At Risk: Community Banks and the Recovery of Losses Due to Merchant Data Breach

Jul 06, 2015

Categories:

Blockchain and Digital Assets
Blogs
Publications

Historically these Banks simply accepted losses not reimbursed by the credit card companies as a cost of doing business. With more data breaches occurring and the costs escalating, however, these Banks must consider the possibility of seeking recovery of these losses. Recent case law and using joint prosecution and cooperation agreements may hold some new promise for this recovery.

As a general matter, once a credit card purchase is made, merchants, such as Target or Home Depo, or the merchant's POS processor forward transaction information to an "Acquirer Bank." Acquirer Banks process the merchant's and essentially feed it into the Card Associations' settlement processes. The Card Associations, like Visa and MasterCard in turn communicate the card transaction data to the Issuer Bank's whose cards were used by the consumer. Ultimately the funds to settle with the merchant are transferred by the Issuer to the Acquirer, for the benefit of the merchant's own bank account balance, all assuming that the consumer has sufficient funds under its credit card with the Issuer Bank. As one can see from this general description of the process, the Issuer Bank has no contractual relationship with the merchant.

But when the consumer's card information is stolen, the pain begins. Under the terms of the contracts between the Card Associations and the Issuer Banks, the Card Association's only have a limited duty to reimburse the Issuer Banks for expenses and costs due to a data breach. As many banks have discovered, this contractual reimbursement is far from sufficient to cover the Issuer Banks' true losses. In the Target litigation, for example, the losses to issuing Credit Unions and community Banks were estimated to be well over $200 million.

Traditionally, claims by Issuer Banks to recover unreimbursed losses from the merchants who were responsible for the data breach have not fared well. Courts often dismiss such claims, finding a lack of

duty of the merchant to the Issuer Bank, or the presence of a superseding intervening cause precluding recovery, or that the claims were barred by the economic loss rule (a complicated and confusing thicket that differs from state to state, with exceptions to the same which often swallow the rule). Recent results in the litigation stemming from the Target data breach do, however, provide some hope for recovery.

The Target Litigation

As most everyone knows, the Target litigation stems out of the theft of credit and debit card information of over 110 million customers of Target in December 2013. Numerous lawsuits were filed and the litigation was assigned to the Multi District Litigation Panel, and transferred to Minnesota before Federal Judge Paul Magnuson.

Two types putative class actions were presented in the Target litigation: one brought by Card Issuer financial institutions, and one by consumers of Target. Late last year Judge Magnuson denied Motions to Dismiss filed by Target regarding both putative classes. This opens the door to the Issuer Banks' possible recovery

The Issuer Banks' Claims

The financial institution putative class in the Target litigation consists of Banks that had issued credit or debit cards to consumers whose information may have been stolen. The named Bank plaintiffs, who filed the litigation on behalf of this class, were Umpqua Bank, Mutual Bank, Village Bank, CSE Federal Credit Union and First Federal Savings of Lorain. These Banks claim losses for:

- Costs associated with notifying customers of the data breach;
- Costs associated with reissuing debit and credit cards;
- Costs in reimbursing customers for fraudulent transactions;
- Costs associated with monitoring customer accounts to prevent fraudulent charges;
- Costs in addressing customer confusion and complaints;
- Costs associated with changing and canceling accounts;
- Costs associated with the decrease and suspension of their customer's use of the affected cards during the busiest

shopping season of the year.

Not claimed as damages were the very real losses of reputation and good will to the Banks growing out of the breach.

The Banks claimed that Target was responsible for these losses because:

- It acted negligently in failing to provide sufficient security to prevent the hackers from obtaining access to the data;
- It failed to prevent the breach violated the Minnesota Plastic Security Card Act and the violation of the Act constituted negligence per se; and
- It failed to inform the Banks of its insufficient security which constituted a negligent misrepresentation.

In seeking to dismiss these claims, Target argued that it had no duty to the Issuer Banks with whom it had no contracts; that by definition, its conduct created no foreseeable risk of harm; that it had no "special relationship" with the Banks to create any duty for the acts by someone else; and that the Minnesota Act did not apply to transaction taking place outside of Minnesota.

The Target Decision

Taking a restrictive view of the Supreme Court's ruling in another case, **Bell Atl. Corp v. Twombly, 550 U.S.544 (2007)**) (in which the Court envisioned a broader and more sweeping view of motions to dismiss and allowed inquiry beyond merely accepting the pleadings on their face to be true), Judge Magnuson held that the plaintiffs' general negligence claim was adequately pled. According to the Court, the claims that Target disabled a security feature that created a foreseeable risk to the Banks, and Target's failure to take timely actions once the attack began would state a cause of action.

Judge Magnuson also held there was a duty owed by Target to Issuer Banks, and that Target was "solely able and responsible" to safeguard the data. The Court commented that its finding would aid the Minnesota public policy of "punishing" companies that do not secure credit and personal information.

Finally and significantly, the Court held that Minnesota's Plastic Security Card Act applied to any data retention practices of any entity conducting business in Minnesota. Even if a transaction did not occur in Minnesota, the Act, which is similar to laws in most states, still applies to Target's actions. (The Court rejected the negligent misrepresentation claim because the plaintiffs pled no reliance on any Target omission. In doing so, the Court commented that it believed Target knew facts about its inability to repel hackers that the Banks could not have known.)

The decision means that Issuer Banks may now have new tools to recover their losses. Significantly, the recognition by the Court that Target's action created a "foreseeable risk of injury to a foreseeable plaintiff" gives Issuer Banks hope that duty and intervening cause issues will not necessarily preclude recovery. (This intervening cause doctrine, use of which was pioneered in part by this law firm, see **Gaines-Tabb v. ICI Explosives, USA, Inc. 163 F3d 613 (10th Cir. 1998)** , provides that a person has no duty to protect another from third party criminal conduct unless that conduct was clearly foreseeable. As more and more criminal data breaches occur, the foreseeability of criminal third party conduct may as a legal matter be increasing as well). The Target decision also lends credence to a board application of state statutes designed to protect against and deter data breaches.

Practical Recovery Questions

But even if there may now be some hope for theories or recovery, how might regional and community Issuer Banks go about successively seeking such recovery– given the substantial costs and risks associated with such litigation?

Clearly, a small Bank attempting to proceed on its own may soon find itself embroiled in lengthy and intolerably costly litigation. Legal fees and costs and the business disruption often means that the individual pursuit of recovery for data breach losses is simply not worth it. Certainly, the use of contingency fees can hold down attorney costs, but getting experienced counsel to assist on a contingency fee basis is problematic, if damages are not significant and probable of recovery.

Another option is to go the litigation route followed by the Plaintiff class in the Target lawsuit: bring a class action on behalf of all effected and similarly situated Banks. This requires one or more named plaintiffs to front the out-of-pocket costs and disruption on behalf of all. Typically, such named plaintiffs will get a marginally increased recovery for their efforts but again such increase may not be worth the time and trouble unless the named plaintiffs suffer substantial losses.

And while the putative class member Banks get in essence a free ride with little direct cost, such free ride is not without risk. Typically the putative class members have little control or influence over the litigation. This can result in all sorts of mischief. In the Target litigation for example, Target negotiated a settlement with MasterCard that required Target to pay MasterCard a token amount that would then be shared with the Issuer Banks. While in this case the Issuer Banks were able to mount sufficient resources to crater the deal, it would be easy to envision a situation where large named plaintiff Issuer Banks would negotiate a settlement that favored them at the expense of other smaller class members.

One approach with which we have had success over the years is the banding together of businesses, such as Banks, through joint prosecution and cooperation agreements to bring common claims. This allows the participants to share the overall costs and for recovery to be allocated on a predetermined basis. By doing so, smaller Issuer Banks could secure competent, experienced counsel, mount an aggressive litigation approach and maximize recovery prospects at an individually affordable cost. Even in the class action context, this banding together often provides to those involved greater clout and influence than they would otherwise have.Community Banks are at risk for losses associated with their Issuer card programs often through no fault of their own. Recovery of such costs and the shifting of responsibility for them to culpable parties is an important and beneficial tool that will ultimately create a more secure system ultimately reducing the overall system risks.

FBT Gibbons