deutsche Bank AG, 443 F. 3d 253, 264-65 (2d Cir. 2006).

<sup>8</sup> Sutton v. St. Jude Med. S.C., Inc., 419 F. 3d 568, 570-75 (6th Cir. 2005).

<sup>9</sup> Central Delta Water Agency v. United States, 306 F. 3d 938, 947-48 (9th Cir. 2002); Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F. 3d 149, 160 (4th Cir. 2000) (en banc).

<sup>10</sup> Johnson v. Allsteel, Inc., 259 F. 3d 885, 887-88 (7th Cir. 2001).

<sup>11</sup> Doe v. Chao, 540 U.S. 614 (2004).

<sup>12</sup> *Id.* at 617-18, 624-25.

<sup>13</sup> Lambert v. Hartman, 517 F. 3d 433, 437 (6th Cir. 2008).

<sup>14</sup> *Id.*

<sup>15</sup> *See, e.g.,* Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 6-8 (D. D.C. 2007); Bell v. Axiom Corp., No. 4:06CV00485-WRW, 2006 WL 2850042, at \*2 (E.D. Ark. Oct. 3, 2006) (unpublished); Key v. DSW, Inc., 454 F. Supp. 2d 684, 689-91 (S.D. Ohio 2006); Giordano v. Wachovia Sec., LLC, Civil No. 06-476 (JBS), 2006 WL 2177036, at \*2-5 (D. N.J. July 31, 2006) (unpublished); Hammond v. The Bank of New York Mellon Corp., No. 08 Civ. 6060 (RMB)(RLE), 2010 WL 2643307, at \*1-2 (S.D. N.Y. June 25, 2010) (unpublished); Allison v. Aetna, Inc., Civil Action No. 09-2560, 2010 WL 3719243, at \*4-6 (E.D. Pa. Mar. 9, 2010).

<sup>16</sup> *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1051 (E.D. Mo. 2009); *see also* McLoughlin v. People's United Bank, Inc., No. 3:08-cv-00944 (VLB), 2009 WL 2843269, at \*4 (D. Conn. Aug. 31, 2009) (unpublished) (citing cases).

<sup>17</sup> *See, e.g.,* In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 133 (D. Me. 2009), *rev'd in part*, Anderson v. Hannaford Bros. Co., 659 F. 3d 151 (1st Cir. 2011).

<sup>18</sup> W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS §30, at 165 (5th ed. 1984).

<sup>19</sup> *See, e.g.,* In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A. 3d 492, 496 (Me. 2010).

<sup>20</sup> *See, e.g.,* Banknorth N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206, 211-14 (M.D. Pa. 2006); In re TJX Cos. Retail Sec. Breach Litig., 524 F. Supp. 2d 83, 90-91 (D. Mass. 2007), *aff'd*, 564 F. 3d 489, 498 (1st Cir. 2009); Pennsylvania State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 326-30 (M.D. Pa. 2005).

<sup>21</sup> For example, in California the damages element of negligence requires "appreciable, nonspeculative, present injury." Aas v. Superior Court, 24 Cal. 4th 627, 646 (2000).

<sup>22</sup> *See, e.g.,* Pisciotta v. Old Nat'l Bancorp, 499 F. 3d 629, 639-40 (7th Cir. 2007).

<sup>23</sup> RESTATEMENT (SECOND) OF TORTS §919 (1979) (emphasis added).

<sup>24</sup> Sutton v. St. Jude Medical S.C., Inc., 419 F. 3d 568, 575 (6th Cir. 2005).

<sup>25</sup> Kuhn v. Capital One Fin. Corp., No. 05-P-810, 2006 WL 3007931, at \*3 (Mass. App. Ct. Oct. 23, 2006) (unpublished).

<sup>26</sup> Edward J. Imwinkelried, *Redress for Loss of Private E-Data*, TRIAL, Feb. 2009, at 48, 51.

<sup>27</sup> Day v. NLO, 851 F. Supp. 869, 880 (S.D. Ohio 1994).

<sup>28</sup> *Id.*

<sup>29</sup> *See* Potter v. Firestone Tire & Rubber Co., 6 Cal. 4th 965, 1005-10 (1993); Miranda v. Shell Oil Co., 17 Cal. App. 4th 1651, 1657 (1993); Duncan v. Northwest Airlines, Inc., 203 F.R.D. 601, 607 (W.D. Wash. 2001); Laxton v. Orkin Extermination Co., 639 S.W. 2d 431, 434 (Tenn. 1982); Merry v. Westinghouse Elec. Corp.,

684 F. Supp. 847, 852 (M.D. Pa. 1988).

<sup>30</sup> Stollenwork v. Tri-West Health Care Alliance, 254 Fed. Appx. 664 (9th Cir. 2007) (unpublished).

<sup>31</sup> *Id.* at 665.

<sup>32</sup> *Id.* at 666.

<sup>33</sup> *Id.*

<sup>34</sup> *See, e.g.,* Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 917-18 (N.D. Cal. 2009), *aff'd*, 380 Fed. Appx. 689, 690-91 (9th Cir. 2010) (unpublished).

<sup>35</sup> *See* McAfee v. Wright, 651 A. 2d 371, 372-73 (Me. 1994).

<sup>36</sup> *See, e.g.,* Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 779-80 (W.D. Mich. 2006).

<sup>37</sup> Doe 1 v. AOL LLC, 719 F. Supp. 2d 1102, 1109-14 (N.D. Cal. 2010).

<sup>38</sup> *Id.* at 1111-12.

<sup>39</sup> Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010) (unpublished).

<sup>40</sup> *Id.* at \*4-9.

<sup>41</sup> Claridge v. RockYou, Inc., 785 F. Supp. 2d 855 (N.D. Cal. 2011).

<sup>42</sup> *Id.* at 865.

<sup>43</sup> *See, e.g.,* Hall v. Time Inc., 158 Cal. App. 4th 847, 849 (2008); BUS. & PROF. CODE §17204.

<sup>44</sup> *See, e.g.,* Arcilla v. Adidas Promotional Retail Operations, Inc., 488 F. Supp. 2d 965, 972-74 (C.D. Cal. 2007).

<sup>45</sup> *See* CIV. CODE §§1798.80 *et seq.*

<sup>46</sup> CIV. CODE §§1798.81.5, 1798.84(b).

<sup>47</sup> *See, e.g.,* COLO. REV. STAT. §6-1-716 (2011).

<sup>48</sup> *See, e.g.,* FLA. STAT. §817.5681 (2011).

<sup>49</sup> 815 ILL. COMP. STAT. 505/1 *et seq.* (2011).

<sup>50</sup> 815 ILL. COMP. STAT. 505/10a (2011).

<sup>51</sup> S.B. 728, 2011 Sen., Reg. Sess. (Haw. 2011), *available at* [http://www.capitol.hawaii.gov/session2011/bills/SB728\\_.pdf](http://www.capitol.hawaii.gov/session2011/bills/SB728_.pdf).

<sup>52</sup> PENAL CODE §1202.4(f)(3)(L).

<sup>53</sup> HITECH Act of 2009, Pub. L. No. 111-5, §§13001-421, 123 Stat. 115, 226-79, 42 U.S.C. §17932.

<sup>54</sup> *Id.* at §13402, 123 Stat. at 260-63.

<sup>55</sup> 74 Fed. Reg. 42,740 at 743 (to be codified at 45 C.F.R. pts. 160, 164) (Aug. 24, 2009); 74 Fed. Reg. 42,962 (to be codified at 16 C.F.R. pt. 318) (Aug. 25, 2009).

<sup>56</sup> Pub. L. No. 109-461, §902, 120 Stat. 3403, 3450-60, 38 U.S.C. §§5721-28.

<sup>57</sup> *See, e.g.,* S. 1326, 109th Cong. (2005); S. 1408, 109th Cong. (2005); S. 1789, 109th Cong. (2005); H.R. 4127, 109th Cong. (2005); H.R. 3997, 109th Cong. (2005); H.R. 5318, 109th Cong. (2006); S. 1408, 112th Cong. (2011); S. 1535, 112th Cong. (2011).

<sup>58</sup> *See, e.g.,* In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., No. 4:09-MD-2046, Settlement Agreement, at 13 (S.D. Tex. Dec. 18, 2009) (providing for identity theft losses up to August 1, 2011—two and a half years after the announcement of the breach, and one and a half years after settlement). Potential plaintiffs who opt out of the settlement have the right to pursue individual claims for damages arising before or after the settlement agreement.

<sup>59</sup> In re Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01998, 2009 WL 5184352, at \*8 (W.D. Ky. Dec. 22, 2009) (unpublished).

<sup>60</sup> *Id.* at \*5-6.

<sup>61</sup> In re TJX Cos. Retail Sec. Breach Litig., No. 07-10162, Motion for Settlement, at 4 (D. Mass. Dec. 20, 2007). *See also* In re TJX Cos. Retail Sec. Breach Litig., No. 07-10162, slip op., at 7 (D. Mass. Sept. 2, 2008) (calling the relief "fair, adequate, reasonable, proper, and in the best [interests] of the Settlement Class").

<sup>62</sup> In re TD Ameritrade Account Holder Litig., No. C 07-2852 VRW, 2011 WL 4079226 (N.D. Cal. Sept. 13, 2011).

## DOUBLE BILLING APPROVED!

Earn 6.5 hours of MCLE credit while taking traffic school (live or) online.



**MCLE 4 LAWYERS**  
CALIFORNIA TRAFFIC SCHOOL

[www.mcle4lawyers.com](http://www.mcle4lawyers.com)

(310) 552-5382

DMV license no. TVS 1343 - Since 1997



**Anita Rae Shapiro**

SUPERIOR COURT COMMISSIONER, RET.

**PRIVATE DISPUTE RESOLUTION**

PROBATE, CIVIL, FAMILY LAW

PROBATE EXPERT WITNESS

TEL/FAX: (714) 529-0415 CELL/PAGER: (714) 606-2649

E-MAIL: [PrivateJudge@adr-shapiro.com](mailto:PrivateJudge@adr-shapiro.com)

<http://adr-shapiro.com>