Credit Monitoring Damages in Cybersecurity Tort Litigation

Vincent R. Johnson
Credit Monitoring Damages in Cybersecurity Tort Litigation

Vincent R. Johnson*

Feb 23, 2011
Credit Monitor Rev.48.wpd

I. Uncertain Compensability
   A. Issue of Widespread Importance
   B. Tort Claims Related to Cybersecurity
   C. Starting Assumptions
      1. Duty to Protect and Disclose Breaches
      2. Not Barred by the Economic Loss Rule
      D. Precedent, Developments, and Arguments

II. Court Decisions and Business Practices
    A. Adverse Decisions
    B. Voluntary Offers of Credit Monitoring
    C. Class Action Settlements
    D. Judicial and Administrative Sanctions
    E. Indicia of Legitimacy

III. Analogy to Medical Monitoring Damages
     A. Exposure Threshold for Recovery
     B. Reasonably Necessary
     C. Duration of Monitoring

IV. Arguments Against Recovery
    A. Present Injury Versus Increased Risk of Harm
       1. Two Categories of Harm
       2. Contrast to Loss of a Chance
       3. Differentiating Damages from Standing
          B. Self-Protection Against This Type of Loss
             1. Not a Proper Subject for Bargaining
             2. Collateral Sources and Causation Principles
V. The Case for Credit Monitoring Damages  40
   A. Deterrence of Deficient Data Practices  41
      1. Precautions and Activity Levels  42
      2. Internalization of Costs  43
         B. Efficient Allocation of Losses  44

VI. Conclusion  46
I. Uncertain Compensability

When computerized personal information is improperly accessed or disclosed, the persons to whom that information pertains are often at an increased risk of identity theft. 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. 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. As a result, the victim of a data security breach can take prompt action to minimize the consequences of identity theft and perhaps avoid financial ruin. Remedial steps may include closing an unauthorized account, placing a fraud alert in credit reporting agency 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.

Credit monitoring will not detect the unauthorized use of existing
accounts or types of data misuse unrelated to credit,\textsuperscript{4} such as fraudulent presentation of credentials to obtain employment or medical care.\textsuperscript{5} 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.

A. Issue of Widespread Importance
Basic credit monitoring is not expensive,\textsuperscript{6} at least when only one
EXPERTS AND THE DUTY TO REPORT MISCONDUCT

individual is concerned. However, breaches of database security (sometimes called “cybersecurity”) occur frequently and often affect thousands, or even millions, of persons. This is especially true in cases of unauthorized intrusion into the data held by credit card issuers, mortgage lenders, student-loan lenders, universities, banks, and large employers. In such instances, credit monitoring expenditures can run into the millions of dollars. 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. On the other hand, plaintiffs in cybersecurity cases often argue that defendants are responsible for such amounts and other expenses as well.\textsuperscript{19}

Whether the costs of credit monitoring are recoverable in tort actions is important for a variety of reasons, including whether qualified counsel are willing to represent affected persons in class action litigation. It is usually difficult for at-risk data subjects to prove that defendants are responsible for losses such as emotional distress\textsuperscript{20} or increased risks of future harm.\textsuperscript{21}
And, until identity theft occurs, other types of damage resulting from data exposure may be modest in amount. 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 involving a creditor's making of an erroneous report to credit reporting agencies or a credit reporting agency's selling of a credit
report to a third person without a “permissible purpose.” Compensation for the costs of credit monitoring is also sometimes sought under non-tort theories of liability. Moreover, some judicial opinions use the phrase “credit monitoring” in ways that have nothing to do with tracking the credit of individuals or are unrelated to recovery of damages for such services.

This article is concerned with the compensability of the costs of credit monitoring only in tort cases involving cybersecurity issues. This range of conduct includes failing to protect data from unauthorized access;
negligently\textsuperscript{28} or intentionally\textsuperscript{29} disclosing or transferring personal information (such as via postings on the Internet, e-mail correspondence, or attachments to court filings\textsuperscript{30}); 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

For purposes of this article, it is assumed \textit{arguendo} that there is a \textit{duty on}
the part of a data possessor to protect the personal information of others from unauthorized access or revelation and to disclose to affected data subjects information about a known breach of data security. These duties are rooted in common law principles; in the terms of, or public policies reflected in, the security breach notification laws and other provisions that have been passed by numerous states; and in various other pieces of state and federal legislation that impose particular data security obligations. Courts have enforced these duties in recent cases, although there is authority to the contrary.
In Shames-Yeakel v. Citizens Financial Bank, 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." The court held that bank customers, who became victims of identity theft when an unknown person gained access to their online accounts and stole thousands of dollars, stated a negligence claim against a bank which employed only a single-password form of account protection.
Numerous commentators are in agreement that there is a duty to prevent improper access or revelation of personal information and to disclose knowledge of security breaches.\textsuperscript{40} Of course, absent proof of duty, a negligence claim will fail. In that case, unless there is some other theory of liability, the question of what damages may be recovered in a cybersecurity action need not be reached.

2. **Not Barred by the Economic Loss Rule**

This article also assumes *arguendo* that recovery of credit monitoring
losses is not barred by the so-called “economic loss rule.” That rule—if it is a rule—is a principle of uncertain dimensions which holds that, at least in some circumstances, negligence which causes purely economic losses, without also producing personal injury or property damage, is not actionable in tort. The elegant simplicity of the “rule” masks a messier reality because the “rule” is subject to a multitude of well-recognized exceptions. Not the least of these qualifications are the causes of action imposing liability for misrepresentation, defamation, professional malpractice, breach of fiduciary duty, nuisance, loss of consortium, wrongful death, and
spoliation of evidence, all of which may afford recovery for negligence causing purely economic losses to the plaintiff.\textsuperscript{43}

In large measure, the economic loss rule is intended to further the private ordering of business transactions.\textsuperscript{44} However, data security statutes in 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.\textsuperscript{45} 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 which have been explored elsewhere, recovery of credit monitoring damages should not be foreclosed by the economic loss rule. However, in one recent case, Paul v. Providence Health System-Oregon, an Oregon appellate court held that patients could not recover, under a negligence theory, purely economic damages related to credit monitoring which they incurred in protecting against the increased risk of identity theft caused by the theft of unencrypted patient records from the car of the defendant’s employee.
D. Precedent, Developments, and Arguments

Part II of this article discusses precedent dealing with credit monitoring damages, as well as 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, including alleged lack of present injury.
in cases where identity theft has not occurred and the plaintiff's ability to self-protect against harm that can be avoided by credit monitoring. Part V then explains why courts should allow victims of data security breaches to recover compensation for the costs of credit monitoring. In particular, 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, those businesses are well-situated to efficiently spread identity theft prevention costs among those who benefit from the use of
computerized personal information. Part VI concludes that the costs of credit monitoring should often be recoverable in cybersecurity litigation.

II. Court Decisions and Business Practices
   A. Adverse Decisions
      Although some courts have ordered defendants to provide credit monitoring services\textsuperscript{49} or pay credit monitoring damages,\textsuperscript{50} a number of cases have held that credit monitoring damages are not recoverable in
cybersecurity tort actions. 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 such expenditures are not compensable.

The decisions adverse to recovery of compensation for credit monitoring expenses generally fall into three categories. First, some cases have rejected the efforts of plaintiffs to analogize credit monitoring to medical monitoring. 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. Data exposure and toxic exposure are analogous in that they both create a need for early detection of potentially emerging threatened harm. Issues related to the analogy between medical monitoring and credit monitoring are explored in Part III of this article.

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. The fallacy of this objection is discussed in Part IV-A of this article.53
Finally, the third group of cases has declined to award credit monitoring damages because the plaintiffs lacked standing to litigate that issue in federal court.54 Issues related to standing are considered in Part IV-A-3 of this article.

**B. Voluntary Offers of Credit Monitoring**

Rather than definitively resolving issues relating to credit monitoring costs, decisions denying recovery have been called into question by recent developments. The first of these occurrences relates to business practices.
Recognizing the appropriateness of expenditures on credit monitoring,\textsuperscript{55} database possessors potentially responsible for unauthorized access to data often voluntarily offer to pay the costs of monitoring the credit of affected persons for a period of time.\textsuperscript{56} Thus, when Wyndham Hotels and Resorts learned that a sophisticated hacker penetrated its computer system and may have used customer information to perpetrate fraudulent transactions, it provided affected customers, at no cost, with credit monitoring for one year.\textsuperscript{57} 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.\textsuperscript{58}

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.\textsuperscript{59} Comparable offers have been voluntarily made by the University of Louisville,\textsuperscript{60} Harley- Davidson,\textsuperscript{61} the St. Louis Metropolitan Police
Department, Tulane University, the Bank of New York Mellon, Ohio State University, Holy Cross Hospital (Ft. Lauderdale), Wachovia Securities, and other potential defendants. Thus, 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.” 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.69

C. Class Action Settlements

Many courts have also recently approved class action settlements in cybersecurity cases where portions of the settlements were intended to cover the costs of credit monitoring.70 Indeed, when aggregate claims are settled, 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 driver's licenses.71
For example, in *In re TJX Companies Retail Securities Breach Litigation*, a federal court in Massachusetts approved an award of $6.5 million in fees to attorneys who represented a class in litigation arising from the theft of personal information relating to 40 million credit cardholders. In that suit, which was then the “largest retail security breach in history,” 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 comfortable characterizing this litigation as creating $177,000,000 in potential benefits for the class . . . .74 Similarly, in In re Countrywide Financial Corp. Customer Data Security Breach Litig.,75 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.”76 Likewise, in Barel v. Bank of America,77 a federal court in Pennsylvania approved a class action settlement which provided non-customers, whose credit reports had been
improperly accessed by the defendant, with four months of credit monitoring and other relief. 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, federal law authorizes the secretary of the Department of Veterans Affairs, in cases of data security breaches, 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.”78 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.”

In another government data security breach, an FDIC intern improperly used agency information to take out fraudulent loans in the names of FDIC employees. The agency reacted by “promptly notifying affected
employees and offering them 2 years of credit monitoring services."81

D. Judicial and Administrative Sanctions

The appropriateness of expenditures on credit monitoring is also evidenced by the fact that courts and administrative agencies have imposed sanctions requiring provision of such services to persons placed at risk of identity theft by breaches of data security. In one recent case, a federal court in Massachusetts ordered a detainee convicted of hacking into a prison's
computer system to pay restitution. The award reimbursed the county for money that it spent for the credit monitoring services that it offered to employees whose personal information was contained in the databases that were hacked.

In another case, *Allstate Ins. Co. v. Linea Latina De Accidentes, Inc.*, 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.” 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.”85

In Connecticut, the state insurance commission fined a health insurer for a major data security breach and untimely notification of affected persons. The fine was part of an agreement requiring the insurer to provide two years of free credit monitoring to insureds.86
E. Indicia of Legitimacy

These developments relating to business practices, litigation settlements, and judicial and administrative sanctions, as well as references in court opinions reflecting the utility of credit monitoring, strongly suggest that expenditures on credit monitoring are a prudent and appropriate response when computerized personal information is placed at risk. To that extent, such amounts should be recoverable 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 which approve expenditures on credit monitoring.

Moreover, to the extent that provision of credit monitoring services is a
customary business practice in cases of breached data security, legal
recognition of a duty to provide such compensation is more easily justified.
88 In such an environment, imposition of liability for credit monitoring
damages will neither disrupt community practices nor impose
unprecedented obligations. This is important because among the policy
considerations typically deemed relevant to whether a duty should be imposed are the resulting “consequences to the community.”

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.” Moreover, the rule that damages must be proven 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.\textsuperscript{91} Consistent with these principles, many states permit toxic exposure plaintiffs to recover the costs of medical monitoring.\textsuperscript{92} "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."\textsuperscript{93}

For example, in \textit{Meyer ex rel. Coplin v. Fluor Corporation},\textsuperscript{94} the Supreme Court of Missouri, \textit{en banc}, so held. The \textit{Meyer} court, discussing
an earlier decision of the Missouri Court of Appeals, *Elam v. Alcolac, Inc.*, 95 stated:

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. . . . 96

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.97

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 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.98

A. Exposure Threshold for Recovery
Medical monitoring damages are not recoverable in cases of insignificant exposure to toxic chemicals. Similarly, credit monitoring damages should
not be awarded if there has been only a trivial breach of data security. The relevant Latin maxim is *de minimis non curat lex*, a phrase which reflects a principle that applies broadly throughout American jurisprudence. “The law does not concern itself with trifles.” 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. Instead, a plaintiff ordinarily must demonstrate a significant injury to his or her personal interests before the law will grant a remedy. Merely technical interference with another's rights is normally overlooked by the courts.
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. A plaintiff who does not otherwise suffer actual losses as the result of a data security breach should be permitted to recover the costs of credit monitoring only if there has been a sufficiently serious exposure of the plaintiff’s personal data to the risk of identity theft that a reasonably prudent person would incur the costs of credit monitoring. Presumably, whether the threshold for recovery has been crossed will be a function of 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. 101

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 made to obtain data. 102
In contrast, the latter category encompasses such things as loss of computers, hardware, or media containing data, unintentional exposure of data on the Internet, and improper disposal of data. 103

In some cases, the seriousness of data exposure will be established by proof that a cybersecurity breach was the result of hostile action. Thus, if a laptop containing social security numbers is stolen, 104 it is easier to conclude that affected data subjects are at an increased risk of identity theft, than if the laptop was merely lost or misplaced. 105 The same may be true if
there is evidence that an unauthorized person opened a new bank account using the social security number of one of the affected data subjects soon after the security breach occurred,\textsuperscript{106} or if a renegade employee with access to thousands of patient files actually sold some of that information to an identity theft ring.\textsuperscript{107} In contrast, if a server containing customers' information is only one of many items of hardware that are taken by thieves, 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 exposure
Similarly, the appropriateness of credit monitoring may be a factor of the period of time for which data was exposed to wrongful access by third persons and the ease with which access could be achieved. If personal information is negligently posted on the Internet or in some other public location for a period of months, there is a greater basis for concluding that data subjects are at heightened risk of identity theft than if the information was accessible for only six days under circumstances where there is no evidence that the personal information was actually accessed or
misused. The same is true if personal information is freely accessible on the web as opposed to password-protected and available only by login.

Finally, in some cases, it may be appropriate to take into account the nature of personal information at issue in determining whether credit monitoring is warranted. 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 names and e-mail addresses.

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 sensitive personal information was actually misused. 113

In *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*114 a federal court
in New York dismissed a negligence claim seeking credit monitoring damages because the plaintiff failed to demonstrate a rational basis for serious concern about the personal information contained on password-protected laptops that were stolen from a pension consultant's office. 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. 115
B. Reasonably Necessary

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

While it is important to consider whether expenditures on credit monitoring 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 yield convincing results. Calculations often unreasonably discount or ignore very real considerations, such as the emotional distress, inconvenience, and lost time that result from breaches of
data security. Whether expenditures on credit monitoring are cost-effective is better assessed by reference to what businesses, courts, and governmental agencies actually do than by judicial calculations seeking to quantify the wisdom of credit monitoring.

In *Stollenwerk v. Tri-West Health Care Alliance*,120 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 placed a fraud alert in their files. However, a once-a-year free credit report121 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.” 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. There is now abundant evidence showing that businesses, courts, and government agencies often authorize expenditures on credit monitoring, even though affected data subjects could obtain a free credit report each year from a credit-reporting agency and place a fraud alert 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. Consideration must be given to the toxicity of the chemical or other matter at issue, the length of the plaintiff's exposure, and the foreseeable period during which resulting symptoms of disease or injury may be latent. 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. There is no binding rule. In some cases, the one or two years of credit monitoring that is offered by a potential defendant may be all that is warranted.\textsuperscript{127} In other cases, it may be reasonable to continue monitoring for a longer period of time. Little more
can be said than that, whatever the period, the plaintiff must prove that the monitoring for that length of time is reasonably necessary. Of course, claims seeking compensation in the form of lifetime monitoring are likely to be greeted with skepticism, except in the rarest case.

IV. Arguments Against Recovery

A. Present Injury Versus Increased Risk of Harm

A number of cases have held that credit monitoring damages are not
recoverable because, until identity theft occurs, a data subject affected by a cybersecurity breach has not suffered an injury. For example, in Rowe v. UniCare Life and Health Ins. Co., the plaintiff sought to recover credit monitoring costs and other damages in a case arising from the temporary posting of personal information on the Internet. 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. 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 calculate 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.132 This line of reasoning misses the point. In cases of breached data security, the costs of credit monitoring must reasonably be incurred 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 the personal data placed at risk is ultimately misused. 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 which are reasonably incurred to prevent identity theft when data security is seriously breached and, second, costs resulting from identity theft. Expenses falling within the first category include the costs of credit monitoring and such 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, these types of expenses should be incurred 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 might be avoided by the exercise of reasonable care, but to redress harm proximately caused. If such losses have accrued prior to trial, or if it can be proven with reasonable certainty that they will occur in the future, they should be recoverable. However, such evidence is often unavailable because the risk of identity theft has not yet come to fruition. In that case, compensation for
damages relating to the second category should be denied 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. There is no reason to follow a different rule in cybersecurity cases.

Courts should focus on the two specified categories of damage (costs incurred to prevent harm and costs resulting from identity theft) and reject 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”[134]) which 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, such as 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. Courts award increased-risk-of-harm damages because generally accepted scientific principles have made it possible to calculate percentage increases in the chance of harm with reasonable precision.\textsuperscript{135} For example, in \textit{Matsuyama v. Birnbaum},\textsuperscript{136} the Supreme Judicial Court of Massachusetts recognized the loss of a 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."\textsuperscript{137} 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." . . . . Survival 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. For 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, 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.
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: "Our 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." 139

In contrast to the field of medical services, there are no established scientific principles which can quantify increased risk of identity theft in cybersecurity cases. Consequently, it is inappropriate for courts to hold that
compensation in such cases is based on increased risk of harm. Rather, damages should be awarded only for losses which can be proved with reasonable certainty. In many cases, the costs of credit monitoring, 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 exposure, or failure to promptly disclose that security has been breached. In some cases, it is also possible to establish with reasonable certainty losses that have occurred as a result of identity theft linked to unprotected personal data. However, damages should not be
awarded 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 necessitates proof of injury in fact. As explained in *Lujan v. Defenders of Wildlife*:

[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.” . . . \textsuperscript{142}

In federal cybersecurity litigation, courts have addressed the Constitutional standing requirement. Thus, in \textit{Pisciotta v. Old National Bancorp},\textsuperscript{143} 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.\textsuperscript{144}

Cases decided subsequent to Pisciotta have generally reached the same
EXPERTS AND THE DUTY TO REPORT MISCONDUCT

conclusion, 145 although there is authority to the contrary. 146 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. Saying that an increased risk of identity theft does (or does not) give one standing to assert a cybersecurity claim should neither depend on whether damages for increased risk of harm are recoverable under state law, nor mean that credit monitoring expenditures are not a compensable form of loss resulting from a security breach. 147 Moreover, not all cybersecurity cases are litigated in federal court. To that extent, federal court
precedent on standing is unlikely to present a useful guide to resolving 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 drafts produced by the project were ever approved. 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. Thus, in assessing the compensability of credit monitoring damages, it is fair to ask whether recovery for this form of loss should be barred by the fact that, before the cybersecurity breach occurred, the plaintiff could have bargained with the defendant about what damages could be recovered in the case of breach. In addition, there is a separate, but related, question about whether a potential plaintiff’s ability to self-protect against unauthorized use of personal information by purchasing credit monitoring services before a breach occurs somehow forecloses recovery of the costs of such services in a cybersecurity
tort action.

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 causing 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." However, by the time of the second Council draft in October 2007, that same provision had been revised to insert the word "reasonably." 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.”151 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 bar recovery in tort 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” 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 breach disclosure obligations
they impose are not a proper subject for bargaining between data possessors and data subjects.\textsuperscript{153} Agreements which vary those duties are normally void as against public policy.

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, 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. Consumers 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.\(^\text{154}\)

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. 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 fund raising. 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 the security of
those records is breached.

2. **Collateral Sources and Causation Principles**

Theoretically, it might be argued that credit monitoring damages should not be recoverable because potential plaintiffs could obtain credit monitoring insurance for themselves prior to any unauthorized intrusion into or revelation of their data. This issue was spotted, but not explored, by a federal court in Michigan. In denying recovery of credit monitoring damages under breach of contract and deceptive trade practices theories, the
court observed that “perhaps it would be prudent for everyone to monitor their credit.”

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,\textsuperscript{156} which is still widely followed outside of the medical malpractice context,\textsuperscript{157} holds that the fact that the plaintiff has insurance does not
reduce the defendant’s liability. 158 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, 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. 159 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. 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 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.161 The second concerns efficient allocation of the economic losses that inevitably arise from the widespread use of computerized 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 with regard to other putative defendants, and as true concerning losses resulting from inadequate data security as 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 could have been avoided.

At various times, courts have imposed liability for the purpose of deterring negligent data practices. For example, in *Remsburg v. Docusearch*,
Inc., a man purchased from an Internet-based investigation service information about a woman's workplace address, then went to that location and killed her. 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. The decision was intended to deter the type of careless data-related practices that create risks of stalking and identity theft.
Similarly, in *Wolfe v. MBNA America Bank*, 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.” 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.\textsuperscript{166}

1. Precautions and Activity Levels

Subjecting potential defendants to liability for the losses 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.”167

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.

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 which 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. Or it may decide that outdated files containing personal information should be purged, rather than retained.

2. Internalization of Costs

In some instances, deterrence is achieved by compelling potential defendants to internalize the costs of their endeavors. In other words, liability is used to reconcile burdens with benefits. 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, in many instances, employers are held liable for the torts of employees occurring within the scope of employment;\textsuperscript{169} possessors of animals, for bites and other attacks;\textsuperscript{170} and contractors, for damage resulting from the use of dynamite in excavation.\textsuperscript{171}

However, as presently configured, American law often allows data
possessors to escape responsibility for the losses resulting from their negligent data practices. Yet, data possessors frequently reap the benefits of assembling, preserving, and using computerized personal information. Imposing liability for credit monitoring damages will help to ensure that data possessors will internalize the costs incidental to their practices and therefore engage in an honest calculation of whether those practices are worthwhile and carried on in a way that reasonably minimizes the risk of losses associated with breaches of cybersecurity.

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. . . . 174
The same analysis applies to recovery of credit monitoring damages in a
digital age where significant harm can be done by delayed detection of
identity theft arising from breaches in cybersecurity. Imposing liability for
the costs of credit monitoring will deter negligent data practices and
facilitate prompt detection of the opening of unauthorized accounts.

B. Efficient Allocation of Losses
The costs associated with injury-producing products and practices, such
as the losses associated with defective consumer goods, can often be
minimized by efficient allocation of those costs. One approach is to shift the loss to the “cheapest cost avoider” 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.

The concepts of loss-shifting and loss-spreading are sometimes controversial. Nevertheless, they have played an important role in the shaping of modern American tort law. They could be equally significant...
with respect to allocation of the costs of credit monitoring that are incurred as a result of 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. 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 100 of those customers is subject to unauthorized access, the costs of monitoring the credit of the 100 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.

VI. 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; that courts approve settlements where compensation for credit monitoring is a large part of class action recoveries; and that judicial and administrative sanctions order provision of credit monitoring or reimbursement for expenditures on such services. These developments, all of which are relatively new, cloak expenditures on credit monitoring with the indicia of
legitimacy\textsuperscript{182} 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.

Because expenditures on credit monitoring are a reasonable and necessary response to any serious breach of data security,\textsuperscript{183} compensation for such amounts should normally be available. An analogy can persuasively be drawn to the awards for medical monitoring that many states permit in cases of toxic exposure involving threats to personal health.\textsuperscript{184} However,
even in the absence of such precedent, awards for credit monitoring can be justified under ordinary tort principles as reasonably necessary expenditures intended to mitigate damages.

Recovery of credit monitoring damages should not be barred by the so-called economic loss rule because the data protection obligations imposed under state data security laws are not a proper subject for bargaining between data possessors and data subjects. Any agreement purporting to diminish the data protection obligations imposed by relevant statutes are likely to be void as against public policy. Nor does the fact that identity theft
may have not yet occurred provide a reason for denying recovery of expenditures on credit monitoring. Such an award is intended to compensate affected data subjects not for an increased risk of future harm, but for the reasonable and necessary costs of minimizing the risks of identity theft through protect detection of the opening of unauthorized new accounts in the victim's name. If negligence has factually and proximately caused a serious breach of cybersecurity, those costs should be recoverable regardless of whether identity theft ever takes place.
Holding data possessors responsible for the cost of credit monitoring will further the deterrence interests of the law by forcing data possessors to implement reasonable precautions and avoid unnecessarily risky practices. 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 who benefit from the businesses activities. 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.

1 See generally Vincent R. Johnson, Cybersecurity, Identity Theft, and the
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 and Health Ins. Co., 2010 WL 86391, *5 (N.D. Ill. 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”).

which "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").

an identity theft passport that proves to creditors and law enforcement officers that someone has used a victim’s identity to commit fraud”); Daniel J. Penofsky, *Litigating Identity Theft Cases*, 112 Am. Jur. Trials 1 § 19 (2009) (discussing specific steps a lawyer should take in representing a victim of credit monitoring).

4 *See* Graves, *supra* note 3, at 70 (point stated).

5 *See id.* at 53 (distinguishing between “new account fraud, existing account fraud, and non-financial fraud”).

6 *But see* David Lazarus, *Spend the $15 a Month on Debts, Not on an Online Debt Organizer*, L.A. Times, Jan. 25, 2011, at 1, 2011 WLNR 1494933 (opining that
if your problem is that you owe businesses too much money . . . you can probably live without daily credit monitoring”).

7 Experian’s “Triple Alert” credit monitoring service, which sells for $4.95 per month, bills itself as the “most affordable credit monitoring product on the market.” See https://www.experiandirect.com/triplealert/default.aspx (last visited March 20, 2010). 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. The Experian Guarantee guarantees the ‘Triple Advantage’

See also Monitoring Your Credit’s Health, Winnipeg Free Press B4, Jan. 7, 2011, 2011 WLNR 384898 (placing the cost of credit monitoring at $15 per month, which includes identity theft insurance); Daniel Wolfe, Regions Offers $5 Anti-Fraud Services, Am. Banker, Jan. 28, 2011, at 10, 2011 WLNR 1715556 (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, 2009 WL 2927950, *2 (Bkrcty. D.S.C.) (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”).

8 Two sites compile up-to-date lists of security breaches: Privacy Rights Clearinghouse, Chronology of Data Breaches, at http://www.privacyrights.org/data-breach (last visited Feb. 15, 2011) and Identity Theft Resource Center, Data Breaches, at

9 See Paul v. Providence Health System-Oregon, 237 Or. App. 584, 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-Madison Warns 60,000 of Card Data Theft, Wis. State Journal, Dec. 10, 2010 (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).

10 See also 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 to almost all of . . . Google's web services”)


13 See In re Countrywide Financial Corp. Customer Data Sec. Breach Litig.,
EXPERTS AND THE DUTY TO REPORT MISCONDUCT

2009 WL 5184352, *9 (W.D. Ky.) (discussing a data security breach that affected more than 10 million persons).

14 See Steve Karnowski, Student Loan Company: Data on 3.3M People Stolen, www.sfgate.com, Mar. 26, 2010 (indicating that the stolen data of more than three million borrowers, located on “portable media,” included names, addresses, Social Security numbers and dates of birth).

15 See, e.g., Derby, supra note 9 (discussing the University of Wisconsin at Madison).

(S.D.N.Y.) (discussing the loss of computer back-up tapes allegedly containing information relating to 12.5 million individuals).

17 See Krottner v. Starbucks Corp., 2010 WL 5141255 (9th Cir.) (involving the unencrypted data of 97,000 employees).

18 See, e.g., In re Countrywide Financial Corp. Customer Data Security Breach Litig., 2010 WL 3341200, *9 (W.D. Ky.) (placing the cost of credit monitoring in a class action at “$37 per person,” or $7 million). See also Andreas M. Antonopoulos, More Censorship, Data Breaches and Devices: Security Predictions for 2011, Network World Dec. 16, 2019, at 16, 2010 WLNR 25089362 (asserting that “just 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”).

19 For example, in Saenz v. Kaiser Permanente Intern., 2010 WL 668038, *2 (N.D. Cal. 2010), 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.”


21 But see Rowe v. UniCare Life and Health Ins. Co., 2010 WL 86391, *6 (N.D. Ill. 2010) (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”).

23 See, e.g., *Wang v. Asset Acceptance, LLC*, 680 F. Supp. 2d 1122, 124 (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 enforcement of the debts was barred by applicable statutes of limitations, the plaintiff sought compensation for "forced purchase of credit reports and creditor monitoring," as well as other expenses).

24 See, e.g., *Daniels v. Experian Information Solutions, Inc.*, 2010 WL 331690 (S.D. Ga. 2010) (recounting that the plaintiff demanded "free credit monitoring for one year").
25 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”).


See, e.g., Rowe v. UniCare Life and Health Ins. Co., 2010 WL 86391, *1 (N.D. Ill. 2010) (involving a variety of claims brought by insurance plan members whose personal information was temporarily accessible to the public on the Internet).
29 See 1-800-East West Mortgage Co., Inc. v. Bournazian, 2010 WL 3038962, *1–*3 (Mass. Super.) (awarding, in an action alleging conversion, breach of contract, and breach of loyalty, credit monitoring damages against a former employee who improperly took and then unlawfully deleted highly confidential personal information of 68 employees).

30 See, e.g., In re Maple, 2010 WL 2950341, *2, *13 (Bkrtcy. E.D. Va.) (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).
31 See Cybersecurity, 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 (D. Colo. 2010) (finding that the plaintiff failed to properly allege actions for invasion of privacy or negligent infliction of emotional distress).

Cybersecurity, 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's list of state laws requiring notice of security breaches can be found at: http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (stating that “[f]orty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information”) (last visited Feb. 15, 2011). The Conference's year-by-year list of


34 See Gina Stevens, Cong. Research Serv., RL 34120, 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).

See generally Lazzarotti, supra note 8, 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 State L. Rev. 1, 4 (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 In re Davis, 430 B.R. 902, 908 (D. Colo. 2010) (holding that Gramm-Leach-Bliley does not create a private right of action); In re Matthey, 2010
WL 2176086, *2 (Bkrtcy. S.D. Ind. 2010) (similar) see also Cybersecurity, supra note 1, at 266-70 (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. Pro. R.5.2(a) (Westlaw 2011). Exceptions to the general rule on redacted filings are set forth in a different subsection. See id. 5.2(b).

35 See Allstate Ins. Co. v. Linea Latina De Accidentes, Inc., 2010 WL 5014386,
EXPERTS AND THE DUTY TO REPORT MISCONDUCT

3038962, *1-*3 (Mass. Super.) (holding a former employee liable for credit monitoring and other damages in a case arising from the improper removal of confidential employee information).


But see In re Countrywide Financial Corp. Customer Data Security Breach Litig., 2010 WL 3341200, *6 (W.D. Ky.) (opining that “the current state of the law
in regards to data breaches does not bode well for Plaintiffs . . . [and] this factor weighs heavily in favor of settlement”).

36 See, e.g., Cf. Krottner v. Starbucks Corp., 2010 WL 5185487, *1 (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., 2010 WL 2643307, *9 (S.D.N.Y.) (finding that no duty was owed to millions of persons whose personal information was contained on computer back-up tapes that were lost).

EXPERTS AND THE DUTY TO REPORT MISCONDUCT

38 Id. at *10.
39 Id. at *11.

40 See, e.g., Bill Piatt & Paula DeWitt, Loose Lips Sink Attorney-Client Ships: Unintended Technological Disclosure of Confidential Communications, 39 St. Mary’s L.J. 781, 815 (2008) (stating that “[a]ttorneys have an ethical obligation . . . to protect data stored electronically from unintended disclosure either through 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”); 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 (2006) (indicating that, “[l]ike legislatures, courts are signaling some willingness to impose a common law duty of care to protect personal information”).


41 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.


43 Boundary-Line Function, supra note 12, at 530-32 (containing abundant citations to primary authority).

44 See Flagstaff Affordable Housing Ltd. Partnership v. Design Alliance, Inc., 223 P.3d 664, 671(Ariz. 2010) (stating that “[t]he 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

45 See Cybersecurity, 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.

46 See Cybersecurity, supra note 1, 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).

47 But see Krottner v. Starbucks Corp., 2010 WL 5185487, *2 (9th Cir. 2010) (finding it unnecessary to determine whether an award of credit monitoring damages was barred by the economic loss rule because failed sufficiently to allege their negligence and breach of contract claims).


increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy).

*Pisciotta v. Old National Bancorp*, 499 F.3d 629, 635-39 (7th Cir. 2007), held that credit monitoring costs were not compensable under Indiana law. However, *Pisciotta* was a narrow decision. As described by another court in a later case, “after 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 and Health Ins. Co.*, 2010 WL 86391, *7 (N.D. Ill. 2010).
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, 2010 WL 724703, *4 (Bkrtcy. N.D. W. Va.) (dicta).

See also In re Killian, 2009 WL 2927950 (Bkrtcy. D.S.C.). Killian was not the typical cybersecurity case. The defendant was not charged 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.

54 *See, e.g.*, Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307, *7* (S.D.N.Y.) (holding that the plaintiff lacked standing because “their claims are future-oriented, hypothetical, and conjectural”).
55 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 Companies Retail Securities Breach Litig., 584 F. Supp. 2d 395, 406 (D. Mass. 2008), the court noted that only about three percent of eligible persons claimed the credit monitoring benefit that was part of a database intrusion settlement.

56 See, e.g., Rowe v. UniCare Life and Health Ins. Co., 2010 WL 86391, *1 (N.D. Ill. 2010) (stating that the defendants responsible for making personal information temporarily available on the Internet “offered to provide one year of
In *Taylor v. Countrywide Home Loans*, 2010 WL 750215 (E.D. Mich. 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 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 In re TJX Companies Retail Securities Breach Litig.*, 584 F. Supp. 2d 395, 400 (D. Mass. 2008) (discussing a settlement which provided affected customers with three years of credit monitoring); *Krottner v. Starbucks Corp.*, 2010 WL 5141255, *1* (9th Cir.) (indicating that one year of credit monitoring was offered to 97,000 employees by the theft of a laptop with unencrypted personal information).

57 Letter to author from Wyndham Hotels and Resorts dated June 2010, at pages 1-2 (on file with author). *See also Saenz v. Kaiser Permanente Intern.*, 2010 WL 668038, *2* (N.D. Cal. 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 the offer was inadequate).

58 See In re Countrywide Financial Corp. Customer Data Sec. Breach Litig., 2009 WL 5184352, *8 (W.D. Ky.) (discussing the offer, which some class members accepted, and the subsequent settlement which the court preliminarily approved). "Approximately 20% of the 2.4 million [persons initially contacted] accepted Countrywide's first offer of free credit monitoring." Id. at 11.

59 Karnowski, supra note 14. 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." \textit{Id.}

60 \textit{See Kitley, supra} note 5, at *43 (discussing a university's disclosure in June 2010 that patient information was posted on the Internet for 20 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”).

61 \textit{See Shafran v. Harley-Davidson, Inc.}, 2008 WL 763177, *1 (S.D.N.Y. 2008) (indicating that one year of free credit monitoring was provided to thousands of persons who personal information was contained on a lost laptop).
62 See Kitley, supra note 5, at *44-45 (indicating that after the department was the victim of a cyberattack in 2010, which was facilitated by an employee’s opening of e-mail, the “department said it would work to contact the affected parties and would pay to monitor their credit for a year”).

63 See John Pope, Tulane Payroll Information Stolen Laptop Had Social Security Numbers, Times-Picayune, Jan. 8, 2011, 2011 WLNR 443080 (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 . . . a year’s free credit monitoring of their accounts”).

65 See Encarnacion Pyle, Server Hacked at OSU: 760,000 Affected, Columbus Dispatch (Ohio), Dec. 16, 2010, at 1A, 2010 WLNR 24862133 (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 free credit-monitoring services as a precaution).
Former Holy Cross Hospital Employee Pleads Guilty to Id Theft, Faces up to 10 Years in Prison, S. Fla Sun-Sentinel, Jan 27, 2011 at 3B, 2011 WLNR 1761028 (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).

See Giordano v. Wachovia Securities, LLC, 2006 WL 2177036, *1 (D.N.J. 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).

155


70 See In re Countrywide Financial Corp. Customer Data Sec. Breach Litig., 2009 WL 5184352, *8 (W.D. Ky.) (approving a settlement encompassing credit monitoring, identity theft insurance, and out-of-pocket expenses). But see In re Trans Union Corp. Privacy Litig., 2009 WL 4799954 (N.D. Ill.), modified and remanded, 2011 WL 117108 (7th Cir. 2011) (opining that “the 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").


73 Id. at 397.

74 Id. at 409.

75 2010 WL 3341200 (W.D. Ky.)
76 Id. at *10.
77 255 F.R.D. 393, 397 (E.D. Pa. 2009) (dealing with the settlement of claims related improperly obtaining credit reports).
78 38 C.F.R. § 75.118 (Westlaw 2011).
80 See GAO Report, supra note 69, at 22-23.
81 Id. at 23 n.39.
82 See Sheri Qualters, Should Prison Hacker Pay for Credit Monitoring as

83 2010 WL 5014386 (D. Minn. 2010).
84 Id. at *1.
85 Id. at *3.


87 See, e.g., Belmont Holdings Corp. v. Sun Trust Banks, Inc., 2010 WL 3545389, *2 (N.D. Ga.) (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 a portfolio); *Saccato v. Gordon*, 2010 WL 3395295, *2 (D. Or.) (noting that the plaintiff’s use of credit monitoring disclosed an allegedly erroneous debt entry); *Dixon- Rollins v. Experian Information Services, Inc.*, 2010 WL 3749454, *1 (E.D. Pa.) (indicating that use of a credit monitoring service revealed the improper listing of a debt on a credit report).

88 *But see Rowe v. UniCare Life and Health Ins. Co.*, 2010 WL 86391, *7 (N.D. Ill. 2010) (stating 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”).
89 *Id.*
91 See, e.g., *In re Paoli Railroad Yard PCB Litig.*, 916 F.2d 829, 850 (3rd 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) (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.

But see Lowe v. Philip Morris USA, Inc., 183 P.3d 181 (Or. 2008) (holding that a smoker was not entitled to medical monitoring damages based on accumulated exposure to cigarette smoke); Paz v. Brush Engineered Materials, Inc., 949 So.2d 1 (Miss. 2007) (holding that the state does not recognize medical monitoring claims in the absence of proof of physical injury).

93 Sutton v. St. Jude Medical 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).

94 220 S.W.3d 712 (Mo. 2007).
95 765 S.W.2d 42 (Mo. App.1988).
96 220 S.W.3d at 717.
97 Graves, supra note 3, at 12.
98 Graves, supra note 3, at 21 (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”).
99 Black’s Law Dictionary (9th ed. 2009) (defining "de minimis non curat lex").