2016 ABA Issue Summary

Identity Fraud

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

Banks work diligently to protect their customers from identity theft.

- Banks use a combination of safeguards to protect your information, such as employee training, strict privacy policies, rigorous security standards and encryption systems.
- Many banks have special fraud detection software that constantly monitors accounts to help flag ID theft.

Bank customers are protected from loss.

- Most bank-related incidents of ID theft limit customer liability to $50 of unauthorized charges, and most lenders will waive that.
- Restoring your identity can be an inconvenience, so it's important to take precautions to avoid becoming a victim (see Consumer Tips below).

Customer protection is paramount for banks.

- Banks invest time and resources to ensure account and identity information is fully secured.
- In 2014, there were 12.7 million victims of identity fraud.[1]
- Total annual fraud decreased from $18 billion in 2013 to $18 billion in 2014, still significantly less than the all-time high of $48 billion reported by Javelin Strategy and Research in 2004.[1]
- Due to the zero-liability fraud protection offered by most banks and credit card companies, most victims don't experience any out-of-pocket costs.
- Businesses, consumers and law enforcement all have vital roles and responsibilities in combating ID theft. We must work together to solve the problem.

If a customer becomes a victim of ID theft, the bank is there to help.

- Once contacted, banks immediately take action by closing accounts when appropriate and beginning an investigation.
- Most banks have special toll free numbers and websites devoted to helping victims of identity theft.
- Many banks offer special worksheets, phone numbers and standardized affidavits to send to other businesses that may need to be contacted. This special affidavit is available from the Federal Trade Commission at www.ftc.gov/idtheft.

Consumer tips for victims:

- If you suspect your identity has been stolen, call your bank and credit card issuers immediately so they can start working on closing your accounts and clearing your name.
- File a police report and call the fraud unit of three credit-reporting companies (see phone numbers below).

© 2016 American Bankers Association, Washington, D.C.

Identity Fraud

(continued)

- Consider placing a victim statement in your credit report.
- Make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down names, titles, and phone numbers in case you need to re-contact them or refer to them in future correspondence.
- For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or www.ftc.gov/idtheft.

Consumer tips to avoid becoming a victim:

- Don't give your Social Security number or other personal credit information about yourself to anyone who contacts you.
- Tear up receipts, bank statements and unused credit card offers before throwing them away.
- Keep an eye out for any missing mail.
- Review your monthly accounts regularly for any unauthorized charges through the Internet, phone or ATM statements.
- Choose to do business with companies you know are reputable, particularly online. When conducting business online, make sure your browser's padlock or key icon is active, indicating a secure transaction.
- Order copies of your credit report at least once a year to ensure accuracy.
- Never give out personal financial information in an email or over the phone unless you have initiated the contact.
- When using social networking sites, never include personal contact information including birth date, email addresses, physical address, mother's maiden name or other information that could provide sensitive information to fraudsters or hints to passwords.
- Don't open email from unknown sources and use virus detection software.
- Protect your PINs (don't carry them in your wallet!) and passwords; use a combination of letters and numbers for your passwords and change them periodically.
- Report any suspected fraud to your bank and the fraud units of the three credit reporting agencies immediately.

The fraud unit numbers are:

TransUnion	(800) 680-7289
Experian	(888) 397-3742
Equifax	(800) 525-6285

Background:
Identity theft is one of the most prevalent types of fraud. Identity theft, also called "account takeover fraud" or "true name fraud," involves criminals stealing personal

© 2016 American Bankers Association, Washington, D.C.

Identity Fraud

(continued)

information about individuals and assuming their identities by applying for credit in their names. They often run up huge bills, stiff creditors and as a result, wreck victims' credit histories. Criminals steal personal information from mailboxes and dumpsters through telemarketing scams, computer hacking and paying employees in retail establishments or financial institutions to copy down information about customers. Congress declared identity theft a federal crime in 1998 by passing the Identity Theft and Assumption Deterrence Act with punishment of up to 15 years in prison.

Sources:

[1] *2015 Identity Fraud Report*, Javelin Strategy & Research (2015). Retrieved from https://www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/d,pressRoomDetail

© 2016 American Bankers Association, Washington, D.C.