2011

Credit-Monitoring Damages in Cybersecurity Tort Litigation

Vincent R. Johnson
St. Mary's University School of Law, vjohnson@stmarytx.edu

CREDIT-MONITORING DAMAGES IN CYBERSECURITY TORT LITIGATION

Vincent R. Johnson[*]

INTRODUCTION

When someone improperly accesses or discloses an individual's personal information, the subject of that data breach is often at an increased risk of identity theft.[1] One way for an affected data subject to guard against this risk is to subscribe to a credit-monitoring service. In this type of arrangement, a business reviews information, generally on a daily basis, from one or more of the major credit-reporting agencies.[2] When a change in the data subject's credit history occurs, such as the unauthorized opening of a new account in the victim's name, the service alerts the data subject.[3] As a result, the victim of a data-security breach can take prompt action to minimize the consequences of identity theft and can, perhaps, avoid financial ruin.[4] Remedial steps may include closing an unauthorized account, placing a fraud alert in a credit-reporting agency's files, freezing distribution of credit reports, or obtaining a declaratory judgment that the data subject is the victim of identity theft, which may aid the data subject in dealing with law enforcement authorities.[5]

---

[*] Professor of Law, St. Mary's University School of Law. Yale University, LL.M.; University of Notre Dame, J.D.; St. Vincent College, B.A., LL.D. Professor Johnson's books include: STUDIES IN AMERICAN TORT LAW (4th ed. 2009) (with Alan Gunn); MASTERING TORTS: A STUDENT'S GUIDE TO THE LAW OF TORTS (4th ed. 2009); and ADVANCED TORT LAW: A PROBLEM APPROACH (2010).

[1] *See generally* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 256-57 (2005) (discussing the potential adverse consequences of database intrusion). The fact that data disclosure increases the risk of identity theft is so well established that some defendants do not contest the issue. *See* Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391, at *5 (N.D. Ill. Jan. 5, 2010) (noting that the defendants responsible for personal information being temporarily available on the Internet did "not seem to challenge whether Rowe and the purported class members were put at a 'substantial risk' of identity theft or some other harm").

[2] *See Credit Monitoring Services: A Comparison*, AAACREDITGUIDE.COM, http://aaacreditguide.com/credit-monitoring-services/ (last visited Sept. 20, 2011).

[3] *See id.*

[4] *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008 (N.H. 2003) ("Victims of identity theft risk the destruction of their good credit histories. This often destroys a victim's ability to obtain credit from any source and may, in some cases, render the victim unemployable or even cause the victim to be incarcerated."); *see also* Guillermo Contreras, *Key Figure Admits Guilt in Huge ID Theft Case*, SAN ANTONIO EXPRESS-NEWS, Apr. 6, 2011, at 2B (indicating that victims of identity theft found it hard to get loans and faced "lingering headaches in trying to straight[en] things out").

[5] *See* Johnson, *supra* note 1, at 259-61 (discussing remedial and preventive options); *see also* James Graves, Note, *"Medical" Monitoring for Non-Medical Harms: Evaluating the Reasonable Ne-*

Credit-monitoring services will not detect the unauthorized use of existing accounts or types of data misuse unrelated to credit,[6] such as fraudulent presentation of credentials to obtain employment or medical care.[7] However, credit monitoring is particularly useful in detecting the opening of new accounts in the victim's name, which is an especially potent form of identity theft.[8]

Recently, potential cybersecurity defendants have provided credit-monitoring services to affected data subjects voluntarily.[9] In addition, courts have approved credit-monitoring compensation as part of class-action settlements[10] and sanctioned defendants by requiring them to provide credit monitoring or to reimburse the costs of such services.[11] These developments demonstrate that credit-monitoring expenditures are both reasonable and necessary when a serious breach of data security occurs.[12]

As this Article shows, compensation for credit monitoring is both analogous to court awards for medical monitoring[13] and justified under ordinary tort principles. Furthermore, the economic-loss rule[14] should not bar recovery of credit-monitoring damages because the data-protection obligations imposed by state and federal data-security laws are not a proper subject for private bargaining. Indeed, courts have held that such agreements are against public policy.[15] If a data possessor negligently and seriously breaches cybersecurity, an affected data subject should be able to recover the resulting costs of credit monitoring regardless of whether identity theft ever occurs.

By requiring data possessors to cover credit-monitoring costs, courts will deter breaches of cybersecurity. Data possessors will have an incentive to implement reasonable precautions to guard against unauthorized data access and to avoid unnecessarily risky practices related to the handling and

---

cessity of Measures to Avoid Identity Fraud After a Data Breach, 16 RICH. J.L. & TECH. 1, ¶¶ 71-78, at 50-56 (2009) (discussing credit freezes and fraud alerts); *see also* 112 AM. JUR. *Trials* § 19 (2009) (discussing specific steps a lawyer should take in representing a victim of credit monitoring); Tim Trainor, *Hard to Prevent Identify Theft*, MONT. STANDARD, Dec. 19, 2010, at A2 (stating that, in Montana, persons can "fill out an identity theft passport that proves to creditors and law enforcement officers that someone has used a victim's identity to commit fraud").

6 *See* Graves, *supra* note 5, ¶ 70, at 50 (discussing some of the problems with credit-monitoring services).

7 *See id.* ¶ 53, at 36 (distinguishing between "new account fraud, existing account fraud, and non-financial fraud").

8 *Fighting Back Against Identity Theft*, FED. TRADE COMMISSION, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Sept. 20, 2011).

9 *See infra* Part II.B.

10 *See infra* Part II.C.

11 *See infra* Part II.D.

12 *See infra* Part II.E.

13 *See infra* Part III.

14 *See infra* Part I.C.2.

15 *See infra* Part I.C.2.

storing of digital personal information.[16] Moreover, judicial recognition of this element of damages will tend to reduce the costs of cyber-related losses by shifting credit-monitoring costs to cheaper cost avoiders and spreading data-protection costs to the classes of people who benefit from commercial use of computerized personal information.[17] Thus, treating credit-monitoring damages as compensable is not only consistent with basic legal principles and established tort theories but also supported by several principles of public policy that have played a major role in shaping contemporary American tort law.

Part I of this Article provides an overview of the importance of credit monitoring and of tort claims related to cybersecurity. It also discusses the duty to protect digital personal information and to disclose breaches of cybersecurity, as well as the reasons why the economic loss rule should not bar claims for the costs of credit monitoring. Part II of this Article discusses the precedent dealing with credit-monitoring damages, related business practices, class-action settlements, and judicial and administrative sanctions. Part III explores the issue of whether credit-monitoring damages are analogous to the medical-monitoring damages that many states award to victims of toxic exposure. Part IV then considers arguments against the compensability of credit-monitoring damages in cybersecurity lawsuits. These include the alleged lack of present injury in cases where the plaintiff has not experienced identity theft and the ability of potential plaintiffs to self-protect against economic harm by purchasing credit-monitoring services. Part V then explains why courts should allow victims of data-security breaches to recover compensation for the costs of credit monitoring. The Article argues that protection from identity theft should be as widespread as commercial use of computerized personal information and that businesses should be required to internalize the costs of their negligent data practices. In many instances, businesses are well-situated to efficiently spread identity theft prevention costs among those who benefit from the use of computerized personal information. Finally, this Article concludes that plaintiffs should be able to recover credit-monitoring costs often in cybersecurity litigation.

I. UNCERTAIN COMPENSABILITY

Credit monitoring has become not only a common method of protecting the security of personal information but also a common claim for damages in tort litigation. This Part discusses how credit monitoring is both affordable and effective. It provides an overview of the starting assumptions related to any discussion of whether credit-monitoring damages are

---

16 *See infra* Part V.A.

17 *See infra* Part V.B.

recoverable in cybersecurity cases. Those assumptions relate to the duty to protect data and disclose breaches of security and to the economic-loss rule.

A. *Issue of Widespread Importance*

Basic credit monitoring is not expensive,[18] at least when it concerns only one individual.[19] However, breaches of database security (sometimes called "cybersecurity") occur frequently[20] and often affect thousands,[21] or even millions,[22] of persons.[23] This is especially true in cases of unauthorized

---

[18] *Comparison of Credit Monitoring Services*, KNOWZY (June 22, 2011, 7:43 PM), http://www.knowzy.com/credit-monitoring-comparison.htm (showing that credit-monitoring costs can range from $8.95 to $29.95 per month). *But see* David Lazarus, *Spend the $15 a Month on Debts, Not on an Online Debt Organizer*, L.A. TIMES, Jan. 25, 2011, at B1 ("[I]f your problem is that you owe businesses too much money . . . you can probably live without daily credit monitoring . . . .").

[19] Experian's "Triple Alert" credit-monitoring service, which sells for $8.95 per month, bills itself as the "most affordable credit monitoring product on the market today." TRIPLEALERT.COM, https://www.experiandirect.com/triplealert/default.aspx (last visited Sept. 20, 2011). Other more expensive forms of credit monitoring, such as Experian's Triple Advantage product, bundle reports based on daily review of the three major credit-reporting agencies with other benefits. Triple Advantage "monitors a person's credit files, sends email alerts of suspicious activity, and allows a person to check their credit reports." *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). "The Experian Guarantee guarantees the 'Triple Advantage' product up to $1 million for identity theft losses." *Id.*; *see also* David Christianson, *Monitoring Your Credit's Health*, WINNIPEG FREE PRESS, Jan. 7, 2011, at B4 (placing the cost of credit monitoring at $15 per month, including identity theft insurance); Daniel Wolfe, *Regions Offers $5 Anti-Fraud Services*, AM. BANKER, Jan. 28, 2011, at 10 (stating that for five dollars per month, Regions Financial Corp. offers "credit monitoring, real-time transaction monitoring for up to 10 payment cards, and up to $2,500 in identity theft insurance. The card-monitoring service alerts consumers of potentially fraudulent activity within 24 hours of its occurrence"). Some lawsuits involve claims where plaintiffs seek to recover the costs of credit monitoring but also the cost of insurance against losses that may result from identity theft. *See In re* Killian, No. 05-14629-HB, 2009 WL 2927950, at *2 (Bankr. D.S.C. July 23, 2009) (indicating that the plaintiff unsuccessfully sought $25.00 per month for credit-monitoring services where the cost included "insurance to cover the cost of any actual identity theft that may occur while the credit monitoring services are in place" (internal quotation marks omitted)).

[20] Two sites compile up-to-date lists of security breaches, *Chronology of Data Breaches*, PRIVACY RTS. CLEARINGHOUSE (Sept. 18, 2011), http://www.privacyrights.org/data-breach, and *Data Breaches*, IDENTITY THEFT RESOURCE CENTER, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml (last visited Sept. 13, 2011) (including data from 2005-2011).

[21] *See* Paul v. Providence Health Sys.-Or., 240 P.3d 1110, 1112 (Or. Ct. App. 2010) (discussing the theft from a car of computerized disks and tapes containing unencrypted records relating to 365,000 patients); Samara Kalk Derby, *UW Warns 60,000 of Card Data Theft*, WIS. ST. J., Dec. 10, 2010, at A7 (discussing the hacking of the identification card information of tens of thousands of former students, faculty, and staff members, which placed social security numbers at risk).

[22] *See* John Markoff, *Hackers Said to Breach Google Password System*, N.Y. TIMES, Apr. 20, 2010, at A1 (discussing the breach of a password system that "controls access by millions of users worldwide to almost all of [Google's] Web services").

[23] *See generally* Jane E. Kirtley, *Privacy Protection, Safety and Security*, *in* 2 COMMUNICATIONS LAW IN THE DIGITAL AGE 2010, at 15, 29-31 (2010) (discussing "a list of notable data breaches"); Jane

intrusions into the data held by credit card issuers,[24] mortgage[25] and student-loan[26] lenders, universities,[27] banks,[28] online marketers,[29] and large employers.[30] In such instances, credit-monitoring expenditures can cost millions of dollars.[31] Thus, it is not surprising that some businesses and other defendants charged with negligent failure to protect personal data or to reveal information concerning unauthorized access have disclaimed responsibility for the costs of credit monitoring.[32] On the other hand, plaintiffs in cybersecurity cases often argue that defendants are responsible for such amounts and for other expenses as well.[33]

Whether plaintiffs can recover the costs of credit monitoring in tort actions is important for a variety of reasons, including whether qualified counsel is willing to represent affected persons in class action litigation. It is usually difficult for at-risk data subjects to prove that defendants are re-

---

K. Winn, *Recent Developments in the Emerging Law of Information Security*, 38 UCC L.J. 391, 400-02 (2006) (discussing numerous data security breaches).

24 *See, e.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 584 F. Supp. 2d 395, 397 (D. Mass. 2008) (involving 45 million credit cardholders).

25 *See In re* Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01998, 2009 WL 5184352, at *9 (W.D. Ky. Dec. 22, 2009) (discussing a data security breach that affected more than 10 million persons).

26 *See Student Loan Company: Data on 3.3M People Stolen*, FOXNEWS.COM (Mar. 26, 2010), http://www.foxnews.com/us/2010/03/26/student-loan-company-data-m-people-stolen/ [hereinafter *Data on 3.3M People Stolen*] (indicating that the stolen data of more than 3 million borrowers, located on "portable media," included names, addresses, Social Security numbers, and dates of birth (internal quotation marks omitted)).

27 *See, e.g.*, Derby, *supra* note 21 (discussing the University of Wisconsin-Madison).

28 *See* Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *4 (S.D.N.Y. June 25, 2010) (discussing the loss of computer back-up tapes allegedly containing information relating to 12.5 million individuals).

29 *See* Editorial, *Who Really Sent That E-Mail*, N.Y. TIMES, Apr. 11, 2011, at A24 (discussing the theft of names and e-mail addresses of customers of some of the nation's largest businesses, and the risk that those customers would be vulnerable to "sophisticated identity-theft ploys" such as "spear phishing").

30 *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (involving the unencrypted data of 97,000 employees).

31 *See, e.g.*, *In re* Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01998, 2010 WL 3341200, at *9 (W.D. Ky. Aug. 23, 2010) (placing the cost of credit monitoring in a class action at "$37 per person," or $7 million); *see also* Andreas Antonopoulos, *Security Predictions for 2011*, NETWORK WORLD, Dec. 20, 2010, at 16 ("[J]ust buying credit monitoring and sending letters to the 500,000 people whose identities you lost can cost tens of millions of dollars and wipe out your business.").

32 *See* Stollenwerk v. Tri-W. Health Care Alliance, 254 F. App'x 664, 665 (9th Cir. 2007).

33 For example, in *Saenz v. Kaiser Permanente International*, the plaintiff alleged that "she and members of the class have suffered economic damages, including the costs of obtaining identity theft insurance, professional credit monitoring, cancelling and obtaining new credit and debit cards, as well as fees for freezing and unfreezing bank and credit accounts." No. C 09-5562, 2010 WL 668038, at *2 (N.D. Cal. Feb. 19, 2010).

sponsible for losses such as emotional distress[34] or increased risks of future harm.[35] And, until identity theft occurs, other types of damage resulting from data exposure may be modest in amount.[36] Thus, credit-monitoring losses may form the lion's share of potentially recoverable damages in a dispute with an allegedly negligent database possessor.

B. *Tort Claims Related to Cybersecurity*

Credit-monitoring damages may be sought in *non-cybersecurity* cases, such as disputes arising when a creditor makes an erroneous report to credit-reporting agencies[37] or when a credit-reporting agency sells a credit report to a third person without a "permissible purpose."[38] Compensation for the costs of credit monitoring is also sometimes sought under *non-tort* theories of liability.[39] Moreover, some judicial opinions use the phrase "credit

---

34 *See* Paul v. Providence Health Sys.-Or., 240 P.3d 1110, 1116-20 (Or. Ct. App. 2010) (denying recovery of emotional distress damages in a case arising from the theft of unencrypted records relating to hundreds of thousands of patients from a car). *But see* Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2296, 2010 WL 86391, at *5 (N.D. Ill. Jan. 5, 2010) (allowing a claim for severe emotional distress damages to proceed).

35 *See* Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006).

> [Plaintiffs] overlook the fact that their expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized. In other words, the plaintiffs' injuries are solely the result of perceived risk of future harm. Plaintiffs have shown no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm.

Id. But see Rowe, 2010 WL 86391, at *6 (holding, in a case based on inadvertent posting of personal information on the Internet, that the plaintiff could "collect damages based on the increased risk of future harm he incurred, but only if he can show that he suffered from some present injury beyond the mere exposure of his information to the public").

36 *Cf. In re* TJX Cos. Retail Sec. Breach Litig., 584 F. Supp. 2d 395, 400 (D. Mass. 2008) (explaining that a settlement allowed compensation for the cost of replacing driver's licenses, "out-of-pocket expenses," and "lost time").

37 *See, e.g.*, Wang v. Asset Acceptance, LLC, 680 F. Supp. 2d 1122, 1124 (N.D. Cal. 2010) (indicating that, in a controversy based on the defendant's reporting of debts to credit-reporting agencies without also disclosing that such debts were disputed or that the applicable statutes of limitations barred the courts from enforcing the debts, the plaintiff sought compensation for "forced purchase of credit reports and credit monitoring," as well as other expenses).

38 *E.g.*, Daniels v. Experian Info. Solutions, Inc., No. CV 109-017, 2010 WL 331690, at *2 (S.D. Ga. Jan. 19, 2010) (internal quotation marks omitted) (recounting that the plaintiff demanded "free credit monitoring for one year").

39 *See* Hendricks v. DSW Shoe Warehouse Inc., 444 F. Supp. 2d 775, 782 & n.6 (W.D. Mich. 2006) (denying recovery of creditor-monitoring damages based on breach of contract or violation of the Michigan Consumer Protection Act, and expressly noting that no claim for negligence had been asserted and that, therefore, an earlier case, which had allowed recovery of credit-monitoring damages, was "neither applicable nor persuasive").

monitoring" in ways that have nothing to do with tracking the credit of individuals[40] or that are unrelated to recovery of damages for such services.[41]

This Article is concerned with the compensability of credit-monitoring costs only in tort cases involving cybersecurity issues. This range of conduct includes failing to protect data from unauthorized access; negligently[42] or intentionally[43] disclosing or transferring personal information (such as via postings on the Internet, e-mail correspondence, or attachments to court filings[44]); and, neglecting to inform data subjects that the security of their personal data has been compromised.

C. *Starting Assumptions*

1. Duty to Protect and Disclose Breaches

This Article assumes *arguendo* that a data processor has a *duty* to protect the personal information of others from unauthorized access or revelation and to disclose information about a known breach of data security to the affected data subjects. These duties are rooted in common law principles;[45] in the terms of, or public policies reflected in, the security-breach notification laws and other provisions that numerous states have passed;[46]

---

[40] *See, e.g.*, Aerotel, Ltd. v. Telco Grp., Inc., No. 1:04-cv-10292-RJH-FM, 2010 WL 1916015, at *2 (S.D.N.Y. May 12, 2010) (discussing, in a patent infringement suit, "credit monitoring" and prepayment features related to telephone systems).

[41] *See* Scandaglia v. Transunion Interactive, Inc., No. 09 C 2121, 2010 WL 3526653, at *5-8 (N.D. Ill. Sept. 1, 2010) (containing an incidental reference to "credit monitoring" in a service mark infringement action); Fed. Trade Comm'n v. RCA Credit Servs., LLC, 727 F. Supp. 2d 1320, 1332 n.20 (M.D. Fla. 2010) (referring to "credit monitoring" in a Federal Trade Commission enforcement action).

[42] *See, e.g.*, Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391, at *1-2 (N.D. Ill. Jan. 5, 2010) (involving a variety of claims brought by insurance plan members whose personal information was temporarily accessible to the public on the Internet).

[43] *See generally* 1-800-E. W. Mortg. Co. v. Bournazian, No. 09CV2123, 2010 WL 3038962 (Mass. Super. Ct. July 18, 2010) (awarding credit-monitoring damages in an action alleging conversion, breach of contract, and breach of loyalty against a former employee who improperly took and then unlawfully deleted highly confidential personal information of sixty-eight employees).

[44] *See, e.g., In re* Maple, 434 B.R. 363, 369, 376-77 (Bankr. E.D. Va. 2010) (declining to dismiss, in a suit arising from a creditor's filing of a claim in bankruptcy litigation that improperly reveals personal information, certain state-law claims seeking compensation for emotional distress, credit monitoring, and other damages).

[45] *See* Johnson, *supra* note 1, at 272-82 (discussing common law principles evidencing a duty to protect data from unauthorized disclosure); *id.* at 288-96 (examining basic tort principles that create a duty to reveal knowledge that data security has been compromised). *But see In re* Davis, 430 B.R. 902, 909 (Bankr. D. Colo. 2010) (finding that the plaintiff failed to properly allege actions for invasion of privacy or negligent infliction of emotional distress).

[46] *See* Joseph J. Lazzarotti, *The Emergence of State Data Privacy and Security Laws Affecting Employers*, 25 HOFSTRA LAB. & EMP. L.J. 483, 489-507 (2008) (discussing state laws that protect data

and in various other pieces of state[47] and federal[48] legislation that impose particular data-security obligations. Courts have enforced these duties in recent cases,[49] although there is authority to the contrary.[50]

---

and require notification of breach); *see also* Johnson, *supra* note 1, at 263-66, 270-72 (discussing the duty to protect computerized personal information under state security breach notification laws); *id.* at 282-87 (examining notification duties imposed by state security breach notification laws). The National Conference of State Legislatures' list of state laws requiring notice of security breaches can be found at: *State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES (Oct. 12, 2010), http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx ("Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information."). The Conference's year-by-year list of security breach legislation is available at: *Breach of Information*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/Default.aspx?TabId=13481 (last visited Sept. 20, 2011).

47 *See* Lazzarotti, *supra* note 46, at 490-92 (discussing state laws that protect social security numbers). *But see* Shames-Yeakel v. Citizens Fin. Bank, 677 F. Supp. 2d 994, 996, 1000-09 (N.D. Ill. 2009) (discussing and rejecting, in part, several statutory theories of liability); Paul v. Providence Health Sys.-Or., 240 P.3d 1110, 1120-22 (Or. Ct. App. 2010) (finding that the plaintiffs failed to establish a claim under the Oregon Unlawful Trade Practices Act in a case arising from the theft of unencrypted patient records).

48 *See generally* GINA STEVENS, CONG. RESEARCH SERV., FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2010), *available at* http://assets.opencrs.com/rpts/RL34120_20100128.pdf (discussing the various federal laws that now have provisions or regulations relating to security and data breaches); Lazzarotti, *supra* note 46, at 487 (stating that "[t]he federal government has yet to pass a broad-based data privacy and security statute" and instead has addressed "specific types of information, in some cases on an industry-by-industry basis"). *But see* Elizabeth D. De Armond, *A Dearth of Remedies*, 113 PENN ST. L. REV. 1, 52 (2008) (arguing that federal enactments, such as the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, and the Gramm-Leach-Bliley Act, which purport to protect privacy, fail to achieve their promise). Some authors have argued the federal Gramm-Leach-Bliley Act, which imposes data protection obligations on financial institutions, is a proper basis for a civil cause of action. *See* Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 MARQ. L. REV. 847, 865-66 (2005) (discussing a negligence per se theory of liability). However, at least two courts have rejected that argument. *See Davis*, 430 B.R. at 908 (holding that Gramm-Leach-Bliley does not create a private right of action); *In re* Matthys, No. 09-16585-AJM-13, 2010 WL 2176086, at *2 (Bankr. S.D. Ind. May 26, 2010); *see also* Johnson, *supra* note 1, at 268-69 (arguing that Gramm-Leach-Bliley lacks the specificity required to support a negligence per se tort action by a data subject against a financial institution). Applicable provisions of the Federal Rules of Civil Procedure reflect the importance of protecting personal information from improper access. Rule 5.2 provides in relevant part:

> (a) Redacted Filings. Unless the court orders otherwise, in an electronic or paper filing with the court that contains an individual's social-security number, taxpayer-identification number, or birth date, the name of an individual known to be a minor, or a financial-account number, a party or nonparty making the filing may include only:
> (1) the last four digits of the social-security number and taxpayer-identification number;
> (2) the year of the individual's birth;
> (3) the minor's initials; and
> (4) the last four digits of the financial-account number.

FED. R. CIV. P. 5.2(a). Exceptions to the general rule on redacted filings are set forth in a different subsection. *See id.* 5.2(b).

In *Shames-Yeakel v. Citizens Financial Bank*,[51] a federal court in Illinois found that "[a] number of courts have recognized that fiduciary institutions have a common law duty to protect their members' or customers' confidential information against identity theft."[52] When an unknown person gained access to the bank customers' online accounts and stole thousands of dollars, the court held that the customers were victims of identity theft.[53] The court ruled that the customers had a valid negligence claim against the bank because it employed only a single-password form of account protection.[54]

Numerous commentators agree that businesses have a duty to prevent improper access or revelation of personal information and to disclose knowledge of security breaches.[55] Of course, absent proof of duty, a negligence

---

[49] *See* Allstate Ins. Co. v. Linea Latina De Accidentes, Inc., No. 09-3681 (JNE/JJK), 2010 WL 5014386, at *2-4 (D. Minn. Nov. 24, 2010) (ordering a party whose electronic case filing improperly disclosed personal information to notify affected individuals of the disclosure and provide twelve months of credit monitoring free of charge); *see also* Poli v. Mountain Valleys Health Ctrs., Inc., No. 2:05-2015-GEB-KJM, 2006 WL 83378, at *3 (E.D. Cal. Jan. 11, 2006) (finding that the plaintiff stated a claim for negligent disclosure of medical information); 1-800-E. W. Mortg. Co. v. Bournazian, No. 09CV2123, 2010 WL 3038962, at *1-3 (Mass. Super. Ct. July 18, 2010) (holding a former employee liable for credit monitoring and other damages in a case arising from the improper removal of confidential employee information); Bell v. Mich. Council 25 of Am. Fed'n of State, Cnty., & Mun. Emps., No. 246684, 2005 WL 356306, at *1, *3 (Mich. Ct. App. Feb. 15, 2005) (per curiam) (holding a union liable for identity theft damages resulting from the union's failure to safeguard members' personal information). Of course, liability may be imposed for failure to safeguard data in hard copy form. *See* Scott v. Minneapolis Pub. Schs., No. A05-649, 2006 WL 997721, at *1, *3 (Minn. Ct. App. Apr. 18, 2006) (affirming a judgment imposing liability under the Minnesota Government Data Practices Act for damages resulting from improper disposal of educational records). *But see In re* Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01998, 2010 WL 3341200, at *6 (W.D. Ky. Aug. 23, 2010) ("[T]he current state of the law in regards to data breaches does not bode well for Plaintiffs. . . . [T]his factor weighs heavily in favor of settlement.").

[50] *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (rejecting claims for negligence and breach of contract arising from the theft of a laptop containing unencrypted employee information); Hammond v. Bank of N.Y. Mellon Corp., No. 08 CIV 6060(RMB)(RLE), 2010 WL 2643307, at *4, *8-9 (S.D.N.Y. June 25, 2010) (finding that no duty was owed to millions of persons whose personal information was contained on computer back-up tapes that were lost).

[51] 677 F. Supp. 2d 944 (N.D. Ill. 2009).

[52] *Id.* at 1007-08.

[53] *Id.* at 996-97.

[54] *Id.* at 1008-09; *see also* Sue Reisinger, *How Fast Is Fast Enough to Tell Customers About Data Breaches?*, CORPORATE COUNSEL (July 25, 2011), http://www.law.com/jsp/cc/PubArticleCC.jsp?id=1202504732096 (discussing a federal court decision holding Comerica Bank liable for data breach losses).

[55] *See, e.g.*, Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?*, 3 SHIDLER J.L. COM. & TECH. 7, ¶ 4 (2006) ("Like legislatures, courts are signaling some willingness to impose a common law duty of care to protect personal information."); Bill Piatt & Paula DeWitte, *Loose Lips Sink Attorney-Client Ships: Unintended Technological Disclosure of Confidential Communications*, 39 ST. MARY'S L.J. 781, 815 (2008) ("Attorneys have an ethical obligation . . . . to protect data stored electronically from unintended disclosure either through

claim will fail. In that case, unless there is some other theory of liability, the courts need not reach the question of what damages plaintiffs may recover in cybersecurity actions.

2. Not Barred by the Economic Loss Rule

This Article assumes *arguendo* that the so-called "economic loss rule" does not bar recovery of credit-monitoring losses. That rule—if it is a rule[56]—is a principle of uncertain dimensions, which holds that, at least in some circumstances, negligence that causes purely economic losses, without also producing personal injury or property damage, is not actionable in tort law.[57] The elegant simplicity of the "rule" masks a messier reality because the "rule" is subject to a multitude of well-recognized exceptions. As noted in a previous article:

> Not the least of these qualifications are the causes of action imposing liability for negligent misrepresentation, defamation, professional malpractice, breach of fiduciary duty, nuisance, loss of consortium, wrongful death, spoliation of evidence, and unreasonable failure to settle a claim within insurance policy limits, all of which may afford recovery for negligence causing purely economic losses to the plaintiff.[58]

In large measure, the economic loss rule is intended to further the private ordering of business transactions.[59] However, data-security statutes in

---

inadvertent release of the information or from failure to secure the data against unauthorized access. . . . [and] must act reasonably to prevent, detect, and remedy security breaches."); *see also* Lori J. Parker, *Cause of Action for Identity Theft*, *in* 31 CAUSES OF ACTION 2d, at 1, 23-25 (2006) (discussing theories of liability); Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. 223, 244-62 (2008) (discussing developments in Canada); Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 923-25 (2007) (discussing tort liability).

[56] Professor Oscar S. Gray, an eminent torts scholar, has expressed doubts about whether there is a single, unified economic loss rule. He wrote that:

> I had not previously thought that there was any such thing as a single "economic loss rule." Instead, I had thought that there was a constellation of somewhat similar doctrines that tend to limit liability, in the case of purely economic loss, from what might have been expected under *Palsgraf* in the case of physical loss. These doctrines seemed to work in somewhat different ways in different contexts, for similar but not necessarily identical reasons, with exceptions where the reasons for limiting liability were absent.

Oscar S. Gray, *Some Thoughts on "The Economic Loss Rule" and Apportionment*, 48 ARIZ. L. REV. 897, 898 (2006) (footnote omitted).

[57] *See* Vincent R. Johnson, *The Boundary-Line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523, 524-34 (2009) (discussing the rule and its exceptions).

[58] *Id.* at 530-32 (footnotes omitted) (containing abundant citations to primary authority).

[59] *See* Flagstaff Affordable Hous. Ltd. P'ship v. Design Alliance, Inc., 223 P.3d 664, 671 (Ariz. 2010) (en banc) ("The principal function of the economic loss doctrine, in our view, is to encourage private ordering of economic relationships and to uphold the expectations of the parties by limiting a plaintiff to contractual remedies for loss of the benefit of the bargain."); *see also* Jay M. Feinman, *The*

many states hold that private agreements disclaiming legislatively imposed obligations related to computerized personal information are not enforceable and are void as against public policy.[60] Consequently, the duties at issue in cybersecurity cases are, in large measure, not a proper subject for private ordering. For this reason, and for other reasons that have been explored elsewhere,[61] the economic loss rule should not foreclose recovery of credit-monitoring damages.[62] However, in *Paul v. Providence Health System-Oregon*[63] an Oregon appellate court has ruled to the contrary. In that case, a thief stole unencrypted patients' records from the defendant's employee's car.[64] The court held that the patients could not recover pure economic damages to cover the expenses they incurred by purchasing credit-monitoring services to lower the risk of identity theft.[65]

II. COURT DECISIONS AND BUSINESS PRACTICES

Not all courts have viewed credit-monitoring damages favorably. This Part discusses court precedent, which failed to recognize the reasonableness and value of credit monitoring. It also discusses voluntary offers of credit monitoring by businesses and governmental entities, and judicial or administrative recognition of credit monitoring as part of class-action settlements or sanctions.

Economic Loss Rule and Private Ordering, 48 ARIZ. L. REV. 813, 814 (2006) (discussing the logic of private ordering).

60 *See* Johnson, *supra* note 1, at 300-01. The article explains:

> Many state laws, such as the Rhode Island Identity Theft Protection Act of 2005, provide that a waiver of the data subjects' rights is against public policy, and therefore void and unenforceable. If that is true, it makes little sense that consumers should bargain and pay for the level of cybersecurity protection—and the right to sue for out-of-pocket damages—that they desire. Moreover, it is simply unrealistic to expect that bargaining to occur between individual consumers and the large corporations that play a pervasive role in modern life.

Id. at 300 (footnotes omitted).

61 *See id.* at 296-303 (discussing the policy concerns that animate the economic loss rule: scope of liability, certainty of damages, and delineation of contract-versus-tort).

62 *See* Johnson, *supra* note 57, at 532 (discussing various causes of actions where damages are not barred by the economic loss rule). *But see* Krottner v. Starbucks Corp., 406 F. App'x 129, 131-32 (9th Cir. 2010) (finding it unnecessary to determine whether the economic loss rule barred an award of credit-monitoring damages because the plaintiffs failed to allege their negligence and breach of contract claims sufficiently).

63 240 P.3d 1110 (Or. Ct. App. 2010).

64 *Id.* at 1112.

65 *Id.* at 1116.

A. *Adverse Decisions*

Although some courts have ordered defendants to provide credit-monitoring services[66] or pay credit-monitoring damages,[67] a number of cases have held that credit-monitoring damages are not recoverable in cybersecurity tort actions.[68] With scant attention to the reasonableness or usefulness of credit monitoring as a response to database intrusion and as a means of mitigating damages, these courts concluded that, at least on certain facts, such expenditures are not compensable.[69]

The decisions that are adverse to recovery of compensation for credit-monitoring expenses generally fall into three categories, which are discussed later in this Article.[70] First, some cases have rejected the plaintiffs' efforts to analogize credit monitoring to medical monitoring.[71] This is significant because many states allow plaintiffs to recover compensation for the medical examinations that are necessary to detect the emergence of a diseased condition caused by toxic exposure.[72] Data exposure and toxic

---

66 *See* Allstate Ins. Co. v. Linea Latina De Accidentes, Inc., No. 09-3681 (JNE/JJK), 2010 WL 5014386, at *2-4 (D. Minn. Nov. 24, 2010) (involving an electronic case filing that improperly disclosed personal information).

67 *See* 1-800-E. W. Mortg. Co. v. Bournazian, No. 09CV2123, 2010 WL 3038962, at *1-3 (Mass. Super. Ct. July 18, 2010) (involving improper removal of confidential employee information).

68 *See, e.g.*, Shafran v. Harley-Davidson, Inc., No. 07 Civ. 01365(GBD), 2008 WL 763177, at *3 (S.D.N.Y. March 20, 2008) (holding that "the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy"). *Pisciotta v. Old National Bancorp* held that credit-monitoring costs were not compensable under Indiana law. 499 F.3d 629, 635-39 (7th Cir. 2007). However, *Pisciotta* was a narrow decision. *Id.* at 636. As described by another court in a later case, "[a]fter an in-depth analysis of Indiana law, the appellate court [in *Pisciotta*] upheld the decision [denying credit-monitoring damages] because there was no precedent supportive of the opposite conclusion and federal courts sitting in diversity should avoid inventing truly novel tort claims on behalf of a state." Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2296, 2010 WL 86391, at *7 (N.D. Ill. Jan. 5, 2010).

69 Some cases contain no analytical discussion, but merely a brief citation to an earlier decision denying recovery of credit-monitoring damages. *See In re* Barnhart, No. 09-bk-01974, 2010 WL 724703, at *4 (Bankr. N.D. W. Va. Feb. 26, 2010) (dicta).

70 *See infra* Part III, IV.

71 *See* Ruiz v. Gap, Inc., 622 F. Supp. 2d 908, 913-14 (N.D. Cal. 2009) (finding that the lack of any public health interest differentiates lost data and medical-monitoring cases), *aff'd*, 380 F. App'x 689 (9th Cir. 2010); *see also* Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 280-81 (S.D.N.Y. 2008) (finding that New York's interest in the public health was greater than the availability of a money remedy for an individual whose stolen information is later misused); Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007) (finding that "identity exposure" cases and medical-monitoring cases are not analogous (internal quotation marks omitted)); Key v. DSW Inc., 454 F. Supp. 2d 684, 689 (S.D. Ohio 2006) (finding that a victim of identity theft has not suffered recoverable harm as has a victim in the medical-monitoring context).

72 *See, e.g.*, *In re* Paoli R.R Yard PCB Litig., 916 F.2d 829, 849-52 (3d Cir. 1990) (differentiating compensation for medical monitoring from compensation for the increased risk of future harm and

exposure are analogous in that they both create a need for early detection of potentially emerging, threatened harm. Second, some decisions have denied recovery of credit-monitoring damages on the ground that the plaintiff has not suffered a present injury but has merely been exposed to a risk of harm in the future.[73] Finally, in the third group of cases, the courts declined to award credit-monitoring damages because the plaintiffs lacked standing to litigate that issue in federal court.[74]

B. *Voluntary Offers of Credit Monitoring*

Rather than definitively resolving issues relating to credit-monitoring costs, recent developments have called decisions denying recovery into question. The first of these occurrences relates to business practices. Recognizing the appropriateness of expenditures on credit monitoring,[75] database possessors potentially responsible for unauthorized access to data often voluntarily offer to pay credit-monitoring costs for affected persons for a period of time.[76] Thus, when Wyndham Hotels and Resorts learned that a

---

allowing the recovery of medical-monitoring damages under Pennsylvania law covering "only the quantifiable costs of periodic medical examinations necessary to detect the onset of physical harm").

[73] *See infra* Part IV.A; *see also In re* Killian, No. 05-14629-HB, 2009 WL 2927950, at *8-9 (Bankr. D.S.C. July 23, 2009). *Killian* was not the typical cybersecurity case. The court did not charge the defendant with failing to protect data from unauthorized access. Rather, the complaint alleged that the defendant "intentionally communicated or otherwise made the Killians' sensitive and personal nonpublic information available to the public by placing that information on the Court's public records." *Id.* at *2. The court found that there was "ample legal authority to support a claim that Defendant had a duty to refrain from placing the Killians' personal information on the public record." *Id.* at *8. However, the court rejected the plaintiff's negligence claim on the ground that the complaint failed to allege compensable damages. The court reasoned:

> The Court must be able to find that the allegations of the Complaint allege an *injury* that is *to accrue in the future*. In this case, the Killians' complaint simply alleges that the cost of credit monitoring, which is a *preventative remedy*, will accrue in the future.

Id. at *9 (citation omitted).

[74] *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., No. 08 CIV 6060(RMB)(RLE), 2010 WL 2643307, at *7 (S.D.N.Y. June 25, 2010) (holding that the plaintiffs lacked standing because "their claims are future-oriented, hypothetical, and conjectural"); *see also infra* Part IV.A.3.

[75] Even though expenditures on credit-monitoring damages are a reasonable means of mitigating the damages that can flow from authorized access to personal information, there is evidence that many consumers are unaware or unconvinced of those benefits. In *In re TJX Cos. Retail Securities Breach Litigation*, 584 F. Supp. 2d 395 (D. Mass. 2008), the court noted that only about three percent of eligible persons claimed that the credit-monitoring benefit was part of a database intrusion settlement. *Id.* at 406.

[76] *See, e.g.*, Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2286, 2010 WL 86391, at *1 (N.D. Ill. Jan. 5, 2010) (stating that the defendants responsible for making personal information temporarily available on the Internet "offered to provide one year of credit monitoring to those affected"). In *Taylor v. Countrywide Home Loans*, No. 08-CV-13258, 2010 WL 750215 (E.D. Mich. Mar. 3, 2010), the defendant, whose "former employee may have sold unauthorized information about plaintiffs to a third party," offered the plaintiffs "a two-year membership in Triple Advantage (a credit monitoring service) to help plaintiffs protect their credit." *Id.* at *12. Ultimately, the court rejected the plaintiffs' vicarious

sophisticated hacker penetrated its computer system and may have used customer information to perpetrate fraudulent transactions, it provided affected customers with credit monitoring for one year at no cost.[77] Similarly, Countrywide Financial volunteered to provide two years of credit monitoring to millions of persons as a result of a security breach related to their mortgage loans.[78]

In another controversy, a company that guaranteed federal student loans notified 3.3 million persons that their data had been stolen and promptly "arranged with credit protection agency Experian to provide affected borrowers with free credit monitoring and protection services."[79] In addition, the University of Louisville,[80] Harley-Davidson,[81] the St. Louis Metropolitan Police Department,[82] Tulane University,[83] the Bank of New

---

liability claim related to the conduct of the former employee because "plaintiffs have admitted that they have suffered no monetary damages nor any impact on their credit report resulting from the possible (and unconfirmed) theft of any of their personal information by the former Countrywide employee. Without any damages, this claim . . . must fail." *Id.* at *13; *see also* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140-41 (9th Cir. 2010) (indicating that the court ordered a thief to provide 97,000 employees with one year of credit monitoring); *TJX*, 584 F. Supp. 2d at 400 (discussing a settlement that provided affected customers with three years of credit monitoring).

77 Letter from Wyndham Hotels & Resorts to Vincent Johnson (June 2010) (on file with author); *see also* Saenz v. Kaiser Permanente Int'l, No. C 09-5562 PJH, 2010 WL 668038, at *2 (N.D. Cal. Feb. 19, 2010) (indicating that the defendants "offered plaintiff and putative members of the class one year of professional credit monitoring through Equifax as a remedy for the security breach" but that the plaintiff maintained that the offer was inadequate).

78 *See In re* Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01988, 2009 WL 5184352, at *8-9 (W.D. Ky. Dec. 22, 2009) (discussing the offer, which some class members accepted and the subsequent settlement, which the court preliminarily approved). The court stated that "[a]pproximately 20% of the 2.4 million [persons initially contacted] accepted Countrywide's first offer of free credit monitoring." *Id.* at *11.

79 *Data on 3.3M People Stolen*, *supra* note 26. According to a news report published within one week of the theft, "[b]orrowers will be receiving letters . . . on how to sign up, gain access to fraud resolution representatives, and be provided with identity theft insurance coverage." *Id.*

80 Kirtley, *supra* note 23, at 29 (discussing a university's disclosure in June 2010 that patient information was posted on the Internet for twenty months and indicating that the university "immediately apologized for the breach, notified the patients or their next of kin, and agreed to pay a credit monitoring agency to watch the affected patients' credit for a year").

81 *See* Shafran v. Harley-Davidson, Inc., No. 07 Civ. 01365(GBD), 2008 WL 763177, at *1 (S.D.N.Y. Mar. 20, 2008) (indicating that one year of free credit monitoring was provided to thousands of persons whose personal information was on a lost laptop).

82 Kirtley, *supra* note 23, at 30-31 (indicating that after the department was "the victim of a cyberattack" in 2010, which an employee facilitated by opening an e-mail, "[t]he department said it would work to contact the affected parties and would pay to monitor their credit for a year").

83 John Pope, *Tulane Payroll Information Stolen*, TIMES-PICAYUNE, Jan. 8, 2011, at B6 (indicating that when a "laptop containing payroll and Social Security information for every full-time and part-time university employee" was stolen, "[e]ach of Tulane's 10,684 employees . . . received a letter . . . offering a year's free credit monitoring of their accounts").

York Mellon,[84] Ceridien Corporation,[85] Ohio State University,[86] Holy Cross Hospital (Ft. Lauderdale),[87] the University of Utah,[88] Wachovia Securities,[89] and other potential defendants have made comparable offers voluntarily.

When hackers stole the personal information of millions of PlayStation gamers, Senator Richard Blumenthal of Connecticut called on Sony to provide affected customers with "financial data security services, including free access to credit reporting services."[90] Sony responded by offering a year of free credit monitoring to victims of the breach.[91]

In Texas, the state left unencrypted information relating to 3.5 million persons on an Internet server for more than a year.[92] Despite a pending government financial crisis,[93] the Texas Comptroller announced that affected individuals would receive one year of free credit monitoring.[94]

---

84 *See* Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *4 (S.D.N.Y. June 25, 2010) (noting that a bank that lost computer back-up tapes voluntarily offered affected individuals, at "no cost . . . a minimum of 24 months of credit monitoring, $25,000 of identity theft insurance . . . [and] reimbursement for certain credit freeze costs").

85 Reilly v. Ceridien Corp., No. 10-5142 (JLL), 2011 WL 735512 (D.N.J. Feb. 22, 2011) (indicating that one year of free credit monitoring was provided to victims of a security breach caused by hacking).

86 Encarnacion Pyle, *Server Hacked at OSU; 760,000 Affected*, COLUMBUS DISPATCH (Ohio), Dec. 16, 2010, at A1 (stating that although there was "no indication that any personal information was taken or that the incident will result in identity theft for any of the affected people," the university offered twelve months of free credit-monitoring services as a precaution).

87 Jon Burstein, *Former Holy Cross Hospital Employee Pleads Guilty to ID Theft, Faces up to 10 Years in Prison*, SUN SENTINEL (Fla.), Jan. 27, 2011, at 3B (indicating that one year of credit monitoring was offered to 44,000 emergency room patients after a hospital employee improperly accessed 1,500 patient files).

88 Colo. Cas. Ins. Co. v. Perpetual Storage, Inc., No. 2:10CV316 DAK, 2011 WL 1231832, at *1 (D. Utah Mar. 30, 2011) (indicating that the university provided credit monitoring to affected patients when a company failed to "to safeguard computer back-up tapes containing highly confidential and sensitive medical records and other data").

89 Giordano v. Wachovia Sec., LLC, No. 06-476 (JBS), 2006 WL 2177036, at *1 (D.N.J. July 31, 2006) (offering one year of free credit monitoring after a list with thousands of social security numbers and other identifying information was lost in the mail).

90 Nick Bilton & Brian Stelter, *Sony Says PlayStation Hacker Got Personal Data*, N.Y. TIMES, Apr. 27, 2011, at B1.

91 *Free Credit Monitoring for Sony PlayStation Breach Victims*, WASH. ST. OFF. ATT'Y GEN. (May 27, 2011, 11:21 AM), http://www.atg.wa.gov/BlogPost.aspx?id=28174 (linking to http://us.playstation.com/news/consumeralerts/identity-theft-protection/).

92 Patricia Kilday Hart, *Comptroller Takes Blame for Personal Data Leak*, SAN ANTONIO EXPRESS-NEWS, Apr. 29, 2011, at 1A (indicating that the State replaced an offer of discounted credit monitoring with free credit monitoring).

93 Dave Mann, *Youth Movement*, TEX. OBSERVER, Apr. 8, 2011, at 4 ("Each day seemingly brings unrelenting bad news from every corner of state policy, with lawmakers facing a fiscal crisis and considering drastic budget cuts to education, health care, criminal justice, nearly everything.").

94 Dave Montgomery, *Comptroller "Really Sorry" for Records Breach*, FORT WORTH STAR-TELEGRAM, Apr. 29, 2011, at 1B.

One recent publication from the insurance field remarked in an article about managing cyber risk that "[i]f identity theft or fraud is possible due to a breach, many organizations offer free credit monitoring for as long as three years."[95] Similarly, a report issued by the federal government stated that "a representative of a large financial management company noted that offering free credit monitoring services after a breach has become standard industry practice."[96]

C. *Class Action Settlements*

Many courts have also recently approved class-action settlements in cybersecurity cases where the parties intended for portions of the settlements to cover the costs of credit monitoring.[97] Indeed, when parties settle aggregate claims, the settlement often encompasses only compensation for credit monitoring, identify theft insurance, and out-of-pocket costs, such as expenses incurred to replace checks or drivers' licenses.[98]

For example, in *In re TJX Cos. Retail Securities Breach Litigation*,[99] a federal court in Massachusetts approved an award of $6.5 million in attorneys' fees in a class-action suit arising from the theft of 40 million credit cardholders' personal information.[100] In that suit, which was then the "largest retail security breach in history,"[101] the settlement included compensation for credit monitoring and identity theft insurance. Explaining the court's ruling, the judge wrote:

> The Court . . . is satisfied that the Agreement creates a concrete benefit insofar as it provides that [customers returning merchandise without a receipt] could receive credit monitoring services. . . . The parties . . . determined with certainty the value, in the form of the cost of the credit monitoring subscription, that would be transferred to each unreceipted return customer who made a claim. Therefore, unlike the figures attached to other benefits—for which it was unclear how many class members, if any, might qualify and what amount they might claim—the $177,000,000 attributed to this benefit has meaning. Accordingly, the Court is comforta-

---

95 *Learn Strategies for Managing Cyber Risk*, BUS. INS., Jan. 3, 2011, at 3, 16.

96 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN 35 (2007) [hereinafter GAO REPORT].

97 *See In re* Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01998, 2009 WL 5184352, at *8, *12 (W.D. Ky. Dec. 22, 2009) (approving a settlement encompassing credit monitoring, identity theft insurance, and out-of-pocket expenses). *But see In re* Trans Union Corp. Privacy Litig., No. 00 C 4729, 2009 WL 4799954, at *14 (N.D. Ill. Dec. 9, 2009) ("[T]he class here (indeed, probably most classes) would rather have cash than in-kind relief. A check for $60 is more valuable to most people than getting free credit monitoring services with a retail value of that amount.").

98 *See Countrywide*, 2009 WL 5184352, at *8, *12 (approving a settlement encompassing credit monitoring, identity theft insurance, and out-of-pocket expenses).

99 584 F. Supp. 2d 395 (D. Mass. 2008).

100 *Id.* at 397, 408.

101 *Id.* at 397.

> ble characterizing this litigation as creating $177,000,000 in potential benefits for the class . . . .[102]

Similarly, in *In re Countrywide Financial Corp. Customer Data Security Breach Litigation*,[103] a federal court in Kentucky approved a class-action settlement, which included, notably, "[f]ree credit monitoring," finding that "the value of this settlement is substantial."[104] Likewise, in *Barel v. Bank of America*,[105] a federal court in Pennsylvania approved a class-action settlement that provided non-customers, whose credit reports had been improperly accessed by the defendant, with four months of credit monitoring and other relief.[106] Judicial endorsement of these settlements strongly suggests that credit monitoring is a legitimate form of damages resulting from exposure of personal information to unauthorized access.

In addition, in cases of data-security breaches, federal law authorizes the Secretary of the Department of Veterans Affairs to provide individuals "subject to a reasonable risk for the potential misuse of any sensitive personal information" with "[o]ne year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports."[107] In a case involving a lost laptop containing the information of 26.5 million veterans, the *National Law Journal* reported that money from the U.S. Treasury would provide compensation for "actual harm, such as physical symptoms of emotional distress or expenses incurred for credit monitoring."[108]

In another government data-security breach, an FDIC intern improperly used agency information to take out fraudulent loans in the names of FDIC employees.[109] The agency reacted by "promptly notifying affected employees and offering them 2 years of credit monitoring services."[110]

D. *Judicial and Administrative Sanctions*

There is other evidence that credit monitoring is an appropriate expenditure. For example, courts and administrative agencies have imposed sanctions requiring defendants to provide such services to persons at risk of identity theft due to breaches of data security. In *United States v. Ja-*

---

102 *Id.* at 409 (footnote omitted).

103 No. 3:08-MD-01998, 2010 WL 3341200 (W.D. Ky. Aug. 23, 2010).

104 *Id.* at *10.

105 255 F.R.D. 393 (E.D. Pa. 2009) (dealing with the settlement of claims related to improperly obtained credit reports).

106 *Id.* at 397.

107 38 C.F.R. § 75.118 (2009).

108 *Vets Will Share $20M in Data Privacy Breach*, NAT'L L.J., Feb. 2, 2009, at 16.

109 GAO REPORT, *supra* note 96, at 22-23.

110 *Id.* at 23 n.39.

nosko,[111] the First Circuit ordered a detainee to pay restitution after the court convicted him of hacking into a prison's computer system.[112] The award reimbursed the county for money that it spent on credit-monitoring services that it offered to employees whose personal information was contained in the hacked databases.[113] Retired Supreme Court Justice David Souter, sitting by designation, found that the county's actions were a reasonable response to the hacking and were, therefore, compensable.[114] Justice Souter wrote:

> It should go without saying that an employer whose personnel records have been exposed to potential identity thieves responds reasonably when it makes enquiry to see whether its employees have been defrauded. This act of responsibility is foreseeable to the same degree that indifference to employees' potential victimization would be reproachable. It is true, of course, that once they were told of the security breach, the individual employees and former workers involved in this case could themselves have made credit enquiries to uncover any fraud, but this in no way diminishes the reasonableness of the Facility's investigation prompted by the risk that its security failure created. And quite aside from decency to its workers, any employer would reasonably wish to know the full extent of criminality when reporting the facts to law enforcement authorities.[115]

In another case, *Allstate Insurance Co. v. Linea Latina De Accidentes, Inc.*,[116] attachments to a litigant's electronic court filing improperly disclosed "birth dates, names of minors, financial account numbers, and at least one social security number."[117] After the litigant failed to remedy the problem, a federal court in Minnesota ordered the party's counsel to "provide a subscription for 12 months to Experian's Triple Advantage Credit Monitoring to each individual whose social security number or date of birth was improperly disclosed, except those individuals who respond in writing . . . that they do not wish to receive the service."[118]

Similarly, in *Weakley v. Redline Recovery Services, LLC*,[119] a federal court in California found that an attorney had filed documents containing social security numbers recklessly and in bad faith, and that he made the documents available on the Internet for more than three weeks.[120] The court

---

111 642 F.3d 40 (1st Cir. 2011).

112 *Id.* at 41-42; *see also* Sheri Qualters, *Inmate Who Computer-Hacked Guards Must Pay Restitution*, NAT'L. L.J. (Apr. 12, 2011), http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202489772767 (discussing the First Circuit's decision); Sheri Qualters, *Should Prison Hacker Pay for Credit Monitoring as Restitution? 1st Circuit to Decide*, NAT'L. L.J. (Jan. 6, 2011), http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202477328396 (discussing the appeal in *United States v. Janosko*).

113 *Janosko*, 642 F.3d at 41.

114 *Id.* at 42.

115 *Id.*

116 No. 09-3681 (JNE/JJK), 2010 WL 5014386 (D. Minn. Nov. 24, 2010).

117 *Id.* at *1.

118 *Id.* at *4.

119 No. 09cv1423 BEN (WMC), 2011 WL 1522413 (S.D. Cal. Apr. 20, 2011).

120 *Id.* at *1-2.

ordered the responsible attorney to pay for five years of credit monitoring to protect the plaintiff from identity theft.[121]

In Connecticut, the state insurance commission fined a health insurer for a major data-security breach and untimely notification of affected persons.[122] The fine was part of an agreement requiring the insurer to provide two years of free credit monitoring to insureds.[123]

E. *Indicia of Legitimacy*

As the preceding discussion demonstrates, business practice, litigation settlement, and judicial and administrative sanction developments, along with court opinions referencing the utility of credit monitoring,[124] strongly suggest that expenditures on credit monitoring are prudent and appropriate when defendants place computerized personal information at risk. To that extent, plaintiffs should be able to recover such amounts in tort litigation because those expenditures are reasonably necessary to mitigate the harm that may flow from a cybersecurity breach. To conclude otherwise would be to suggest that corporate, judicial, and administrative officials now routinely sanction the waste of resources when they approve voluntary offers, settlements, fines, or sanctions involving credit-monitoring expenditures.

Moreover, it is easier to justify a legal duty to provide credit-monitoring services when such provision is a customary business practice in cases of breached data security.[125] In such an environment, imposition of liability for credit-monitoring damages will neither disrupt community practices nor impose unprecedented obligations. This is important because

---

121 *Id.* at *2 (assessing the cost of credit monitoring at $900).

122 Ryan Doran, *Privacy Breaches Spell Tighter Controls of Patient Records*, FAIRFIELD COUNTY BUS. J., Dec. 6, 2010, at 4.

123 *Id.*

124 *See, e.g.*, Dixon-Rollins v. Experian Info. Solutions, Inc., No. 09-0646, 2010 WL 3749454, at *1 (E.D. Pa. Sept. 23, 2010) (indicating that use of a credit-monitoring service revealed the improper listing of a debt on a credit report); Belmont Holdings Corp. v. Sun Trust Banks, Inc., No. 1:09-cv-1185-WSD, 2010 WL 3545389, at *2 (N.D. Ga. Sept. 10, 2010) (stating, in the context of a securities law class action, that the plaintiff used "credit monitoring . . . to provide 'early warning' alerts for problem loans in the portfolio"); Saccato v. Gordon, No. 10-6111-HO, 2010 WL 3395295, at *2 (D. Or. Aug. 26, 2010) (noting that the plaintiff's use of credit monitoring disclosed an allegedly erroneous debt entry).

125 For instance, in determining whether a defendant breached a duty, courts frequently refer to the relevant industry practices. *See* Glow v. Union Pac. R.R. Co., 652 F. Supp. 2d 1135, 1141 (E.D. Cal. 2009) ("It is the jury's duty to consider industry practice and available alternatives as part of its calculus to determine whether defendant's conduct was negligent."). However, in *Rowe v. UniCare Life & Health Insurance Co.*, the court stated that the fact that the defendants attempted to mitigate the costs of credit monitoring by offering free credit monitoring for a year did "not resolve the question of whether credit monitoring costs are actual damages." No. 09 C 2286, 2010 WL 86391, at *7 (N.D. Ill. Jan. 5, 2010).

among the policy considerations relevant to whether a duty should be imposed are the resulting "consequences to the community."[126]

III. ANALOGY TO MEDICAL-MONITORING DAMAGES

According to Professor Dan B. Dobbs, in the personal injury context, "[n]o rule of law excludes recovery for expenses of diagnosis or limits the recovery to expenses of treatment."[127] Moreover, the rule that a party must prove damages with reasonable certainty "does not, even taken literally, exclude recovery for expenses of minimizing damages or of determining the nature and extent of the plaintiff's injury."[128] Consistent with these principles, many states permit toxic-exposure plaintiffs to recover the costs of medical monitoring.[129] As one court noted, "[a] medical monitoring award aids presently healthy plaintiffs who have been exposed to an increased risk of future harm to detect and treat any resultant harm at an early stage."[130]

In *Meyer ex rel. Coplin v. Fluor Corp.*,[131] the Supreme Court of Missouri, *en banc*, made a similar ruling. The *Meyer* court, discussing an earlier decision of the Missouri Court of Appeals, *Elam v. Alcolac, Inc.*,[132] stated:

---

126 Rowland v. Christian, 443 P.2d 561, 564 (Cal. 1968).

127 DAN B. DOBBS, LAW OF REMEDIES § 8.1(3), at 651 (2d ed. 1993).

128 *Id.*

129 *See, e.g.*, *In re* Paoli R.R Yard PCB Litig., 916 F.2d 829, 850 (3d Cir. 1990) (differentiating compensation for medical monitoring from compensation for the increased risk of future harm and allowing the recovery of medical-monitoring damages under Pennsylvania law covering "only the quantifiable costs of periodic medical examinations necessary to detect the onset of physical harm"); Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824 (Cal. 1993) (en banc) (holding "that the cost of medical monitoring is a compensable item of damages where the proofs demonstrate, through reliable medical expert testimony, that the need for future monitoring is a reasonably certain consequence of a plaintiff's toxic exposure and that the recommended monitoring is reasonable"). According to the Supreme Court of Nevada:

> Since the landmark decision *Askey v. Occidental Chemical Corp.*, 102 A.D.2d 130, 477 N.Y.S.2d 242, 247 (1984), in which a New York appeals court acknowledged medical monitoring could be a recoverable damage, appellate courts in at least ten other states have recognized claims for medical monitoring. In addition, federal courts have interpreted state law in at least seven additional states and the District of Columbia as permitting claims for medical monitoring.

Badillo v. Am. Brands, Inc., 16 P.3d 435, 438 (Nev. 2001) (en banc) (per curiam) (footnote omitted). *But see* Paz v. Brush Engineered Materials, Inc., 949 So. 2d 1, 9 (Miss. 2007) (holding that the state does not recognize medical-monitoring claims in the absence of proof of physical injury); Lowe v. Philip Morris USA, Inc., 183 P.3d 181, 182 (Or. 2008) (en banc) (holding that a smoker was not entitled to medical-monitoring damages based on accumulated exposure to cigarette smoke).

130 Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568, 571 (6th Cir. 2005) (finding that the plaintiffs had standing to seek medical-monitoring damages related to potentially defective implants).

131 220 S.W.3d 712 (Mo. 2007) (en banc).

132 765 S.W.2d 42 (Mo. Ct. App. 1988).

> The *Elam* court recognized that among the potential damages sustained by a plaintiff who is exposed to a toxin is the need for medical monitoring for the "early detection of serious disease from the chronic exposure" to toxins. The court further reasoned that medical monitoring costs are recoverable because "compensation for necessary medical expenses reasonably certain to be incurred in the future rests on well-accepted legal principles." These "well-accepted" principles of Missouri law provide that a plaintiff is entitled to recover for the prospective consequences of the defendant's tortious conduct if the injury is reasonably certain to occur. Recognizing that a defendant's conduct has created the need for future medical monitoring does not create a new tort. It is simply a compensable item of damage when liability is established under traditional tort theories of recovery.[133]

Jurisdictions vary in how they state the elements of a medical-monitoring claim. In general:

> Recovery of medical monitoring costs requires proof that (1) the plaintiff was exposed to a toxic substance, (2) the exposure resulted from the defendant's negligence, (3) the exposure increased the plaintiff's risk of serious disease or illness, (4) there exist beneficial medical procedures to treat that disease or illness, and (5) those procedures are reasonably necessary.[134]

For similar reasons, it can be argued that credit monitoring is appropriate when there has been a serious breach of data security. Expenditures on credit monitoring are necessary to enable the data subject to detect serious kinds of identity theft promptly and take steps to minimize the resulting harm. Indeed, it can be argued that credit monitoring is even more appropriate than medical monitoring. Credit-monitoring procedures are not physically invasive, do not involve follow-up visits or tests, and rarely produce "false positives"—results that are erroneously misleading.[135] This Part explores the analogy between credit-monitoring damages and medical-monitoring damages in further detail.

A. *Exposure Threshold for Recovery*

Plaintiffs cannot recover medical-monitoring damages in cases of insignificant exposure to toxic chemicals.[136] Similarly, courts should not award credit-monitoring damages if only a trivial breach of data security occurred. The relevant Latin maxim is *de minimis non curat lex*, a phrase

---

133 *Meyer*, 220 S.W.3d at 717 (citations omitted) (quoting *Elam*, 765 S.W.2d at 209).

134 Graves, *supra* note 5, ¶ 12, at 9-10 (footnotes omitted).

135 *Id.* ¶ 21, at 16 (noting that, with respect to medical monitoring, many "procedures are invasive and carry health risks that must be weighed against the procedures' potential benefits" and "there are risks that patients may take false reassurance from the monitoring, or that false positives could lead to unnecessary, costly, or dangerous follow-up procedures").

136 *See In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 852 (3d. Cir. 1990) (requiring that a plaintiff be "significantly exposed to a proven hazardous substance" in order to establish a cause of action for medical-monitoring damages).

that reflects a principle that applies broadly throughout American jurisprudence. Literally translated, it means "[t]he law does not concern itself with trifles."[137] In the field of torts, this means that a person who is unable to prove actual losses is rarely able to recover an award of nominal damages.[138] Instead, a plaintiff ordinarily must demonstrate a significant injury to his or her personal interests before the law will grant a remedy.[139] Courts usually overlook mere technical interference with another's rights.[140]

The de minimis principle suggests that it is appropriate for judges to apply a threshold requirement in cybersecurity litigation when deciding whether to award credit-monitoring damages. The courts should permit a plaintiff who would not otherwise suffer actual losses from a data-security breach to recover credit-monitoring costs only if the defendant has seriously exposed the plaintiff's personal data to the risk of identity theft to the extent that a reasonably prudent person would incur credit-monitoring costs. Presumably, whether the plaintiff has crossed the threshold for recovery will depend on various factors relating to the nature of the breach. According to one formulation:

> The factors used in determining whether remedial measures are reasonably necessary include the likelihood of future harm, whether a plaintiff (or her data) has been exposed, how much of the risk of future harm comes from the exposure instead of from other sources, and the cost-effectiveness of remedial measures.[141]

It may be useful to differentiate between intentional and negligent breaches of security. The former category includes hacking, theft of information or equipment, and misrepresentations deliberately made to obtain data.[142] In contrast, the latter category encompasses such things as loss of computers, hardware, or media containing data, unintentional exposure of

---

137 BLACK'S LAW DICTIONARY 496 (9th ed. 2009) (defining "*de minimis non curat lex*").

138 *See* VINCENT R. JOHNSON & ALAN GUNN, STUDIES IN AMERICAN TORT LAW 51 (4th ed. 2009) (indicating that nominal damages are normally available only in actions involving the five intentional torts which descended from the writ of trespass).

139 DAN B. DOBBS, THE LAW OF TORTS § 377, at 1047 (2000).

140 *See, e.g.*, United States v. Place, 660 F.2d 44, 53 (2d Cir. 1981) ("[T]he mere detention of mail not in his custody or control amounts to at most a minimal or technical interference with his person or effects, resulting in no personal deprivation at all."), *aff'd*, 462 U.S. 696 (1983).

141 Graves, *supra* note 5, ¶ 36, at 25-26. According to one court discussing medical monitoring:

> In determining the reasonableness and necessity of monitoring, the following factors are relevant: (1) the significance and extent of the plaintiff's exposure to chemicals; (2) the toxicity of the chemicals; (3) the relative increase in the chance of onset of disease in the exposed plaintiff as a result of the exposure, when compared to (a) the plaintiff's chances of developing the disease had he or she not been exposed, and (b) the chances of the members of the public at large of developing the disease; (4) the seriousness of the disease for which the plaintiff is at risk; and (5) the clinical value of early detection and diagnosis.

Potter v. Firestone Tire & Rubber Co., 863 P.2d 795, 824-25 (Cal. 1993) (en banc).

142 GAO REPORT, *supra* note 96, at 19 (discussing intentional breaches of data security).

data on the Internet, and improper disposal of data.[143] In American tort law generally, courts routinely extend liability further in cases involving intentionally tortious conduct than in suits based on mere negligence.[144]

In some cases, proof that a hostile action caused the cybersecurity breach will establish the seriousness of data exposure.[145] Thus, if a thief steals a laptop containing social security numbers,[146] it is easier to conclude that affected data subjects are at an increased risk of identity theft, than if the owner merely lost or misplaced the laptop.[147] The same may be true if an unauthorized person opened a new bank account using an affected data user's social security number soon after the security breach occurred[148] or if a renegade employee with access to thousands of patient files actually sold some of that information to an identity theft ring.[149] In contrast, if a server containing customers' information is only one of many items of hardware that thieves took and no evidence exists that the thieves had any interest in the data rather than the hardware, it may be difficult to conclude that the plaintiffs have reached the exposure threshold for an award of credit-monitoring damages.[150]

---

143 *Id.* (discussing negligent breaches of data security).

144 *See, e.g.*, Ross v. Holton, 640 S.W.2d 166, 174 (Mo. Ct. App. 1982) ("In the area of intentional torts a submissible punitive damages question is made for the jury once the plaintiff has presented sufficient evidence of legal malice—the intentional doing of a wrongful act without just cause or excuse." (citing Pollack v. Brown, 569 S.W.2d 724, 733 (Mo. 1978) (en banc))).

145 *Cf. EMU Probes Security Breach of Student Data*, DETROIT NEWS, Mar. 11, 2011, at 3A (discussing a situation where "[n]ames, birth dates, and Social Security numbers were improperly accessed by two former student employees" who improperly transmitted that information); Editorial, *supra* note 29 (discussing the theft of customers' names and e-mail addresses).

146 *Cf.* Garnett v. Millennium Med. Mgmt. Res., Inc., No. 10 C 3317, 2010 WL 5140055, at *1 (N.D. Ill. Dec. 9, 2010) (involving the theft of a portable hard drive during a burglary).

147 *See* Giordano v. Wachovia Sec., LLC, No. 06-476 (JBS), 2006 WL 2177036, at *5 (D.N.J. July 31, 2006) (denying recovery of credit-monitoring damages based on lack of standing, and noting that "Plaintiff failed to allege even that her financial information was stolen or ended up in the possession of someone who might potentially misuse it. . . . [and] merely alleges that a version of her personal financial information was lost"); *see also* Graves, *supra* note 5, ¶ 31, at 23 ("[S]ome courts have imported the 'exposure' question into data loss cases by requiring plaintiffs to show that their data was either (a) acquired or (b) misused by a third party, as opposed to merely lost."); *id.* ¶ 65, at 47 ("A plaintiff who seeks monitoring costs following a hacking-related breach probably has a greater chance of suffering identity fraud than a plaintiff who sues after a laptop is lost; their claims should not be treated the same.").

148 *See* Krottner v. Starbucks Corp., 628 F.3d 1139, 1140-41 (9th Cir. 2010) (involving similar facts). The court stated in the context of a standing inquiry that "[w]ere Plaintiffs-Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible." *Id.* at 1143.

149 Burstein, *supra* note 87 (indicating that the hospital offered one year of free credit monitoring to 44,000 patients after the information of some patients had been sold).

150 *See* Stollenwerk v. Tri-W. Health Care Alliance, 254 F. App'x 664, 665 (9th Cir. 2007) (denying credit-monitoring damages on these facts).

Similarly, credit monitoring's appropriateness may be a factor of the time period for which the defendant exposed the plaintiff's data to wrongful third-party access and the ease with which third parties could achieve access. A court has a stronger basis to conclude that a data subject is at a heightened risk for identity theft if the defendant negligently posted personal information on the Internet or in another public location for a period of months,[151] than if the information was accessible for only six days and no evidence exists that anyone actually accessed or misused the data.[152] The same is true if third persons could freely access personal information on the web rather than obtain it only via a password and login.[153]

Finally, in some cases, it may be appropriate to take into account the nature of personal information at issue in determining whether courts should award credit-monitoring damages. The loss of data linking a person's name, social security number, and birth date is undoubtedly more serious than the loss of data involving only a name and e-mail address.[154]

It is not possible to state a precise rule defining the threshold for an award of credit-monitoring damages. In any given case, many factors may be relevant. On the one hand, courts should not permit an award of credit-monitoring damages in cases where there is no significant threat that the affected data subjects will become victims of identity theft. On the other hand, an award of credit-monitoring damages should not hinge upon the plaintiff's showing that the intruder actually misused sensitive personal information.[155]

---

151 Kirtley, *supra* note 23, at 29 (discussing a data security breach at a university where patient information was improperly posted on the Internet for twenty months); Jaymes Song, *APNewsBreak: University Posts Info of 40K Students*, BOS. GLOBE (Oct. 29, 2010), http://www.boston.com/news/education/higher/articles/2010/10/29/apnewsbreak_university_posts_info_of_40k_students/ (stating that "Social Security numbers, grades and other personal information of more than 40,000 former University of Hawaii students were posted online for nearly a year before being removed" because a faculty member studying student success rates uploaded the material to what he believed was a secure server).

152 *See In re* Davis, 430 B.R. 902, 907 (Bankr. D. Colo. 2010) (finding that the plaintiff lacked standing to recover credit-monitoring damages for alleged harm resulting from improper exposure of data for six days). The court noted that the "Plaintiff's need for credit monitoring is conjectural or hypothetical." *Id.*

153 *See In re* Matthys, No. 09-16585-AJM-13, 2010 WL 2176086, at *3 (Bankr. S.D. Ind. May 26, 2010) (rejecting an invasion of privacy claim related to a court filing that improperly disclosed a social security number).

154 *Cf.* Allison v. Aetna, Inc., No. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010) (denying relief on federal standing grounds and noting that "[e]ven assuming that the hackers obtained Plaintiff's email address, it is highly speculative that they obtained any other information that would be necessary to commit identity theft"); Editorial, *supra* note 29 (discussing the theft of customer names and e-mail addresses).

155 *Cf. In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 851 (3d Cir. 1990) (stating that, in the medical-monitoring context, "the appropriate inquiry is not whether it is reasonably probable that plaintiffs will suffer harm in the future, but rather whether medical monitoring is, to a reasonable degree of medical certainty, necessary in order to diagnose properly the warning signs of disease").

In *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*,[156] a federal court in New York dismissed a negligence claim seeking credit-monitoring damages.[157] In that case, a thief stole password-protected laptops from a pension consultant's office.[158] The court held that the plaintiff had failed to demonstrate a rational basis for serious concerns about the personal information contained on the laptops.[159] As the court explained:

> Factors giving rise to a demonstrable basis for a serious concern over misuse may include evidence of the following: (1) the [lack of] any password-protection for use of the computer such that an unsophisticated user could boot the computer and immediately access the file; (2) that the person stealing the hard drive was motivated by a desire to access the data and had the capabilities to do so; or (3) actual access or misuse of information of the plaintiff or another person whose data was stored on the same hard drive. This Court cannot say with confidence that New York would recognize a claim if any or all of these elements were met. However, the Court can comfortably conclude that New York would not allow a claim to proceed where none of these elements are present.[160]

B. *Reasonably Necessary*

The critical question is whether, based on the facts of a case, credit-monitoring expenditures are reasonably necessary. In this regard, courts should give considerable weight to community practices. If a cybersecurity breach involves the type of facts that commonly prompt businesses to offer credit monitoring to affected persons,[161] courts to approve settlements including compensation for credit monitoring,[162] or governmental entities to provide for or require the provision of credit-monitoring services or reimbursement for such expenses,[163] there should be little question about the reasonable necessity of such expenditures.

While it is important to consider whether credit-monitoring expenditures are cost-effective, it is unreasonable to expect courts to engage in the type of economic analysis that will yield a convincing mathematical answer to this question. Estimates about the risks and costs of identity theft are simply too various to produce convincing results.[164] Calculations often unreasonably discount or ignore very real considerations, such as the emotional distress, inconvenience, and lost time that result from breaches of

---

156 580 F. Supp. 2d 273 (S.D.N.Y. 2008).

157 *Id.* at 275-76.

158 *Id.* at 282.

159 *Id.*

160 *Id.*

161 *See supra* Part II.B.

162 *See supra* Part II.C.

163 *See supra* Part II.D.

164 For one such effort, see Graves, *supra* note 5, ¶¶ 79-82, at 56-58.

data security.[165] Judges can better assess whether expenditures on credit monitoring are cost-effective by reference to what businesses, courts, and governmental agencies actually do rather than by judicial calculations seeking to quantify the wisdom of credit monitoring through economic analysis.

In *Stollenwerk v. Tri-West Health Care Alliance*,[166] the Ninth Circuit concluded the expenditures on credit monitoring were not reasonably necessary because the plaintiffs could have reviewed their credit reports for free and could have placed a fraud alert in their files.[167] However, a once-a-year free credit report[168] is no substitute for daily credit monitoring to detect the opening of unauthorized accounts and "a fraud alert is only available for ninety days, unless the victim has already suffered fraud."[169] *Stollenwerk*'s conclusion that there was "no showing that a normally prudent person in these circumstances would have taken precautions beyond the free services" is at odds with recent developments.[170] There is now abundant evidence showing that businesses,[171] courts,[172] and government agencies[173] often authorize expenditures on credit monitoring, even though affected data subjects could obtain free credit reports each year from credit-reporting agencies and place fraud alerts in their file that would be effective for a limited period of time.

C. *Duration of Monitoring*

Medical-monitoring precedent recognizes that the length of time during which monitoring is appropriate varies with the facts of a case.[174] Courts must consider the toxicity of the chemical or other matter at issue, the length of the plaintiff's exposure, and the foreseeable period during which

---

165 *See, e.g., id.* ¶ 55, at 39 (discussing attempts to calculate average loss incurred by fraud victims as measured by "out-of-pocket losses" alone (footnote omitted)).

166 254 F. App'x 664 (9th Cir. 2007).

167 *Id.* at 667.

168 The Fair Credit Reporting Act requires each of the nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to provide persons with a free copy of their credit report, upon request, once every twelve months. *Facts for Consumers*, FED. TRADE COMMISSION, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm (last modified Aug. 24, 2010).

169 Graves, *supra* note 5, ¶ 77, at 55.

170 *Stollenwerk*, 254 F. App'x at 667.

171 *See supra* Part II.B.

172 *See supra* Part II.C.

173 *See supra* Part II.D.

174 *See* Bourgeois v. A.P. Green Indus., Inc., 716 So. 2d 355, 361 (La. 1998) ("[T]o ensure that only meritorious claims are compensated, plaintiff's recovery of medical monitoring costs must be both reasonable and limited in duration to the maximum latency period (if known) of the diseases for which there is an increased risk."); *see also* Day v. NLO, 851 F. Supp. 869, 884 (S.D. Ohio 1994) ("The extent and duration of diagnostic monitoring is a matter for medical professionals under the supervision of the court to decide.").

resulting symptoms of disease or injury may be latent.[175] Based on particular facts, a longer period of monitoring may be more appropriate in one case than in another.

Similarly, the length of time that credit monitoring should continue depends on the circumstances. Exposure of highly sensitive personal information, such as social security and bank account numbers for a long period of time, will undoubtedly call for longer monitoring than brief exposure of less significant information. However, there is no binding rule. In some cases, the one or two years of credit monitoring that a potential defendant offers may be all that the facts warrant.[176] In other cases, it may be reasonable to continue monitoring for a longer period of time.[177] Little more can be said than that, whatever the period, the plaintiff must prove that the proposed length of time for monitoring is reasonably necessary.[178] Of course, courts will likely greet claims seeking compensation in the form of lifetime monitoring with skepticism,[179] except in the rarest case.

IV. ARGUMENTS AGAINST RECOVERY

An important hurdle to overcome in recovering credit-monitoring damages is convincing a court that the victim of a serious cybersecurity breach suffers a legally cognizable injury even before the perpetrator steals his or her identify.[180] Not all courts are willing to accept this proposition, and some courts operate under the misconception that a claim for credit-monitoring damages is a request for compensation for increased risk of

---

175 *See Bourgeois*, 716 So. 2d at 360-61.

176 *Cf.* Ruiz v. Gap, Inc., 380 F. App'x 689, 691 (9th Cir. 2010) (indicating that although "California courts have not considered whether time and money spent on credit monitoring as the result of the theft of personal information are damages sufficient to support a negligence claim," the court did not need to reach that question because the plaintiff "failed to establish a genuine issue of material fact on whether he suffered damages because he offered no evidence on the amount of time and money he spent on the credit monitoring, or that Gap's offer would not fully recompense him").

177 *Cf. Bourgeois*, 716 So. 2d at 361 (stating that medical-monitoring costs should be based on the "maximum latency period . . . of the diseases for which there is an increased risk").

178 *Cf. In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 851 (3d Cir. 1990) (stating that, in the medical-monitoring context, "concerns about the degree of certainty required can easily be accommodated by requiring that a jury be able reasonably to determine that medical monitoring is probably, not just possibly, necessary"); Askey v. Occidental Chem. Corp., 102 A.D.2d 130, 137 (N.Y. App. Div. 1984) (indicating that expenses for medical monitoring are recoverable as consequential damages "provided that plaintiffs can establish with a reasonable degree of medical certainty that such expenditures are 'reasonably anticipated' to be incurred by reason of their exposure").

179 *See* Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281 n.2, 283-84 (S.D.N.Y. 2008) (rejecting a negligence claim seeking lifetime monitoring damages).

180 *See* Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010) (supplemental opinion).

harm.[181] This Part explains that credit-monitoring damages are preventive expenditures that are wholly distinct from both the unwieldy concept of increased risk of harm (which is not a proper basis for measuring damages in a cybersecurity case) and from the harm that results if a data-security breach ultimately causes identity theft. In addition, this Part argues that, contrary to the holdings of some cases, standing principles should not control the compensability of credit-monitoring damages because issues of standing and damages are legally distinguishable. Finally, this Part contends that courts have no basis to hold that plaintiffs cannot recover credit-monitoring damages from negligent defendants simply because they can purchase credit monitoring for themselves in order to self-protect against the harm that breaches of cybersecurity cause.

A. *Present Injury Versus Increased Risk of Harm*

A number of cases have held that plaintiffs cannot recover credit-monitoring damages because, until identity theft occurs, a data subject affected by a cybersecurity breach has not suffered an injury.[182] For example, in *Rowe v. UniCare Life & Health Insurance Co.*,[183] the plaintiff sought to recover credit-monitoring costs and other damages when the defendants temporarily posted personal information on the Internet.[184] In addressing those claims, a federal court in Illinois decided several legal issues in the plaintiff's favor and denied the defendants' motion to dismiss.[185] However, with respect to the claim for credit-monitoring damages, the court wrote:

> [F]ederal courts have accepted the increased risk of future harm as an injury and allowed for the recovery of future damages. If Rowe is able to show an increased risk of future harm, the Court may admit evidence regarding the cost of credit monitoring services in order to calcu-

---

181 *See* Rowe v. UniCare Life & Health Ins. Co., No. 09 C 2296, 2010 WL 86391, at *7 (N.D. Ill. Jan. 5, 2010).

182 *See, e.g.*, *Krottner*, 406 F. App'x at 131 (stating, in an action arising from the theft of a laptop containing employee information, which raised issues related to credit monitoring, that the "mere danger of future harm, unaccompanied by present damage, will not support a negligence action" (quoting Gazija v. Nicholas Jerns Co., 543 P.2d 338, 341 (Wash. 1975) (en banc)) (internal quotation marks omitted)); *see also* Hendricks v. DSW Shoe Warehouse Inc., 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006). In *Hendricks*, the plaintiff sued not for negligence, but for breach of contract and violation of the Michigan Consumer Protection Act. *Id.* at 780-81. In denying recovery of credit-monitoring damages, the court noted that Michigan does not permit recovery of medical-monitoring damages, writing:

> There is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss. Indeed, there is reason to believe that Michigan's highest court would reject a novel legal theory of damages which is based on a risk of injury at some indefinite time in the future.

Id. at 783.

183 No. 09 C 2296, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010).

184 *Id.* at *1.

185 *Id.* at *9.

late the damages that can be attributed to that increased risk. Nonetheless, the costs of credit monitoring services are not a present harm in and of themselves. Instead, they may be useful in the evaluating some cognizable future harm.[186]

This line of reasoning misses the point. In cases of breached data security, the defendant must incur the costs of credit monitoring to minimize the special threat of economic harm resulting from data exposure, regardless of whether identity theft ever occurs. As such, credit-monitoring expenses are independent of, and distinguishable from, whatever harm may mature in the future if a perpetrator ultimately misuses the personal data placed at risk. Credit-monitoring costs are not merely a factor in valuing increased risk of harm.

1. Two Categories of Harm

To put the matter somewhat differently, it is useful to segregate the damages resulting from data exposure into two categories: first, costs that plaintiffs reasonably incur to prevent identity theft when defendants seriously breach data security, and second, costs resulting from identity theft. Expenses falling within the first category include the costs of credit monitoring and certain out-of-pocket expenditures, such as replacing drivers' licenses, changing account numbers, and ordering new checkbooks. If there is credible evidence of a serious data-security breach,[187] the defendant should incur these types of expenses because they minimize the likelihood of future economic harm. This is especially true because such expenditures are typically modest in comparison to the harm that can result from identity theft.

In contrast, expenses falling within the second category, namely losses resulting from identity theft, are intended not *to prevent* harm that the plaintiff can avoid by the exercise of reasonable care, but *to redress* harm already proximately caused. If the plaintiff has accrued such losses prior to trial, the plaintiff should be able to recover them. However, such evidence is often unavailable because the risk of identity theft has not yet come to fruition. In that case, courts should deny compensation for damages relating to the second category because it is a matter of speculation whether identity theft will ever occur, and the law routinely denies recovery for damages not proven with reasonable certainty.[188] There is no reason to follow a different rule in cybersecurity cases.

Courts should focus on the two specified categories of damages (costs incurred to prevent harm and costs resulting from identity theft) and reject

---

186 *Id.* at *7.

187 *See supra* Part III.A (discussing the threshold for recovery of credit-monitoring damages).

188 *E.g.*, Landry v. Spitz, 925 A.2d 334, 347 (Conn. App. Ct. 2007).

the idea that cybersecurity cases provide compensation for increased risk of harm. Increased risk of harm is an unworkable measure for damages in these types of cases because there is no way to estimate with reasonable precision the degree to which data exposure increases the risk of identity theft.

2. Contrast to Loss of a Chance

A useful contrast can be drawn by reference to the concepts of increased harm (alternatively known as "loss of a chance"[189]) that have crystallized in the field of medical-malpractice liability. Many courts permit a patient harmed by a physician's negligence to recover compensation for an increased risk of harm.[190] For example, this may include the increased chance of dying that results from negligent failure to detect or disclose a diseased condition which, though capable of treatment, grows more severe as a result of delayed attention.[191] Courts award increased-risk-of-harm damages because generally accepted scientific principles have made it possible to calculate percentage increases in the chances of harm with reasonable precision.[192] For example, in *Matsuyama v. Birnbaum*,[193] the Supreme Judicial Court of Massachusetts recognized the loss of chance doctrine and held that "[i]n order to prove loss of chance, a plaintiff must prove by a preponderance of the evidence that the physician's negligence caused the plaintiff's likelihood of achieving a more favorable outcome to be diminished."[194] Explaining the operation of the doctrine, Chief Justice Margaret H. Marshall wrote:

> We reject the defendants' contention that a statistical likelihood of survival is a "mere possibility" and therefore "speculative." . . . [S]urvival rates are not random guesses. They are estimates based on data obtained and analyzed scientifically and accepted by the relevant medical community as part of the repertoire of diagnosis and treatment, as applied to the specific facts of the plaintiff's case. . . . The key is the reliability of the evidence available to the fact finder. . . . [F]or certain conditions, medical science has progressed to the point that physicians can gauge a patient's chances of survival to a reasonable degree of medical certainty,

---

189 *See* Alberts v. Schultz, 975 P.2d 1279, 1281, 1283 (N.M. 1999) (recognizing the "loss of a chance" doctrine and stating that "[s]ome courts seek to clarify the theory by use of the term 'increased risk of harm'" (quoting Gardner v. Pawliw, 696 A.2d 599, 613 (1997))).

190 *See, e.g.*, Scafidi v. Seiler, 574 A.2d 398, 403 (N.J. 1990).

191 *See* O'Brien v. Stover, 443 F.2d 1013, 1018 (8th Cir. 1971).

192 *See* Matsuyama v. Birnbaum, 890 N.E.2d 819, 828 n.23 (Mass. 2008). The court observed that:

> The highest courts of at least twenty States and the District of Columbia have adopted the loss of chance doctrine. . . . Ten States' high courts have, in contrast, refused to adopt the loss of chance doctrine. . . . Other States' high courts have not addressed the issue or have explicitly left the question open. The Draft Restatement discusses loss of chance but 'takes no position on this matter, leaving it for future development and future Restatements'.

Id. (citations omitted).

193 890 N.E.2d 819 (Mass. 2008).

194 *Id.* at 832.

> and indeed routinely use such statistics as a tool of medicine. . . . The availability of such expert evidence on probabilities of survival makes it appropriate to recognize loss of chance as a form of injury.[195]

However, the *Matsuyama* court was quick to point out the limits of a doctrine permitting recovery in a tort action for increased risk of harm. The court cautioned: "[O]ur decision today is limited to loss of chance in medical malpractice actions. . . . [because] reliable expert evidence establishing loss of chance is more likely to be available in a medical malpractice case than in some other domains of tort law."[196]

In contrast to the field of medical services, there are no established scientific principles that can quantify increased risk of identity theft in cybersecurity cases. Consequently, it is inappropriate for courts to base compensation in such cases on increased risk of harm. Rather, courts should award damages only for losses that the plaintiff can prove with reasonable certainty. In many instances, credit-monitoring costs and other measures intended to prevent identity theft are reasonable, appropriate, and foreseeable consequences of a defendant's negligent failure to protect data from unauthorized access or to promptly disclose a security breach.[197] In some instances, it is also possible to establish, with reasonable certainty, losses that resulted from identity theft linked to unprotected personal data.[198] However, courts should not award damages for mere increased risk of harm in cases where identity theft has not occurred.

3. Differentiating Damages from Standing

It is important to distinguish proof of damages from standing to litigate in federal court. Article III's "case" or "controversy" requirement necessi-

---

195 *Id.* at 833-34.

196 *Id.* at 834-35.

197 For example, when Sony's PlayStation Network was hacked, resulting in 77 million accounts being jeopardized, Sony attempted to "win back customers . . . with free credit monitoring." *Sony Offers Credit Monitoring to Playstation Network Customers*, MYCREDITSPECIALIST.COM, http://blog.mycreditspecialist.com/2011/05/11/sony-offers-credit-monitoring-to-playstation-network-customers/ (last visited Sept. 20, 2011); *see also* Patrick Klepek, *PSN Hacked: What Sony's Security Breach Means for You (And What Comes Next)*, GIANT BOMB (Apr. 27, 2011), http://www.giantbomb.com/news/psn-hacked-what-sonys-security-breach-means-for-you-and-what-comes-next/3092/. One customer stated that Sony's offer of credit monitoring "is the single biggest item in Sony's apology" which will help prevent its customers from falling prey to "phishing scams, attempted address changes . . . and other chicanery for years to come." *Sony to Offer Help with Credit Monitoring*, GAMEWIT (May 1, 2011, 1:36 AM), http://gamewit.blogs.pressdemocrat.com/13485/sony-to-offer-help-with-credit-monitoring/.

198 Johnson, *supra* note 1, at 299-300 (explaining how out-of-pocket damages are "susceptible to proof with a high degree of certainty" because the plaintiff can introduce receipts as evidence of expenses).

tates proof of injury in fact.[199] As explained in *Lujan v. Defenders of Wildlife*:[200]

> [O]ur cases have established that the irreducible constitutional minimum of standing contains three elements. First, the plaintiff must have suffered an "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—the injury has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision."[201]

In federal cybersecurity litigation, courts have addressed the Constitutional standing requirement. Thus, in *Pisciotta v. Old National Bancorp*,[202] Judge Kenneth F. Ripple wrote for the Seventh Circuit:

> Many . . . cases have concluded that the federal courts lack jurisdiction because plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing. We are not persuaded by the reasoning of these cases. As many of our sister circuits have noted, the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions. We concur in this view. Once the plaintiffs' allegations establish at least this level of injury, the fact that the plaintiffs anticipate that some greater potential harm might follow the defendant's act does not affect the standing inquiry.[203]

Cases decided subsequent to *Pisciotta* have generally reached the same conclusion,[204] although there is authority to the contrary.[205] However, for present purposes, the critical point is that federal issues related to standing are different and properly distinguishable from state-law issues related to tort damages.[206] Whether or not an increased risk of identity theft gives one

---

199 U.S. CONST. art. III, § 2, cl. 1.

200 504 U.S. 555 (1992).

201 *Id.* at 560 (second, third, fourth, fifth, and sixth alterations in original) (citations omitted).

202 499 F.3d 629 (7th Cir. 2007).

203 *Id.* at 634 (footnotes omitted).

204 *See, e.g.*, Krottner v. Starbucks Corp., 628 F.3d 1139, 1140 (9th Cir. 2010) (finding that allegations that the theft of a laptop subjected thousands of employees to an increased risk of future identity theft was sufficient to establish injury-in-fact standing).

205 *See* Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1051-52 (E.D. Mo. 2009) (finding that the plaintiff lacked standing because the alleged injury was not "imminent" but noting that otherwise "[s]ubsequent to the Seventh Circuit's decision in *Pisciotta*, district courts have consistently determined that claims of increased risk of identity theft resulting from security breaches sufficiently allege an injury-in-fact to confer Article III standing to those persons bringing such claims"); *In re* Davis, 430 B.R. 902, 907 (D. Colo. 2010) (finding that the plaintiff lacked standing because the harm resulting from improper exposure of data for six days was not "actual" or "imminent" where there was no evidence that the data was "accessed or misused" (first and second internal quotation marks omitted)).

206 *See* Krottner v. Starbucks Corp., 406 F. App'x 129, 131 (9th Cir. 2010) (supplemental opinion) (citing Doe v. Chao, 540 U.S. 614, 624-25 (2004)).

standing to assert a cybersecurity claim should not depend on whether a plaintiff can recover damages for increased risk of harm under state law. It also should not mean that credit-monitoring expenditures are not a compensable form of loss resulting from a security breach.[207] Moreover, parties do not litigate all cybersecurity cases in federal court.[208] To that extent, federal court precedent on standing is unlikely to present a useful guide to resolve state-law issues related to tort damages.

B. *Self-Protection Against This Type of Loss*

The American Law Institute's project on tort liability for economic loss is now in abeyance, and none of the project's drafts were ever approved.[209] However, Council Draft No. 2 proposed that there should be no liability for negligently-caused, pure economic loss if "the claimant reasonably could have, by contract with the actor or through an intermediary, protected itself from the loss."[210] Thus, in assessing the compensability of credit-monitoring damages, it is fair to ask whether the courts should bar recovery for this form of loss because, before the cybersecurity breach occurred, the plaintiff could have bargained with the defendant about what damages he or she could recover. In addition, a separate, but related, question is whether a potential plaintiff is foreclosed from recovering credit-monitoring costs in cybersecurity tort actions when the plaintiff had the ability to self-protect against unauthorized use of personal information by purchasing credit-monitoring services.

---

207 *See id.* (holding, in a cybersecurity action, that although the plaintiffs "pled an injury-in-fact for purposes of Article III standing" they did not "adequately [plead] damages for purposes of their state-law claims"). *But see* Hammond v. Bank of N.Y. Mellon Corp., No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *9 (S.D.N.Y. June 25, 2010) (finding that the plaintiffs lacked standing, and, if they had standing, they would also be unable to prove damages).

208 *See supra* Part II.

209 The American Law Institute states:

> The Council approved the start of the project in 2004. Thus far, no part of the work has been approved by the Council or by the membership. Professor Mark Gergen resigned as the project's Reporter in late 2007; the project is in abeyance while the Director seeks a successor Reporter.

Johnson, *supra* note 57, at 535 n.60 (internal quotation marks omitted) (quoting material previously posted at *Current Projects: Restatement Third, Torts: Liability for Economic Harm*, AM. L. INST., http://www.ali.org/index.cfm?fuseaction=projects.proj_ip&projectid=15). Although work on the Restatement (Third) of Torts has been underway for roughly twenty years, and many parts have been completed, numerous important subjects remain to be addressed. *See* Vincent R. Johnson, *The Vast Domain of the* Restatement (Third) of Torts, 1 WAKE FOREST L. REV. ONLINE 29, 29-35 (2010), *available at* http://lawreview.law.wfu.edu/files/2011/01/Johnson_Forum.pdf (surveying challenges relating to the unfinished work).

210 RESTATEMENT (THIRD) OF TORTS: ECON. TORTS & RELATED WRONGS § 8(3)(c)(i) (Council Draft No. 2, 2007).

In thinking about these questions, it is useful to note that the proposed *Restatement* language changed during the drafting process. The first draft submitted to the American Law Institute Council in October 2006 proposed that there should be no liability for negligence that causes pure economic loss if "the claimant could have obtained redress for the harm from the actor by contract with the actor or through an intermediary."[211] However, the Reporter revised that same provision in the second Council draft in October 2007 by inserting the word "reasonably." The second Council draft proposed that there should be no liability for negligently caused pure economic loss if "the claimant *reasonably* could have, by contract with the actor or through an intermediary, protected itself from the loss."[212] The insertion of the word "reasonably" was significant in terms of the sweep of the proposed provision. That word narrowed the range of cases in which hypothetical contract remedies would limit recovery in tort cases for pure economic losses to only those cases where it would have been reasonable under the existing circumstances for the plaintiff to seek contractual protection. By including the word "reasonably," the proffered *Restatement* rule no longer reflected a broad preference for contract remedies in any case in which a contract remedy might be theoretically possible. Rather, the revised rule, framed in terms of reasonableness, would have "separate[d] tort and contract claims by encouraging parties to allocate risk contractually"[213] only in the range of cases where contractual protection was reasonably feasible.

1. Not a Proper Subject for Bargaining

As noted earlier, the language of state security breach notification laws strongly suggests that the data-protection and the breach-disclosure obligations that they impose are not a proper subject for bargaining between data possessors and data subjects.[214] Agreements that vary those duties are normally void as against public policy.[215]

Of course, bargaining about remedies is not the same as bargaining about duties. Nevertheless, the fact that bargaining about cybersecurity duties may be futile is a good basis for concluding that a reasonable person would not bargain about related cybersecurity remedies. To that extent,

---

211 *Id.* § 8(4)(c)(i). The draft stated that:

> (4) An actor who unintentionally (and without dishonesty or disloyalty) causes pure economic loss is not subject to negligence or strict liability in tort for the loss . . . when . . . (c) liability is unnecessary to deter the conduct or avoid or redress the harm because (i) the claimant could have obtained redress for the harm from the actor by contract with the actor or through an intermediary . . . .

Id.

212 *Id.* § 8(3)(c)(i) (emphasis added).

213 City of Boston v. Smith & Wesson Corp., 12 Mass. L. Rptr. 225, 231 (Super. Ct. 2000).

214 *See supra* Part I.C.2.

215 *See supra* Part I.C.2.

contracting with a defendant is not a reasonable alternative for protecting oneself against the costs of credit monitoring that are made reasonably necessary by a breach of cybersecurity.

Furthermore, because data about any given person is held by a large and ultimately unpredictable range of entities, it would be unreasonable to expect persons to bargain with all possible defendants over liability for credit-monitoring damages. In that case, "[c]onsumers would spend an inordinate amount of resources on efforts to perform often duplicative, time-consuming tasks relating to assessment of the risks of injury and the need for economic protection."[216]

In assessing whether bargaining provides a reasonable option for a potential plaintiff to safeguard economic interests, it is important to consider the relative economic positions of the parties. Such facts bear upon the issue of whether the plaintiff had adequate bargaining power to make contractual protection a *reasonable* possibility.

Where the defendant, acting from a position of economic advantage, deals with the plaintiff on a "take it or leave it basis," bargaining for remedies related to breaches of cybersecurity may not be feasible. For example, many cybersecurity breaches have involved unauthorized access to university alumni records.[217] A graduate of a university might theoretically succeed in bargaining with the university to remove his or her name from some database on a take it or leave it basis, such as by purging the graduate's name from the mailing lists for the university magazine or fundraising. But it seems fanciful to suggest that the graduate could negotiate with the university over the availability of credit-monitoring damages for losses that may occur if the graduate remains on those lists. Moreover, it is highly unlikely that, under any circumstances, the graduate could reach a bargain with the university obliging the latter to remove the graduate's name from its academic records databases, or to pay for credit monitoring if a perpetrator breaches the security of those records.

2. Collateral Sources and Causation Principles

Theoretically, one might argue that plaintiffs should not recover credit-monitoring damages because potential plaintiffs could obtain credit-monitoring insurance for themselves prior to any unauthorized intrusion into or revelation of their data. A federal court in Michigan spotted, but did not explore, this issue. In denying recovery of credit-monitoring damages

---

216 Vincent R. Johnson, *Liberating Progress and the Free Market from the Specter of Tort Liability*, 83 NW. U. L. REV. 1026, 1042 (1989) (book review).

217 White Paper, An Examination of Database Breaches at Higher Education Institutions, at 1, http://www.appsecinc.com/techdocs/whitepapers/Higher-Ed-Whitepaper-Edited.pdf (last visited Sept. 20, 2011).

under breach of contract and deceptive trade practices theories, the court observed that "perhaps it would be prudent for everyone to monitor their credit."[218]

However, even if one assumes that it is unreasonable for a potential plaintiff not to buy credit-monitoring protection as a matter of course, that failure should have no bearing on the defendant's liability for credit-monitoring expenditures for at least two reasons. First, the collateral-source rule,[219] which is still widely followed outside of the medical-malpractice context,[220] holds that the fact that the plaintiff has insurance does not reduce the defendant's liability.[221] To hold otherwise would undercut the incentive for persons to self-protect against the costs of accidents. When persons purchase insurance, they intend to protect their own interests and not the interests of potential defendants.

Second, a plaintiff's failure to purchase credit-monitoring services should not be treated as a form of contributory negligence, comparative negligence, or comparative fault.[222] For conduct to constitute a defense within those categories, it must have unreasonably multiplied the chances that the injury for which recovery is sought would occur.[223] Unlike jaywalking into a busy street or using a defective electrical appliance in a wet location, the failure to purchase credit-monitoring insurance does not multiply

---

218 Hendricks v. DSW Shoe Warehouse Inc., 444 F. Supp. 2d 775, 779 (W.D. Mich. 2006).

219 *See* RESTATEMENT (SECOND) OF TORTS § 920A cmt. c, at 514 (1979) ("The rule that collateral benefits are not subtracted from the plaintiff's recovery applies to . . . [i]nsurance policies, whether maintained by the plaintiff or a third party."); *see also* Christian D. Saine, Note, *Preserving the Collateral Source Rule: Modern Theories of Tort Law and a Proposal for Practical Application*, 47 CASE W. RES. L. REV. 1075, 1119 (1997) ("Many states have not changed the traditional rule and some that have changed it have had the statute overturned by state supreme courts.").

220 *See* Kenneth S. Abraham, *What Is a Tort Claim? An Interpretation of Contemporary Tort Reform*, 51 MD. L. REV. 172, 190-91 (1992) (stating that the collateral source rule is a "traditional rule" but has been abolished in numerous jurisdictions in medical malpractice cases). While "firmly entrenched in the American jurisprudence of the law of damages for over a century," the collateral source rule has been the source of debate for many scholars. Nora J. Pasman-Green & Ronald D. Richards Jr., *Who Is Winning the Collateral Source Rule War? The Battleground in the Sixth Circuit States*, 31 U. TOL. L. REV. 425, 425-26 (2000).

221 *See* Joseph M. Perillo, *The Collateral Source Rule in Contract Cases*, 46 SAN DIEGO L. REV. 705, 706 (2009) (stating that under tort principles, "damages assessed against a tortfeasor generally are not diminished by any payments received by the injured party from medical insurance, pension and disability plans, or any sources other than the tortfeasor or the tortfeasor's insurer").

222 *See* JOHNSON & GUNN, *supra* note 138, at 19-20 (differentiating contributory negligence, comparative negligence, and comparative fault).

223 A defendant seeking to base a defense on the plaintiff's negligence must prove that the alleged negligence was a legal cause of the plaintiff's injuries. RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT OF LIAB. § 4 (2000) (discussing "Proof of Plaintiff's Negligence and Legal Causation"). The same causation rules apply in evaluating the conduct of plaintiffs and defendants. *Id.* § 4 cmt. d. A "defendant's conduct can never be a factual cause unless the chances of harm to the plaintiff have been multiplied." VINCENT R. JOHNSON, MASTERING TORTS: A STUDENT'S GUIDE TO THE LAW OF TORTS 117 (4th ed. 2009) (discussing Reynolds v. Tex. & Pac. Ry. Co., 37 La. Ann. 694 (1885)).

the chances of an accident. Failure to subscribe to credit monitoring does not make a breach of cybersecurity more likely.

V. THE CASE FOR CREDIT-MONITORING DAMAGES

There are strong arguments in favor of holding data possessors liable for credit-monitoring damages in cases involving negligently caused breaches of information security. As explained below, these arguments fall into two broad categories. The first deals with effective deterrence of deficient data practices.[224] The second concerns efficient allocation of the economic losses that inevitably arise from the widespread use of digital personal information in contemporary life.

A. *Deterrence of Deficient Data Practices*

Defendants who are not held accountable for the losses they negligently cause often have an insufficient incentive to exercise care and thereby minimize the costs of preventable harm. This is as true with respect to data possessors as it is with regard to other putative defendants. Moreover, it is as true concerning losses resulting from inadequate data security as it is with damages arising from threats of physical injury. However, tort law can play an important role in deterring unnecessary losses. It does this by providing a legal mechanism through which those who neglect to exercise care are called to account for harm that they could have avoided.

At various times, courts have imposed liability for the purpose of deterring negligent data practices. For example, in *Remsburg v. Docusearch, Inc.*,[225] a man purchased information about a woman's workplace address from an Internet-based investigation service, then went to that location and killed her.[226] In a subsequent wrongful death action, the Supreme Court of New Hampshire held that a private investigator or information broker who sells information to a client pertaining to a third party has a duty to the third party to exercise reasonable care in disclosing that information.[227] The court

---

224 That such deficiencies exist is beyond dispute. *See, e.g.*, Doran, *supra* note 122 ("33 percent of medical practices said they did not conduct a security risk analysis of their electronic health records . . . . "). In particular, law firms have been slow to recognize cybersecurity threats and reluctant to disclose information about data security breaches. *See* Karen Sloan, *Firms Slow to Awaken to Cybersecurity Threat*, NAT'L L.J., Mar. 8, 2010, at 5 (indicating that law firms may be targeted not just by run-of-the-mill hackers but by "advanced persistent threats," spying for a long period of time to obtain information about business or litigation strategies (internal quotation marks omitted)).

225 816 A.2d 1001 (N.H. 2003).

226 *Id.* at 1005-06.

227 *Id.* at 1007.

intended for the decision to deter the type of careless data-related practices that create risks of stalking and identity theft.[228]

Similarly, in *Wolfe v. MBNA America Bank*,[229] a federal court in Tennessee held that a bank has a duty "to implement reasonable and cost-effective verification methods that can prevent criminals, in some instances, from obtaining a credit card with a stolen identity."[230] The decision was rooted in concerns about deterring unnecessary economic losses. As the court explained:

> With the alarming increase in identity theft in recent years, commercial banks and credit card issuers have become the first, and often last, line of defense in preventing the devastating damage that identity theft inflicts. Because the injury resulting from the negligent issuance of a credit card is foreseeable and preventable, the Court finds that under Tennessee negligence law, Defendant has a duty to verify the authenticity and accuracy of a credit account application before issuing a credit card.[231]

1. Precautions and Activity Levels

Subjecting potential defendants to liability for the losses that their enterprises cause not only influences what steps those persons take to ensure that an activity does not cause harm, but also the selection of activities in which those persons choose to engage. That is, the risk of liability influences both the choice of precautions and activity levels. For example, "[a] data handler could . . . prospectively limit its exposure to litigation not only by handling data carefully, but also by limiting the number of people about whom it collects data."[232]

In some instances, the implementation of precautions is sufficient to reasonably minimize the chances that certain losses will occur. However, if the exercise of care cannot effectively manage risks, the threat of liability may cause an actor to decide that the activity is not worth undertaking. Risky technologies or practices may be eschewed in favor of other modes of doing business.

---

228 *See id.* at 1008 ("The threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client.").

229 485 F. Supp. 2d 874 (W.D. Tenn. 2007). After the defendant bank issued a credit card bearing the plaintiff's name to an unauthorized person at an address where the plaintiff never lived, the cardholder then ran up charges that exceeded the card's limit and failed to pay. *Id.* at 878-79. After demanding payment from the plaintiff and being informed that he was the victim of identity theft, the bank notified a credit-reporting agency that plaintiff's account was delinquent. *Id.* at 879. That caused a potential employer to reject the plaintiff for a job because of his poor credit score. *Id.*

230 *Id.* at 882.

231 *Id.*

232 Graves, *supra* note 5, ¶ 37, at 27.

For example, a business subject to liability for the loss of computerized information might guard against that risk by encrypting the information of data subjects. If encryption is too inconvenient or expensive, the company might eliminate practices that pose a particular risk of harm, such as by prohibiting employees from taking laptops with unencrypted information away from the business premises. Similarly, the risk of liability may convince a business not to make computerized personal information accessible to company employees via the web because the risk of hacking is just too great. Alternatively, a company may decide that it should purge, rather than retain, outdated files containing personal information.[233]

2. Internalization of Costs

In some instances, the law can promote deterrence by compelling potential defendants to internalize the costs of their endeavors. In other words, the courts use liability to reconcile burdens with benefits.[234] Under this approach, persons cannot keep the profits of an endeavor while simultaneously avoiding responsibility for resulting losses. A person who enjoys the benefits must also bear the costs. This is why courts will hold employers liable for the torts of employees occurring within the scope of employment;[235] possessors of animals liable for bites and other attacks;[236] and contractors liable for damages resulting from the use of dynamite in excavation.[237]

However, as presently configured, American law often allows data possessors to escape responsibility for the losses resulting from their negligent data practices.[238] Yet, data possessors frequently reap the benefits of

---

233 *Cf.* Editorial, *supra* note 29 (recommending federal adoption of a data security policy imposing "maximum periods for retaining personal data").

234 *See, e.g.*, Jones v. Manhart, 585 P.2d 1250, 1252 (Ariz. Ct. App. 1978) (stating that strict liability applies to dog owners, regardless of whether the owner has knowledge of "the vicious propensities of the animal"); JOHNSON & GUNN, *supra* note 138, at 7-8 (explaining that the idea that "[t]hose who benefit from dangerous activities should bear resulting losses" has played an important role in the shaping of modern tort law (emphasis omitted)).

235 *See, e.g.*, Phila. & Reading R.R. Co. v. Derby, 55 U.S. (14 How.) 468, 485-87 (1853) (applying the principle of *respondeat superior* to a railroad company); RESTATEMENT (THIRD) OF AGENCY § 2.04 (2006) (discussing *respondeat superior*).

236 *See, e.g.*, *Manhart*, 585 P.2d at 1252; RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM §§ 22-23 (2010) (discussing liability for harm caused by wild and domestic animals).

237 *See, e.g.*, Starkel v. Edward Balf Co., 114 A.2d 199, 201 (Conn. 1955) ("The explosion of dynamite is an intrinsically dangerous means. Hence, one who explodes dynamite acts at his peril." (citation omitted)); RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 20 & cmt. e (2010) (discussing liability for harm caused by abnormally dangerous activities).

238 Similar conclusions have been reached by a Canadian author. *See* Chandler, *supra* note 55, at 272 ("There is evidence that existing regulatory and market sanctions are insufficient to deter careless

assembling, preserving, and using digital personal information.[239] Imposing liability for credit-monitoring damages will help to ensure that data possessors will internalize the costs that are incidental to their practices. To that extent, they are more likely to engage in honest calculations of whether those practices are worthwhile and carried on in a way that reasonably minimizes the risk of losses associated with breaches of cybersecurity.[240]

With respect to liability for medical-monitoring damages, the Third Circuit explained:

> Medical monitoring claims acknowledge that, in a toxic age, significant harm can be done to an individual by a tortfeasor, notwithstanding latent manifestation of that harm. . . . Allowing plaintiffs to recover the cost of this care deters irresponsible discharge of toxic chemicals by defendants and encourages plaintiffs to detect and treat their injuries as soon as possible. These are conventional goals of the tort system as it has long existed . . . .[241]

The same analysis applies to recovery of credit-monitoring damages in a digital age where delayed detection of identity theft arising from breaches in cybersecurity can cause significant harm. Imposing liability for the costs of credit monitoring will deter negligent data practices and facilitate prompt detection of the opening of unauthorized accounts.

In Texas, state records showed that prior to a massive breach of data security, "information technology departments shrank by 20 percent, saw high employee turnover and faced heavy productivity demands—sometimes at the expense of security."[242] Ultimately, a public outcry forced the responsible state agency to offer free credit monitoring to millions of persons.[243] Courts should consider whether a reduced investment in data security is "penny wise and pound foolish."

---

behaviour in many cases."). Some sources focusing on the United States offer high estimates of costs arising from breaches of data security. *See* Edward Murray, *Breaches*, POST MAG., Jan. 13, 2011, at 18, 18. According to the Ponemon Institute in Michigan:

> [E]ach compromised customer record costs companies a little over $200 . . . and includes outlays for detection, escalation, notification and response along with legal, investigative and administrative expenses, customer defections, opportunity loss and reputation management. . . . [and] costs associated with customer support such as information hotlines and credit monitoring subscriptions.

Id.; *see also* PONEMON INST., 2009 ANNUAL STUDY: COST OF A DATA BREACH 4-5 (2010), *available at* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf.

239 *See* Brian Azcona, *Transaction-Generated Data*, *in* ENCYCLOPEDIA OF PRIVACY 562, 564 (William G. Staples ed., 2007).

240 *See* Chandler, *supra* note 55, at 273 ("The recognition of potential liability in negligence might assist by forcing careless custodians of personal information to internalize the very real costs of their carelessness . . . .").

241 *In re* Paoli R.R. Yard PCB Litig., 916 F.2d 829, 852 (3d Cir. 1990).

242 Kelley Shannon, *Combs Staff Swamped Before Data Breach*, DALL. MORNING NEWS, May 14, 2011, at 1A.

243 Hart, *supra* note 92 (discussing the offer and surrounding circumstances).

B. *Efficient Allocation of Losses*

Efficient allocation of costs often can minimize the economic burdens associated with injury-producing products and practices, such as the losses associated with defective consumer goods.[244] One approach is to the shift the loss to the "cheapest cost avoider"[245] and, thereby, reduce the magnitude of the loss. Another, often complementary, approach is to distribute the loss among a broad class of persons, such as all those who benefit from the injury-producing product or practice, so that no one suffers the full weight of the loss and many persons each bear a minor share thereof.[246]

The concepts of loss-shifting[247] and loss-spreading[248] are sometimes controversial. Nevertheless, they have played an important role in the shaping of modern American tort law.[249] They could be equally significant re-

---

244 *See generally* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 134, 163-65 (1970) (discussing methods of allocating accident costs to reduce the total impact of accidents and injuries).

245 The concept of cheapest cost avoider (sometimes framed in the rubric of "least cost avoider") is an established feature of law-and-economics scholarship. *See, e.g.*, HENRY N. BUTLER & CHRISTOPHER R. DRAHOZAL, ECONOMIC ANALYSIS FOR LAWYERS 319 (2d ed. 2006). Judicial opinions occasionally discuss this topic. Thus, in a case dealing with liability for allegedly negligent marketing and distribution of handguns, a federal court in New York found that as "[a]s between a negligent handgun manufacturer and an injured bystander, the former must be regarded as the 'cheapest cost avoider.'" Hamilton v. Accu-Tek, 62 F. Supp. 2d 802, 827 (E.D.N.Y. 1999), *vacated sub. nom.* Hamilton v. Beretta U.S.A. Corp., 264 F.3d 21 (2d Cir. 2001). The cheapest cost avoider principle has been influential in the shaping of modern American tort doctrine. For example, it has been said that "[t]he product liability action for breach of warranty is an action in strict liability, not based on fault, allocating a risk of loss for policy reasons to the cheapest cost avoider." Schneider Nat'l, Inc. v. Holland Hitch Co., 843 P.2d 561, 580, 587 (Wyo. 1992). However, it was probably an overstatement for the Fifth Circuit to write that "[m]odern negligence principles are to a large extent designed to place liability on the party who is the cheapest cost avoider or cheapest insurer." Rankin v. City of Wichita Falls, Tex., 762 F.2d 444, 448 n.4 (5th Cir. 1985). Many factors have shaped modern American tort law, including, among others, fault, proportionality, deterrence, efficient loss allocation, administrative convenience, predictability, and respect for the actions of co-equal branches of government. *See* JOHNSON & GUNN, *supra* note 138, at 7-10 (discussing the policy foundations of tort law). However, in some tort cases, courts have held that the cheapest cost avoider principle is decisive. For example, the Ninth Circuit held in a public nuisance action "that the defendants are under a duty to commercial fisherman [sic] to conduct their drilling and production in a reasonably prudent manner so as to avoid the negligent diminution of aquatic life" because the defendants were "unmistakably . . . the best cost-avoider." Union Oil Co. v. Oppen, 501 F.2d 558, 569-70 (9th Cir. 1974) (extensively discussing the economic theories of Guido Calabresi).

246 *See* JOHNSON & GUNN, *supra* note 138, at 8 (discussing loss-spreading and the idea that those who benefit from activities should bear any losses that result).

247 *See id.* (discussing the idea that "[t]he costs of accidents should be shifted to those best able to bear them" and how this can minimize the economic burden of accidents (emphasis omitted)).

248 *See id.* (discussing the idea that "[t]he costs of accidents should be spread broadly" and noting that "[l]osses can be spread not only through increases in the costs of goods and services, but through other devices such as taxation and insurance" (first emphasis omitted)).

249 *Id.*

garding allocation of credit-monitoring costs that plaintiffs incur due to data-security breaches. By taking advantage of the economies of scale, it is reasonable to conclude that large data possessors, such as banks, universities, and national retailers can purchase credit-monitoring coverage for data subjects cheaper than those persons could purchase coverage for themselves.[250] Moreover, in many instances, the costs of credit monitoring can be spread to some or all of the persons who benefit from a data possessor's activities. This may reduce the magnitude of the burden that must be carried.

For example, if a data possessor has 100,000 customers, and information relating to one hundred of those customers is subject to unauthorized access, the costs of monitoring the credit of the one hundred affected data subjects can be spread among all of the data possessor's customers. The burden will not fall exclusively on those who happened to be among the unlucky one hundred. Thus, if the use of computerized information makes a business more effective or efficient, the costs related to such productivity will be spread among those who potentially benefit from that efficiency.

CONCLUSION

In recent years, expenditures on credit monitoring have become common. Today, it is often the case that potential cybersecurity defendants voluntarily provide such services to affected data subjects;[251] that courts approve settlements where compensation for credit monitoring is a large part of class-action recoveries;[252] and, that judicial and administrative sanctions order provision of credit monitoring or reimbursement for expenditures on such services.[253] These developments, all of which are relatively new, cloak expenditures on credit monitoring with the indicia of legitimacy[254] and provide compelling grounds for courts to consider, afresh, the issues relating to whether a negligent data possessor can be held liable for the costs of credit monitoring.

---

250 *See In re* Countrywide Fin. Corp. Customer Data Sec. Breach Litig., No. 3:08-MD-01998, 2009 WL 5184352, at *8, *11 (W.D. Ky. Dec. 22, 2009) (calculating the cost of two years of credit monitoring provided in-kind at $37); *Comparison of Credit Monitoring Services*, *supra* note 18 (showing that the cost of credit monitoring, when purchased by an individual, can range from $8.95 to $29.95 per month); *see also Learn Strategies for Managing Cyber Risk*, *supra* note 95, at 16 (stating that annual costs for credit monitoring offered by a data possessor in cases of security breach "can range from $20 to $100 per person").

251 *See supra* Part II.B.

252 *See supra* Part II.C.

253 *See supra* Part II.D.

254 *See supra* Part II.E.

Expenditures on credit monitoring are a reasonable and necessary response to any serious breach of data security,[255] and therefore, compensation for such amounts should normally be available. A persuasive analogy can be drawn between credit monitoring and the awards for medical monitoring that many states permit in cases of toxic exposure involving threats to personal health.[256] However, even in the absence of such precedent, ordinary tort principles provide justification for credit-monitoring awards as reasonably necessary expenditures intended to mitigate damages.

The so-called economic loss rule should not bar recovery of credit-monitoring damages because the data protection obligations imposed under state data-security laws are not a proper subject for bargaining between data possessors and data subjects.[257] Any agreements purporting to diminish the data-protection obligations imposed by relevant statutes[258] are likely to be void as against public policy. Likewise, the fact that identity theft may have not yet occurred is no reason for courts to deny the recovery of credit-monitoring expenditures.[259] Such an award is intended to compensate affected data subjects not for an increased risk of future harm,[260] but for the reasonable and necessary costs of minimizing the risks of identity theft through protective detection of the opening of unauthorized new accounts in the victim's name.[261] If negligence has factually and proximately caused a serious breach of cybersecurity, plaintiffs should recover those costs regardless of whether identity theft ever takes place.

Holding data possessors responsible for credit-monitoring costs will further the deterrence interests of the law by forcing data possessors to implement reasonable precautions and avoid unnecessarily risky practices.[262] Moreover, placing the cost of credit monitoring on data possessors will, at least in the case of businesses, often shift the costs of credit monitoring to the cheapest cost avoider and, typically, spread the costs of data use to a broad class of persons will who benefit from the businesses' activities.[263]

Consequently, in a wide range of circumstances, recovery of credit-monitoring damages is appropriate. Compensation for such expenditures is consistent with sound community practices, basic legal principles, and the important public policies relating to deterrence and efficient loss allocation.

---

255 *See supra* Parts III.A-B.

256 *See supra* Part III.

257 *See supra* Part I.C.2.

258 *See supra* Part I.C.1.

259 *See supra* Part IV.A.

260 *See supra* Part IV.A.2.

261 *See supra* Part IV.A.1.

262 *See supra* Part V.A.

263 *See supra* Part V.B.