KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

How Do Banks Protect You From Cybersecurity Breaches?

Banking Law / June 25, 2015

It is completely understandable to feel a sense of anxiety when you hear the words “cybersecurity breach” and “bank” in the same sentence. What reasonable person wouldn’t be concerned? You put your hard earned money into a bank, thinking it will be safe from thieves, and yet some hacker uses technologically advanced means to infiltrate your bank’s digital infrastructure to execute a heist, which makes a bank cybersecurity breach all the more frightening. But how does a breach of your bank’s cybersecurity actually impact you?

Financial Gain Is The Number One Motivation For Cybercrime

The main reason that cybercriminals commit crimes is for financial gain. Whether it is stealing personal information, credit card numbers or Social Security numbers, the end goal is to profit from the use or sale of the illegally obtained information. Luckily, when a bank customer is the victim of identity theft or bank fraud, the customer is generally not liable for the amount stolen (instances of a lost or stolen credit or debit card that go unreported until after fraudulent charges are made may result in some liability to the cardholder). Rather, the liability, especially in instances of a cybersecurity breach, often lies with the bank.

What Are Banks Doing To Combat Cybercrime?

In light of the highly publicized data thefts that have occurred in recent months, what are some things that banks are doing to protect customers from cybercrime?

- Nearly every state in the nation has laws in place that require a bank to notify customers in the event that there is a breach in security regarding customer data.
- Many banks also will shoulder the costs associated with reissuing cards and new account numbers for compromised accounts, although banks are not required by law to do so.
- Many banks are switching to chip-based payment cards (also known as Europay, Mastercard and Visa, or EMV standard), which uses a smart chip and a pin instead of a magnetic strip. These types of cards are more secure and harder to counterfeit.
- In the age of smartphones, many banks have taken advantage of push alerts that notify customers if a transaction is made, which helps customers identify fraud sooner rather than later.
- Many banks monitor customer transactions for unusual spending behavior, which it recognizes as suspicious and potentially fraudulent activity.

What Can You Do To Help Protect Yourself?

There are steps that you can take to help better protect yourself and your personal information from cyber theft. For example:

- Checking credit card and bank statements frequently to monitor for instances of fraud.
- When shopping online, only entering your credit card information for trusted sites that are certified as secure, e.g., the url for the webpage begins with http**s**://www.
- Regularly changing your banking passwords and pin numbers.
- Staying away from using credit and debit cards at retailers and websites that you do not trust.

Preventative Action Goes Along Way Towards Protecting Yourself

The resounding commonality among all of the efforts to combat cybertheft of personal financial data and bank information discussed above is to be proactive. When banks take steps to notify their customers that they could be potential victims, it empowers the customer to take steps to proactively combat any acts of fraud.