



ATM and Debit Fraud

Contact: Sarah Grano, ABA Public Relations (202) 663-5470 or sgrano@aba.com

Thieves are increasingly targeting ATMs with skimming devices.

- Thieves rig the machine with a device that can steal a customer's card data and PIN number. The crook can then use the data to make a counterfeit card and withdraw money from the associated bank account.
- In 2015, the number of ATM compromises jumped 546 percent from 2014.¹
- Cyberthieves make at least 1.5 million illicit ATM cash withdrawals in the U.S. each year, according to consulting firm Tremont Capital Group. That figure represents a tiny fraction of the 5.8 billion ATM withdrawals consumers made in 2013, according to a Federal Reserve estimate.
- We expect the shift to more secure ATMs to tackle skimming. Soon, many ATMs will accept chip cards, which fights this type of fraud by creating a one-time code for each transaction, limiting the ability of a thief to steal and replicate data. (see Chip Payment Cards)

Banks protect consumers.

- Consumers are always protected against unauthorized fraud losses and are refunded by their bank.
- Banks take preventative measures to enhance consumer safety including installation of surveillance cameras, increased lighting and withdrawal limits.
- Banks stopped more than \$8 out of every \$10 (or 85 percent) of attempted deposit account fraud in 2014, according to ABA's 2015 Deposit Account Fraud Survey.²

Debit card fraud continues to rise.

- The banking industry lost \$1.3 billion to debit card fraud in 2014, according to ABA's 2015 Deposit Account Fraud Survey.²
- In 2014, 6 in 10 banks (60 percent) reported having check fraud losses and more than 9 in 10 banks (94 percent) reported having debit card fraud losses.²
- According to the Federal Reserve, fraud losses on debit and prepaid card transactions totaled \$2.41 billion in 2015, a 44 percent increase from 2013.³
- The Fed attributed the increase to two factors: a 28 percent increase in average fraud losses as a share of transaction value and a 12 percent increase in the value of total transactions from 2013 to 2015.³

Consumers can protect themselves by following a few simple rules.

- If an ATM looks suspicious – for instance, if it has a discolored or loose card reader or an unresponsive keypad – use another machine.
- Regularly check your monthly statement for strange withdrawals, and contact your bank immediately if you notice something suspicious.
- Never give your PIN number to anyone who does not share your account (not even family members).

ATM and Debit Fraud

(continued)

Use your hand to “shield” the ATM keypad as you enter your PIN. Often, criminals attempt to capture your PIN using a tiny camera attached to, or around, the ATM.

Consumer Tips:

To avoid becoming a victim of debit card fraud, follow these tips from the American Bankers Association:

- **Immediately notify your bank if your card is lost or stolen.**
- **If you have a reason to suspect fraud, check your account balance** right away by calling the bank, visiting your account online or through a mobile app, or at the ATM.
- **Use your hand to shield** the ATM keyboard as you enter your PIN. Often, criminals attempt to capture your PIN using a tiny camera attached to the ATM.
- **Keep your receipts** to check against your statement.
- **Keep a record of card numbers, expiration dates and 1-800 numbers** for banks so you can contact the issuing bank easily in cases of theft.
- **Mark through any blank spaces on debit receipts**, including the tip line at restaurants, so the total amount cannot be changed.
- **Know your limits.** Many issuers limit daily purchases and withdrawals for your protection.
- **Be wary of those trying to help you**, especially when an ATM “eats” your card. They may be trying to steal your card number and PIN.
- **Do not give your PIN number to anyone over the phone.** Thieves often steal cards and then call the victims for their PIN, claiming to be law enforcement or the issuing bank.
- **Always take your receipts or transaction records with you.**
- **Do not leave your ATM card lying around** the house or on your desk at work. No one should have access to the card but you.
- **Check your bank statements often.** Report unauthorized transactions immediately.

Source:

¹ATM Compromises in U.S. Jumped Six-Fold in 2015, FICO (2016). Retrieved from <http://www.fico.com/en/newsroom/atm-compromises-in-us-jumped-six-fold-in-2015-fico-reports-04-08-2016>

²ABA's 2015 Deposit Account Fraud Survey, ABA (2016). Retrieved from <http://www.aba.com/Products/Surveys/Pages/default.aspx>

³2015 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions, Federal Reserve (2016). Retrieved from https://www.federalreserve.gov/paymentsystems/files/debitfees_costs_2015.pdf