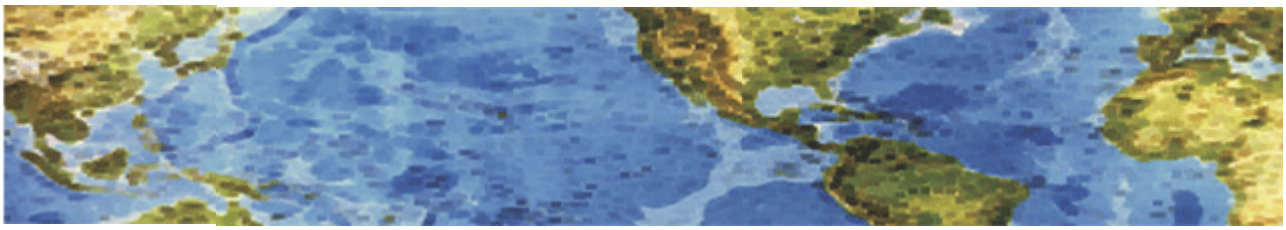
HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 January 2014 Newsletter

Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen

Some additional information about the Target data breach covered in earlier newsletters –

Target disclosed that a data breach discovered last month **exposed the names, mailing addresses, phone number and email addresses for up to 70 million individuals**. "As part of Target's ongoing forensic investigation, it has been determined that certain guest information — separate from the payment card data previously disclosed — was taken during the data breach," the company said in a statement. "This theft is not a new breach, but was uncovered as part of the ongoing investigation. At this time, the investigation has determined that the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 million individuals." Target said much of the data is partial in nature, but that in cases where Target has an email address, it will attempt to contact affected guests with informational tips to guard against consumer scams. **The retail giant was quick to note that its email communications would not ask customers to provide any personal information as part of that communication**. **Watch out for email scams trying to get you to reveal even more personal information.**

Target still has not disclosed any details about how the attackers broke in. This lack of communication appears to have spooked many folks responsible for defending other retailers from such attacks, as it should since they can't know if they are defending appropriately. This latest disclosure also raises questions about what other types of information may have been jeopardized in this data breach. As part of its statement, Target said it would be offering a year's worth of free credit monitoring services to those affected. Target does collect Social Security numbers from customers who apply for Target Red Cards, which offer applicants 5 percent cash back if they agree to tie their debit accounts to the Red Card. So far, however, Target has not said anything about compromised Social Security numbers.

Reading between the lines, one might wonder why Target is providing credit monitoring services to those hit by what is essentially a credit card breach. Many people conflate credit card fraud with identity theft, but these are two very different problems. The former is quite easy for the consumer to resolve, and he or she has very little (if any) liability for fraud. Identity theft, on the other hand, generally involves the creation of new or synthetic lines of credit in the consumer's name, which can take many years and cost thousands of dollars to resolve.

The reason Target is offering ID theft protection as a result of this breach probably has more to do with the fact that this step has become part of the playbook for companies which suffer a data breach. Since most consumers confuse credit card fraud with ID theft, many will interpret that to mean that the breached entity is somehow addressing the problem, whereas experts tell me that this offer mainly serves as a kind of "first response" to help the breached entity weather initial public outrage over an intrusion.

Also interesting is this from a Chicago Tribune article:
Target customers whose information — name, addresses, phone numbers and email addresses — was stolen need not have shopped at the retailer's stores during the busy holiday shopping season, a spokeswoman confirmed Friday. The information, said Target spokeswoman Molly Snyder, was collected during the "course of normal business," and could include online shopping.
Target's latest announcement on the Target web site doesn't state that online shoppers were affected, nor does it state that this newly-identified theft occurred outside of the initial breach period. If this article has correct information, then for how long was the personal data of customers available to thieves?

So is there anything else you can do to protect yourself other than watching your credit card transactions?
Change your credit/debit card account – and get new cards
Ask your bank about what they are doing to protect you about this breach
Be careful with the personally identifiable info you share online
Change your email password so that is long and strong
Do not use the same password you use for your email account on any other sites
Buy using cash…and make sure you use an ATM which sits inside an actual bank

And when you receive an email from Target or your bank explaining what happened and how sorry they truly are and asking for additional information, **don't click on the link or open the attachment. It's a scam. You will get hit again, and again, and again.**
http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/

Firm Bankrupted by Cyberheist Sues Bank

A California escrow firm that was forced out of business last year after a $1.5 million cyberheist is now suing its former bank to recoup the lost funds. A state-appointed receiver for the now defunct Huntington Beach, Calif. based Efficient Services Escrow has filed suit against First Foundation Bank, alleging that the bank's security procedures were not up to snuff, and that it failed to act in good faith when it processed three fraudulent international wire transfers totaling $1,558,439 between December 2012 and February 2013.

On Dec. 6, the lawyer appointed to be Efficient's receiver sued First Foundation in a bid to recover the outstanding $1.1 million on behalf of the firm's former customers. The suit alleges that the bank's security procedures were not "commercially reasonable," and that the bank failed to act in "good faith" when it processed international wire transfers on behalf of the escrow firm.

The lawsuit, filed in the Superior Court for Orange County, is the latest in a series of legal battles over whether banks can and should be held more accountable for losses stemming from account takeovers. In the United States, consumers have little to no liability if a computer infection from a banking Trojan leads to the emptying of their bank accounts — provided that victims alert their bank in a timely manner. Businesses of all sizes, however, enjoy no such protection, with many small business owners totally unaware of the risks of banking online.
http://krebsonsecurity.com/2014/01/firm-bankrupted-by-cyberheist-sues-bank/