



Financial Institution Fraud

Alan P. Peak

Special Agent

FBI Kansas City Division

Springfield Resident Agency



Financial Institution Fraud

Federal Jurisdiction

- Scheme to defraud
- Federally insured financial institution



Financial Institution Fraud

Common Schemes

- Misapplication and Embezzlement
- Bad Loans/Improper Lending
- Check Fraud
 - Altered Checks
 - Counterfeit Checks
- ACH Fraud
- Closed Account Fraud



Financial Institution Fraud

Credit Card Fraud

- Stolen Credit Cards
- Counterfeit Credit Cards



Financial Institution Fraud

Credit Card Fraud

- Hacking
- Skimming
- Recruiting
- Phishing



ACH Fraud

- **According to NACHA statistics, the number of ACH network payments reached 15.6 billion in 2010, worth more than \$31.7 trillion**
- **Payroll fraud is among the latest threats to ACH payments. This is generally accomplished through a combination of ACH Fraud, social engineering and computer hacking.**



ACH Fraud

- **How does ACH Fraud happen?**
 - **Generally accomplished through a targeted phishing email which tricks the victim into running malicious software, thereby installing keylogging software.**
 - **Many larger schemes use “mules” who are hired accomplices, usually through work-at-home schemes, to knowingly or unknowingly move funds to overseas accounts.**



ACH Fraud

- **Who is at risk?**
 - **FBI analysis has found in most cases, the victims' accounts are held at local community banks and credit unions, some of which use third-party service providers to process ACH transactions.**
 - **The account holders are often small to medium sized business, in addition to court systems, school districts, and other public institutions.**



ACH Fraud

- **What are some best practices to avoid ACH Fraud?**
 - **Detection is key. Consumers need to alert their institution within 60 days in order to recover funds. Businesses, however, only have as little as one business day.**
 - **ACH Blocks, ACH Filters and Positive Pay**



Identity Theft

Involves the misuse of another individual's personal identifying information for fraudulent purposes



Identity Theft

- Almost always committed to facilitate other crimes, such as credit card fraud, mortgage fraud, and check fraud
- FBI investigations reveal the majority of illicit proceeds derived from Identity Theft are used to purchase illegal drugs, pay established debt, purchase cars, real estate or furniture, for gambling or prostitution.



Identity Theft Statistics

- A survey conducted by the Federal Trade Commission (FTC) in 2006 estimated that 8.3 million American consumers, or 3.7% of the adult population, became victims of Identity Theft in 2005. The same survey determined that victim consumers spent over 200 million hours in 2005 attempting to recover from Identity Theft.
- Identity Theft losses estimated at \$15.6 billion in 2005.
- 56% of victims don't know how their information was taken. Among those who knew how their information was taken, most common was that their information was stolen by someone they personally knew.



Questions

Special Agent Alan P. Peak
Federal Bureau of Investigation
1932 W Chesterfield Blvd, Suite 200
Springfield, MO 65807
(417) 890-2452