Target & Neiman Marcus Data Breaches Should Be a Wakeup Call to Retail Industry/Banks

January 13, 2014 - Late last week, Target Stores was forced to announce that its data breach is December was much larger than originally thought. Up to 110 million target customers could find that their data was stolen and is now being used by fraudsters; making it the largest criminal data breach in retail history. Then, over the weekend, Neiman Marcus announced a breach of its own, currently of unknown size. These two incidents should be a wakeup call to retailers around the United States that it is time to beef up their cyber-security or face the wrath of consumers.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Target's data breech is proving to be costly. Prior to announcing the breech, the chain had announced that its December sales were flat when compared to last year. After the announcement, the company said that its sales had declined noticeably. The same can probably be expected for Neiman Marcus. And of course, all of this is prior to the inevitable lawsuits that are likely to follow. These mistakes are likely to cost each company millions of dollars.

Making matters worse, the Target breach was probably completely preventable with existing technology. The same may prove true with Neiman Marcus.

For a wide variety of reasons, American retailers and banks have resisted the use of increased security measures that are common in other areas of the world. Specifically, embedding smart chip technology in credit cards. This technology is so widely used in Europe now that Americans are finding it difficult to use their credit cards when traveling there. Most American cards simply don't have this technology embedded in them; choosing instead to rely on using magnetic strips on the back of each card.

Smart chips in credit cards are much more difficult to hack, and nearly impossible to reproduce. But if a thief can steal the data in a cards magnetic strip which doesn't have this technology, then producing a counterfeit card is a fairly simple task. The bottom line is that stealing a credit card number doesn't buy the thief much if the card also has the chip in it.

But the cost of converting to smart chip cards isn't cheap. Retailers will need to change out a lot of equipment to make it work and banks will find that it is more expensive to manufacture their credit cards. Those are probably the two largest factors that have prevented smart chip introduction in the United States. Fortunately, that may be about to change. That's because new banking rules are set to go into effect that will force the company responsible for the data breach to bear the cost of it. That will include bank charges for reissuing credit cards.

But smart chips aren't the only answer either. That's because the technology works at the point of sale but may not be able to prevent fraud associated with online purchases. But single-use credit card numbers may be able to pick up that gap.

A few years ago, American Express offered single use numbers for precisely this purpose. As an AMEX customer, you could simply log into your account and generate a credit card number that was good for your next purchase. Once the number was used, it couldn't be used again. It was a great system but it was eventually eliminated. It may be time to bring it back.

The point here is that there are already technologies available to reduce fraud. Companies just need to start using them, or making them available to consumers.

The Target data breach could impact nearly 50% of the adult population in the US. How large does a breach have to be before banks, retailers and regulatory agencies all agree that it may be less expensive to protect the public than it is to clean up the mess after a breach has already occurred?
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