# After a data breach, it's consumers left holding the bag

November 28 2014, by Diana S. Dolliver

Is it a crime scene or just a store checkout? Could be both. Credit: Marlith, CC BY-SA

Shoppers have launched into the holiday buying season and retailers are looking forward to year-end sales that make up almost 20% of their annual receipts. But as you check out at a store or click "purchase" on your online shopping cart, you might be setting yourself up as the victim of a crime.

Major data breaches at big retail companies have brought this form of

cybercrime to the international stage. Between November 27 and December 15, 2013, hackers accessed Target's point of sale machines – the cash registers – that housed millions of credit and debit card numbers in addition to the names, addresses, email addresses and phone numbers of shoppers. They stole an estimated 40 million credit and debit card numbers. In 2014, hackers stole approximately 56 million customer credit and debit card numbers from Home Depot.

These numbers are astronomical – where does all that stolen information go? And who is behind it?

## Hidden hackers

The individuals or groups of people responsible for these kinds of cybercrimes are varied. There are teenage opportunists operating alone, hackers looking for a challenge and even sophisticated organized criminal syndicates. Some criminals simply want to see if they can break through security systems as practice to hone their hacking skills. Speculation circulates that some hacking is state-sponsored; there's little published research to back it up, but it appears China, for one, engages in cyber espionage.

Criminals seeking to profit from stolen information may open bank accounts in victims' names or access financial institutions for monetary gain. Of course, no single person is opening 40 million new credit cards. Hackers who steal identities and credit card information in the massive volumes of the Target or Home Depot breaches may break down the millions of credit and debit accounts into bulk batches – groups of 10,000, for instance – and sell them to the highest bidder via online illegal marketplaces, such as those on the Tor Network.

Once personal data is stolen and sold, the possibilities are endless. Criminals use stolen identities to create fake state or country IDs and to

purchase things like plane tickets, cars, and weapons. Email addresses become spamming targets. Credit/debit card information is valid as long as the victim remains unaware of the theft. That's why it's so important for consumers to vigilantly check their accounts on a regular – even daily – basis.

Some of the biggest headaches come when a criminal steals valid identity details – such as name, date of birth or social security number. It can be extremely challenging for a victim to prove he is the REAL John Doe. Bank accounts can be closed and credit/debit card numbers changed as soon as foul play is detected, but a person's name and SSN cannot. The greater risk for holiday shoppers is that stolen financial information will be used to make unauthorized purchases, but having someone create a new identity with stolen personal information isn't outside of the realm of possibility.

## (Lack of) legal response

In today's world, victim and offender no longer need to be in physical proximity. And because of the wide range of cybercrime perpetrators, each with different motives, law enforcement agencies have quite a challenge on their hands. The FBI's Internet Crimes Complaint Center receives over 250,000 reports each year from victims of cybercrimes, totaling over US$781 million per year in losses. It's estimated that many times more victimizations are never reported – the so-called "dark figure" of cybercrimes.

Law enforcement agencies struggle to hire and train personnel on detecting and investigating these types of crimes. Currently, if you discover yourself to be the victim of cybercrime, your local police department is probably ill-equipped to handle the case. Instead, your financial institution will most likely work with you to investigate the issue, and you should report the incident to the FBI's Internet Crimes

Complaint Center.

The average financial loss for complaints the FBI received in 2013 (that involved any monetary loss) was $6,245. Each bank has its own policies, but for the most part they eventually remove the fraudulent charges from hacked credit cards – typically after a lot of paperwork on the part of the victimized consumer. Regaining money stolen from a debit card or checking account can be much harder.

## Consumers as cybercrime-fighters

While lawmakers consider how to target cybercrime and agencies work out how to equip themselves, it falls to citizens to protect themselves.

- Request new debit and credit cards from your financial institutions once or twice a year. You'll receive new numbers and won't have to pay for the new cards. Change your PIN on a regular basis. Monitor your credit report annually.
- Don't over-share on social media. Protect your image and personal info.
- Never open an email or link from someone you don't know.
- Never share passwords or personal info with an untrusted source. When in doubt, call the institution to clarify the situation.
- Report any suspicious activity or instances of victimization to the FBI's Internet Crime Complaint Center.
- Limit the number of online payments you make.
- Only complete online payments on secured (https) websites from a password-protected computer. Using your smartphone or tablet on a wifi network gives bad guys an easy way to capture your info.
- Use security software on your devices and perform routine checks to ensure your system is bug-free.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: After a data breach, it's consumers left holding the bag (2014, November 28) retrieved 4 May 2024 from https://phys.org/news/2014-11-breach-consumers-left-bag.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.