



Up and Coming

New interpretations of the Identity Theft Enforcement and Restitution Act could present risks for insurers.

by John F. Mullen and Mark Camillo

Contributors: John F. Mullen Sr. is chair of the Complex Litigation Group at Nelson Levine de Luca & Horst. He may be reached at jmullen@nldhlaw.com. Mark Camillo is a vice president, professional liability, in the New York office of Chartis Insurance and may be reached at Mark.Camillo@ChartisInsurance.com.





IDENTITY CRISIS: A law passed by Congress in 2008 provides that perpetrators of identity theft must reimburse their victims for the value of the time the victims spent trying to repair their credit records. It's one of a number of federal and state laws designed to address the ever-growing problem of stolen identities.

tiffs to proceed by finding that there is no injury-in-fact to the consumers or employees whose personal information was compromised as a result of a data security breach. That is, the risk of future harm is too uncertain. Some courts reason that without more certain injury in data loss cases, individuals lack standing to pursue such claims.

Other courts rely on state laws requiring sufficient injury before tort damages are awarded. An example of such a decision occurred in *Hinton v. Heartland Payment Systems Inc.*, where a federal district court in New Jersey dismissed an action by an individual who alleged information loss, but not identity theft, as failing to state a cause of action.

To date, courts have generally recognized claims for damages based on future harm only in two limited circumstances. First, where the threat of future harm is based on present injury. Second, where future harm is reasonably certain, such as medical cases where plaintiffs are exposed to a proven hazardous substance at significant levels.

Credit monitoring and lost time damages may be sufficient to satisfy the damages hurdle if the likelihood of a future identity theft can be shown to the satisfaction of the court. Accordingly, in a case involving a large breach, an attorney who demonstrates that a certain percentage of the affected individuals actually experienced

Key Points

- ▶ **The Situation:** Victims of data breaches have a difficult time recovering costs solely for credit monitoring.
- ▶ **What Happened:** The Identity Theft Enforcement and Restitution Act allows for restitution of expenses incurred by victims.
- ▶ **Watch For:** The act's mandate that victims should be compensated for the time they spend to remediate potential harm may create greater risks for insurers and the companies they cover.

identity theft may see their cases survive motion practice. This is a critical juncture in the litigation, as once past dispositive motions, plaintiffs' claim value and the costs/risks faced by the insured/insurer, increase.

But generally, there is no available contract or tort redress for costs associated with lost data unless linked to actual identity-theft events. The reasoning is that the risk of possible future identity theft in the event of a data breach does not rise to the level of appreciable harm necessary to substantiate a negligence or contractual claim or to support a damages award.

A New Law

Recognition of the ever-increasing seriousness of identity theft, and its repercussions to individuals and society, has prompted

Professional Services

ATTENTION MGAs / INSURERS



CSI is an A+ A.M. Best rated P&C/A&H insurer licensed in all 50 states, the District of Columbia and Guam, with a Life insurance affiliate. (*Rating is effective May 6, 2010. For the latest rating, access www.ambest.com*). We have been in business over 33 years and our Parent Company has an AA+ rating from Standard & Poors. **CSI is looking for unique partnership opportunities.**

If interested contact:
jjuricek@csi-omaha.com
Central States Indemnity Co. of Omaha
402-997-8338

Individuals whose personal information may have been compromised as a result of a data breach historically face an uphill battle in seeking restitution from the company whose network systems are involved. The law does not yet recognize lost time spent ensuring that potentially compromised personal information is adequately protected or credit monitoring/repair as damages. That may soon change.

When faced with the typical data breach lawsuit alleging credit monitoring damages, courts have routinely refused to allow plain-

federal and state governments to enact laws to protect consumers from actual and potential harm stemming from data breaches involving personal information. Until recently, these laws typically focused on notifying victims of data breaches and preventing such occurrences.

However, in 2008, the federal government passed the Identity Theft Enforcement and Restitution Act of 2008. The act, among other things, provides a vehicle to compensate victims of data loss as a result of a criminal data breach by providing direct restitution for the value of their time spent repairing the intended or actual harm suffered.

The statute specifically provides that convicted offenders must “pay an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense.”

As a result, the plaintiffs’ bar may now argue that this provision of ITERA constitutes acknowledgment by the federal government of the serious impact of potential identity theft on data breach victims and provides plaintiffs the means to recoup their time-related losses.

In essence, they will posit, federal law now agrees that in the world of data security and compromised personal information, time is money and lost time alone should also constitute sufficient damage to sustain a civil suit.

Extending the Law

Although the statute did not go so far as to provide a similar remediation right in data security civil litigation, this provision of the act may persuade federal courts that lost time alone or combined with the costs associated with credit monitoring and identity theft/repair insurance are sufficient recoverable damages.

Considering the consequences of

The current defense-friendly environment is eroding. The barrier of dispositive motions should no longer engender a sense of security in companies and institutions that store personal data, or the insurers of those institutions.

identify theft and the steps potential victims may reasonably take to protect themselves in the event of a data breach, an argument can now be made that an extension of ITERA into the civil law governing data breaches is reasonable, necessary and warranted. The loss of personal information is tantamount to personal injury or property damage when balanced against the risks borne by inaction in securing one’s finances or identity.

While not a positive development in the defense of data security class-action claims, the fact remains that plaintiffs have a strengthened argument that such an extension would be nothing more than society’s recognition (given its growing importance to consumers, government and business) that personal information is valuable property subject to loss and that the time spent safeguarding one’s finances and privacy after such information is compromised is real injury.

In a service economy, there are many examples of time being used as a measure of value—accounting, consulting, medicine and law. ITERA is the first federal recognition of that time-is-money reality in the world of network and data security.

The current defense-friendly environment is eroding. The barrier of dispositive motions should no

longer engender a sense of security in companies and institutions that store personal data, or the insurers of those institutions.

The net impact is that the act presents another potential damages argument to courts that have been generally unwilling to consider restitution for credit monitoring, credit repair, or lost time as sufficient damages.

A combination of this ITERA argument with class representatives, who can demonstrate identity theft subsequent to a breach event, may well overcome the “insufficient damages” barrier that has long protected insureds and their insurers from the unknowns of jury verdicts.

For insurers providing coverage to companies for network security (a rare growth area in the insurance world), ITERA’s mandate that victims should be compensated for the time they reasonably spend to remediate potential harm will create greater costs and risks. Courts may come to feel that institutions that collect, store and protect consumer information and can more easily insure for its loss, should compensate victims for their lost time.

The coverage available in most security and privacy insurance policies could become an even more important benefit in response to security breaches. By proactively notifying individuals providing identity monitoring, credit restoration, and victim reimbursement, plaintiffs’ arguments using ITERA could be weakened and subsequent risk reduced.

The enactment of ITERA and the growing collection and use of personal information by business entities, combined with growing societal recognition that time may, indeed, be money, may result in a shift in how courts view the alleged harm suffered by individuals whose personal information is compromised. **BR**