2016 ABA Issue Summary

ATM and Debit Fraud

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

Consumers should beware of "skimming" and other scams.

- Thieves have targeted some stand-alone ATMs or retailers' point-of-sale machines for "skimming" scams. They rig the "swipe" machine with a device that can capture the magnetic stripe and key pad information.
- Be wary of your surroundings and of other people who may be near you at the ATM.
- A favorite tactic of purse-snatchers and pickpockets is to call you and claim to be the police or your bank and ask for your PIN number for verification. Never give your PIN number to anyone.

Banks protect consumers.

- Consumers are always protected against unauthorized fraud losses and are refunded by their bank.
- Banks are taking preventative measures to enhance consumer safety including installation of surveillance cameras, increased lighting and withdrawal limits.
- The banking industry lost $1.3 billion to debit card fraud in 2014, according to ABA's 2015 Deposit Account Fraud Survey. [1]
- In 2014, more than 6 in 10 banks (60 percent) reported having check fraud losses and over 9 in 10 banks (94 percent) reported having debit card fraud losses.[1]

Consumers can protect themselves by following a few simple rules.

- If an ATM looks suspicious – for instance, if it has a discolored 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).

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 utilizing online banking, telephone banking, or by printing an interim statement at the ATM.
- **Use your hand to shield** the ATM keyboard as you enter your PIN.
- **Keep your receipts** to check against your statement.

ATM and Debit Fraud

(continued)

- **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:

[1] *ABA's 2015 Deposit Account Fraud Survey*, ABA (2016). Retrieved from http://www.aba.com/Products/Surveys/Pages/default.aspx