Target Data Breach Losses Begin to Add Up for Retailer

February 7, 2014 - There was never any doubt that the data breach at Target Stores last December would be costly to the retailer. After all, when you breach information on up to 110 million people, someone is going to have to foot the bill. The real questions have been who will pay the bill how much it will cost? The way that things look now is that the "who" will probably be Target, leaving only the question of "how much" outstanding. The fall-out from this breach should provide an object lesson to the entire retail industry as to just how expensive a data breach can become.

Since making the data breach public, Target has also stated that its sales were down. Based on the wide variety of new releases since the breach, one has to wonder if Target could have purchased all of the bad publicity that the company has received since. In my opinion, the company has bungled virtually every opportunity that it has had to stop the damage.

First, the company announced that the breach impacted only in-store sales and 40 million people. Shortly thereafter, they had to announce that online transactions were actually involved and that as many as 70 million additional people could have been impacted.

The company's website provided minimal information on the breach right after the initial announcement, but it did provide a phone number for people to call if they thought their information may have been released in the breach. But calling the number and getting through to a live body was difficult at best. There were numerous reports of people being forced to hold for prolonged periods of time only to be disconnected and forced to call again. And those report concerned people who had Target credit accounts. It was even worse for people who used non-Target debit and credit cards. Those people were connected to a recorded message telling them to call their bank or credit card company. After the message was delivered, the calls were disconnected. Not exactly a great way to make consumers feel appreciated.

Target then announced that it would be offering credit monitoring to victims of the breach. That's turned into another bungled opportunity to repair some the damage. It took the company several weeks to provide the credit monitoring. Making matters worse, Consumer Reports is now saying that the monitoring offered is substandard. In fact, it appears to be a bait and switch, covering only Experian credit reports. According to the article, anyone signing up for it is almost immediately solicited to pay for a more complete credit monitoring service covering all three credit bureaus. (NOTE: Credit monitoring will only notify you after you have been victimized and ACCESS considers the service to be worthless when it comes to preventing future victimization.)

In addition to the above mentioned woes, there are now multiple lawsuits that have been filed against target. Some of these are consumer lawsuits. But others are being filed by banks. The final cost to Target is unknown at this point but the bank suits alone are likely to cost tens of millions of dollars. In fact, since it costs a bank roughly 50 cents to issue a credit card, if banks are forced to reissue 100 million cards, their actual costs would start out at $50 million. And that's before lawyers' fees, the costs of any actual fraud or punitive damages.

There is probably no way to prevent data breaches. There are simply too many variables in an often disjointed electronic banking system on a daily basis. But the Target example appears to be a case study in how not to handle a data breach. As bad as the initial breach was, from what I can see Target's actions have repeatedly increased the damage done to the company's image. If nothing else, retailers need to have a plan of action in place not only to prevent data breaches, but also to swiftly address them once they occur.

byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow me on Twitter:

Follow ACCESS