What Can Be Done About the Epidemic of Retail Data Breaches?

Springfield, Illinois - March 11, 2015

Schnuck's, Target, Home Depot… the list of retail data breaches goes on and on. How can consumers be certain their personal information stays just that – personal – and doesn't fall into the hands of criminal identity thieves?

You may have heard about chip technology and that it can help reduce fraud. That's true, but just up to a point. Chip technology, which is already being implemented by some banks and merchants, is not a cure-all for retail breaches. While many credit and debit card issuers have begun issuing cards loaded with chip technology, the fact is there is no single form of security that is a panacea for card fraud. The technology does nothing to protect customer information used for online purchasing and other forms of "card-not-present" fraud, which is where the majority of card fraud takes place. In fact, chip technology would not have stopped the Target breach, and we caution those who think this technology by itself will do the trick.

No standards or regulations exist for merchants that come close to those in place for banks in securing customer data or notifying customers. While merchants claim that they are subject to card industry security standards, there is no regulator enforcing of these standards or examining them for compliance. In fact, most merchants self-certify their compliance, and consumers affected by the dozens of recent merchant breaches know all too well that this self-regulation is not working.

You may already know that the banking industry invests billions of dollars to maintain the strongest data security systems and to train employees on customer privacy and security protocols. Banks by law are required to adhere to strict customer privacy policies and rigorous data security standards. Banks also are subject to laws and regulations telling them how to respond and how to notify customers when any data breach occurs, and they must use additional steps to freeze or close compromised accounts, cancel and reissue cards, and monitor accounts for suspicious activity, all while handling customer inquiries and reimbursing their customers for any fraud losses.

What you may not know is that banks often foot the majority of the bill when it comes to reimbursing customers in a breach, even though the breach was the fault of a retailer and not the bank. The fact is that every player in the payment system – banks, retailers, card issuers and processors – must share the responsibility and accountability for keeping customer information safe. This obligation should not fall solely on the banking industry.

To help protect your sensitive financial data, Congress should mandate that every business and person who collects and handles customer account and personal information should be held to similar security and privacy standards. Congress should also adopt universal standards for reporting breaches and notifying customers when a breach occurs – and every party, including merchants, should be accountable and financially responsible for losses suffered by others as a result of their negligence. You, the Illinois consumer, deserve nothing less!

CONNECT WITH
Debbie Jemison
524 South Second St.
Suite 600
Springfield, IL 62701

217-789-9340
djemison@ilbanker.com
ilbanker.com

OUR MISSION
Advocacy. Education. Industry Resource... for all Illinois Bankers

OUR VISION
Connecting Bankers. Advancing Banking.