


# 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 customer's bank account.

- In 2017, the number of ATM compromises rose 8 percent, following a 30 percent increase in 2016.[1]

- The migration to EMV-enabled cards and ATMs have helped reduce skimming. More than 90 percent of U.S. ATMs are EMV capable, 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.[2] (see Chip Payment Cards)

- While the adoption of chip cards has helped reduce ATM skimming, fraudsters have resorted to new tactics – like "shimming" – to steal data. In this fraud, criminals insert a device into the ATM's card reader to intercept or manipulate the chip data.

**Banks protect consumers.**

- Consumers are always protected against unauthorized fraud losses and are refunded by their bank.

- Banks stopped $9 out of every $10 (or 89 percent) of attempted deposit account fraud in 2016, according to ABA's 2017 Deposit Account Fraud Survey.[2]

**Debit card fraud remained flat in 2016.**

- The banking industry lost $1.3 billion to debit card fraud in 2016, according to ABA's 2017 Deposit Account Fraud Survey. That's the same amount that was reported lost in 2014.[3]

**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 any 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.

- **Mark through any blank spaces on debit receipts**, including the tip line at restaurants, so the total amount cannot be changed.

# ATM and Debit Fraud

(continued)

- **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 or through texts and emails**. Thieves often steal cards and then contact 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:*

[1] *FICO Data: 10 Percent More Debit Cards Were Compromised in U.S. Last Year* (2018). Retrieved from http://www.fico.com/en/newsroom/10-percent-more-debit-cards-were-compromised-in-us-last-year

[2] *New ATMIA EMV Survey Reveals 86% Migration Rate For U.S.* (2018). Retrieved From https://www.atmia.com/news/new-atmia-emv-survey-reveals-86-migration-rate-for-us/5674/

[3] *ABA's 2017 Deposit Account Fraud Survey*, ABA (2017). Retrieved from http://www.aba.com/Products/Surveys/Pages/default.aspx