



December 29, 2016

FOR IMMEDIATE RELEASE**Contact: Bruce E. Spitzer**
bspitzer@massbankers.org
617-523-7595

HOW TO PROTECT YOURSELF FROM ATM SKIMMING

BOSTON, Dec. 29, 2016 –As we head into the New Year, it's important to note that ATM skimming is on the rise, costing banks and customers an estimated \$3 billion a year, according to the credit-scoring agency FICO.

Criminals can "skim" your credit or debit card information using a fake card reader on an ATM or gas station pump, combined with a hard-to-see "pinhole" camera that records your PIN on the keypad. Unfortunately, thieves have been using increasingly sophisticated hardware affixed to machines that looks like it belongs there; consumers have a hard time spotting it. The criminals then make fraudulent cards with the data and can use it to drain your bank account.

"The theft can occur almost anywhere, but consumers should be particularly vigilant at gas pumps and nonbank ATMs," said Daniel J. Forte, president and CEO of the Massachusetts Bankers Association. "The good news is, if you know what to look for you can avoid such transactions, and if you do happen to be defrauded, report it as soon as you are aware of it and you will be protected by your bank."

The MBA is offering a few tips to help you avoid and detect fraud from skimming:

- * Talk to your bank about card security. Most banks already have in place security checks to monitor out-of-region use of your card. Ask about other protections.
- * It helps if you use the same ATM regularly. That way you might notice if anything looks different. When using a non-familiar ATM, or at the gas pump, keep an eye out for anything that looks suspicious, like an off-kilter or taped-on reader. Look for that tell-tale pinhole on the machine, or a new camera behind you.
- * When using the keypad, cover it up with your free hand – that's the best protection you have. (There is also another insidious and sophisticated scenario that consists of a keypad overlay to record your PIN, but that too might look like an overlay.) If you spot any of this, report it immediately to your bank or the local authorities.
- * Checking your account regularly can help tremendously. You have fraud protections in place from your financial institution but only if you report suspicious activity on a timely basis.

- * In a restaurant, ask your server if he or she can do a card transaction in front of you.
- * Ask your bank to temporarily freeze your card if you suspect that someone else other than you is making transactions and, of course, your bank can issue a new card for you.
- * If you use a debit card, ask your bank if it can put a threshold limit on your card. For example, if you have a \$1,200 limit and somebody tries to make a larger transaction the transaction would be declined.
- * Ask your financial institution for a “chip” card. If it is available, the electronic chip is more secure and cannot be as easily replicated as the traditional “mag stripe, providing a higher level of security. (The code on chip cards changes with each transaction.)

“While any one of these suggestions is a good idea, implementing them together will provide higher levels of security,” said Forte. “In addition, consumers can visit www.MassMostWanted.org to help identify ATM skimming suspects.”

The Massachusetts Bankers Association represents approximately 155 commercial, savings and co-operative banks and savings and loan associations, with 65,000 employees located in Massachusetts and elsewhere in New England.

###

Massachusetts Bankers Association, Inc.
One Washington Mall, 8th Floor
Boston, MA 02108-2603
Tel: 617-523-7595 / Fax: 617-523-6373
<http://www.massbankers.org>
Twitter: @MaBankersAssoc
Facebook.com/MassBankers



[Unsubscribe or update your email address.](#)

Massachusetts Bankers Association | One Washington Mall, 8th Floor |
Boston, MA 02108-2603

