Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How New Credit Freeze Law May Affect Data Breach Cases

By **Robert Kriss and Corwin Carr** (August 3, 2018, 12:06 PM EDT)

Robert Kriss

Corwin Carr

Congress recently enacted a law that enables consumers to freeze their credit reports to prevent identity theft at no cost.[1] This law may have significant implications for whether data breach class actions will be certified and the amount of potential damages in class actions if classes are certified.

It is not apparent how a plaintiff can prove damages on a classwide basis in a data breach case. In Dieffenbach v. Barnes & Noble, the Seventh Circuit recently expressed skepticism concerning class certification given the individualized nature of most types of damages that might flow from a data breach.[2]

Before the Credit Freeze Act, some plaintiffs contended that a court could provide a classwide remedy by ordering a defendant to purchase credit monitoring services for the entire class or pay the cost of implementing credit freezes. The cost of establishing credit freezes ranged from $3 to $10 per credit reporting agency, depending upon the agency in question and applicable state regulations. Unfreezing and refreezing credit could trigger additional charges. To obtain broader protection, a consumer had to separately request each agency to implement a credit freeze.

Companies suffering data breaches have sometimes appropriately offered to provide customers with free credit monitoring services for a year or two. There are, however, some limits to what credit monitoring services can do. They provide notice to consumers after a new account has been opened in their name so they can take steps to close the account and repair the damage if they were not the person who established the new line of credit. Credit monitoring does not prevent identity theft; it allows the consumer to mitigate the effects of identity theft after it happens.

Credit freezes, on the other hand, prevent most forms of identity theft involving opening new accounts and remain in effect until removed by the consumer. After a consumer activates credit freezes at the three credit bureaus, no wrongdoer can open a new line of credit in the consumer's name using the consumer's stolen social security number. New credit lines for that consumer can be established only by the consumer 'unfreezing" his or her credit records at the reporting agency using unique authentication information.

Of course, credit freezes will not prevent all forms of identity theft. For example, credit freezes do not stop wrongdoers from submitting false requests for tax refunds, do not prevent injury allegedly resulting from disclosure of medical information and do not prevent fraud committed with respect to existing accounts, including credit card accounts (but false credit card charges generally are reversed upon request). Nevertheless, credit freezes are more effective than credit monitoring in preventing loss due to identity theft after a data breach. And now credit freezes are free. Generally, it should take only a few minutes to institute a credit freeze or to unfreeze credit.

In light of the new Credit Freeze Act, defendants facing data breach litigation can argue that plaintiffs have a duty to mitigate damages arising from a data breach by implementing free credit freezes and, if they choose not to do so, they should not be entitled to any damages that could have been prevented by a freeze.[3] Furthermore, defendants may argue that it would be unreasonable for a company suffering a data breach to be forced to pay for credit monitoring services, which can cost hundreds of dollars per class member, when credit freezes, which arguably are more effective, are now free.

If the cost of credit monitoring or a credit freeze is not recoverable in a data breach class action, what other types of damages might be assessed on a classwide basis? Plaintiffs might try to argue that they should be able to recover damages to compensate them for their lost personal time in responding to a data breach, e.g., the time spent disputing credit card charges or sorting out instances of identity theft in connection with wrongful opening of new accounts.

The decision in Dieffenbach might be read to suggest that lost time damages are recoverable, at least on an individualized basis under California law. Yet the California case cited in the opinion held only that lost time might be a sufficient injury to establish standing, and alleging harm sufficient to satisfy standing requirements does not mean that the applicable law allows for the recovery of damages for such a claimed injury.[4] Furthermore, other courts have squarely held that lost time remedying the effects of a data breach is not compensable under contract or tort law (whether or not it is sufficient to establish injury for standing purposes).[5]

But even if a cause of action does provide monetary compensation for lost time, how could a court determine such damages in a putative class action? The amount of time a person must spend to mitigate damages and the value of a person's "lost time" would appear to vary greatly depending on individual circumstances.

In view of the foregoing, a court might decide not to certify a data breach class action. As mentioned above, the Seventh Circuit in Dieffenbach has expressed doubts about the appropriateness of certifying data breach class actions because of the individualized issues relating to choice of law and damages.

Even if a class is certified with respect to liability issues and the defendant is found liable for failing to implement reasonable data security, the damage phase of the proceeding most likely will involve individualized determinations of damages. Under the Rules Enabling Act, defendants cannot be deprived of individualized defenses as a result of class certification. Individual plaintiffs will have to present evidence of their alleged damages and be cross-examined by defendants' counsel.[6] In a large data breach class action, conducting thousands, if not millions, of mini-trials over these issues would render class trials unmanageable.

There is very little law concerning class certification in contested data breach cases because virtually all cases have been dismissed, most often on standing grounds, or settled. No cases have been tried on the merits. Because the law is not well-developed in these areas, there remains considerable uncertainty

regarding litigation risk in data breach cases. And the harms flowing from data breaches extend beyond litigation risk, of course. As a result, prudent companies undoubtedly will implement reasonable data security measures to minimize litigation and business risks.

However, if a breach should occur and a putative class action is commenced, the recent Credit Freeze Act may reduce the likelihood of class certification or, at minimum, reduce the amount of damages potentially recoverable on a classwide basis.

Robert J. Kriss is a partner and Corwin J. Carr is an associate at Mayer Brown LLP.

[1] See Public Law S 115-174, entitled the "Economic Growth Regulatory Relief and Consumer Protection Act" (Credit Freeze Act).

[2] See Dieffenbach v. Barnes & Noble Inc., 887 F.3d 826, 829 (7th Cir. 2018) ("It is also far from clear that this suit should be certified as a class action; both the state laws and the potential damages are disparate.").

[3] See e.g., Sackin v. TransPerfect Global Inc., 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (recognizing that victims of data breaches have a duty to mitigate damages, and that "[plaintiffs] could not passively wait for their identities and money to be stolen.").

[4] See, e.g, Pisciottav. Old Nat. Bancorp, 449 F.3d 629, 663, 637-40 (7th Cir. 2007) (risk of future harm from data breach was sufficient to establish Article III standing, but was not a compensable injury under applicable Indiana statute).

[5] See, e.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 4 A.3d 492, 496 (Me. 2010).

[6] See, e.g., Tyson Foods, supraat 1048, citing Wal-Mart Stores Inc. v. Dukes,564 U.S. 338 (2011) ("The Court [in Walmart] held that this 'Trial by Formula' was contrary to the Rules Enabling Act because it 'enlarge[d]' the class members' 'substantive right[s]' and deprived defendants of their right to litigate statutory defenses to individual claims.").