

Identity Theft Presentation Outline  
Detective Jackelyn Weibel

- I. Identity theft
  - a. Definitions
  - b. Examples
  - c. FTC Statistics
- II. Protecting business and personal identifying information
  - a. Business information
    - i. Businesses' identifying information
    - ii. Clients' identifying information
      - 1. The law
      - 2. Ethical considerations
  - b. Personal identifying information
  - c. Importance of monitoring individual and business credit reports regularly
- III. Types of identity theft
  - a. Medical
  - b. Child
  - c. Elderly
  - d. Government
  - e. Financial
    - i. Identity theft schemes
      - 1. Skimming
      - 2. Phishing
      - 3. Pharming
      - 4. Spyware
- IV. Consumer rights for use of credit and debit cards
- V. Corporate responsibilities
  - a. The law
  - b. Ethical considerations
- VI. Business precautions
- VII. Safeguarding information
  - a. Identifying information
  - b. Client information
- VIII. What to do if you or your business becomes a victim of identity theft

# IDENTITY THEFT

Detective Jackelyn Weibel, CFE  
Allegheny County District Attorney's Office

---

---

---

---

---

---

---

▶ Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

-U.S. Department of Justice



---

---

---

---

---

---

---

- ▶ For the 12<sup>th</sup> year in a row, identity theft was the #1 consumer complaint to the FTC.
- ▶ In 2011, approximately 7% of adults in the United States were affected by identity theft.
- ▶ Each instance resulted in an average loss of \$3,500.
- ▶ Each instance averaged 25 hrs to fix. For many, it takes years to repair the damage.

---

---

---

---

---

---

---

- ▶ In 2011, over 15 million U.S. residents had their identities used fraudulently with financial losses upwards of \$50 billion.
- ▶ Close to 10 million additional Americans have had their personal identifying information placed at risk when records maintained by government or corporate databases are lost or stolen.

---

---

---

---

---

---

---

---

## Discovery

- ▶ 38-48% of victims discover their identity has been stolen within three months.
- ▶ 9-18% of victims do not discover their identity has been stolen for 4 or more years.
- ▶ Over 50 million Americans (businesses) are utilizing a credit monitoring service.
- ▶ 44% of consumers view their credit reports using [AnnualCreditReport.com](http://AnnualCreditReport.com).

---

---

---

---

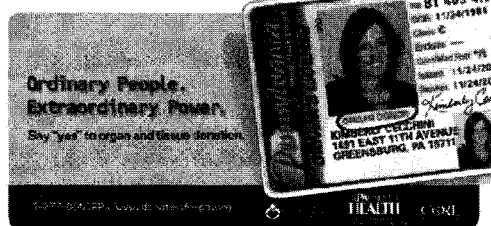
---

---

---

---

## Personal Information is Everywhere!



No way to protect personal information 100%  
 Individual information v. client information  
 Actual laws v. ethical responsibilities

---

---

---

---

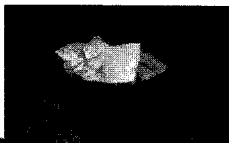
---

---

---

---

## At Work...



- › Businesses and places of employment.
- › Co-workers and visitors have easy access to information.
- › Employee training.



---

---

---

---

---

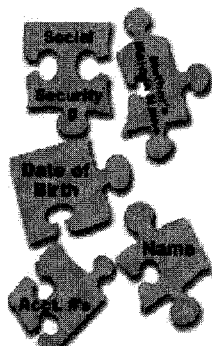
---

---

---

## Types of Identity Theft

- › Medical identity theft
- › Child identity theft
- › Senior identity theft
- › Government identity theft
- › Financial identity theft



---

---

---

---

---

---

---

---

## Medical Identity Theft

- › 25,000 Americans are victims of medical identity theft each year.
- › The most difficult identity theft to detect.
- › Thieves steal identities for the purpose of receiving free medical care and as a result create a false medical record for the victim.
- › Consequences include:
  - ✓ Incorrect treatment for victims;
  - ✓ False health insurance claims filed;
  - ✓ Denial of legitimate medical claims.

---

---

---

---

---

---

---

---

## Child Identity Theft

- ▶ Perpetrator may be family member or someone known to the family.
- ▶ Targets children because of the length of time it takes to discover the theft.
- ▶ Children were targeted by scammers 35 times more often than adults, with 15% of the victims under the age of five.




---

---

---

---

---

---

---

---

## Senior Identity Theft

- ▶ In 2010, reports of identity theft targeting people 50 and older represented about 28 percent of the total 236,765 cases.

Senior Citizens more susceptible to acts of deception and manipulation.

- ▶ They have worked diligently their whole life to achieve good credit.

They rarely check their credit reports.

---

---

---

---

---

---

---

---

## Government Identity Theft

- ▶ Stealing personal information to obtain government assistance such as:
  - Social Security retirement or disability
  - Medical insurance or welfare benefits.



- ▶ Stealing personal information to fraudulent income tax returns to receive refundable credits such as earned income or child tax credits. (Always paid by debit card.)

- ▶ Billions of taxpayer dollars are wasted each year on fraudulent tax refunds!

---

---

---

---

---

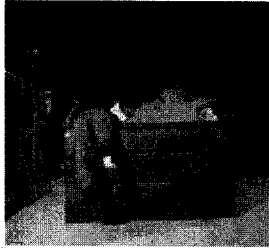
---

---

---

## Financial Identity Theft

- ▶ Individuals or businesses can be affected.
- ▶ Personal identifying information everywhere!
- ▶ Billion dollar business.
- ▶ Most common form of identity theft!




---

---

---

---

---

---

---

---

## WHO IS STEALING YOUR IDENTITY?

- ▶ Retail Merchants and Their Employees
- ▶ Restaurant Employees
- ▶ Bank Employees
- ▶ Drug Abusers
- ▶ Terrorist Groups
- ▶ Organized Crime Members
- ▶ Illegal Immigrants
- ▶ Your Family Members
- ▶ Your Co-Workers
- ▶ Your Employees
- ▶ Neighbors




---

---

---

---

---

---

---

---

## WHERE IS YOUR IDENTITY STOLEN?

- ▶ Your mailbox
- ▶ Retailers
- ▶ Restaurants
- ▶ Hospital or health care facilities
- ▶ Discarded/stolen computers
- ▶ Internet
- ▶ Your motor vehicle
- ▶ ATM machines
- ▶ On the telephone
- ▶ Your place of employment
  - Certifications or licenses on walls
  - Personal information in desk / cubicle
  - By employees acting as accomplices




---

---

---

---

---

---

---

---

### WHY IS YOUR IDENTITY STOLEN?

- ▶ Financial gain.
  - Money
  - Assets
  - Good credit rating
- ▶ Obtain a better life, history or job
  - Hide from criminal past
  - Stay in country
  - Desire for better social status-keep up with Joneses
- ▶ Revenge, cause malicious harm.
- ▶ Domestic reasons.
- ▶ Addictions to vice.

---

---

---

---

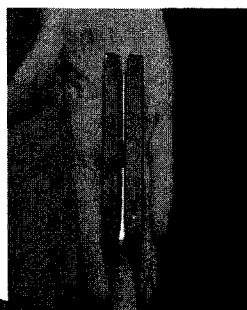
---

---

---

---

### HOW IS YOUR IDENTITY STOLEN?



- ▶ Theft of your trash ("Dumpster Diving")
- ▶ Purse or wallet theft
- ▶ Dishonest employees
- ▶ Public Records
- ▶ Shoulder surfing
- ▶ "Pharming"
- ▶ "Phishing"
- ▶ Skimming devices
- ▶ Counterfeit documents
- ▶ eBay & Craigslist scams

---

---

---

---

---

---

---

---

### Identity Theft Schemes

- ▶ Database Hacking
- ▶ Social Engineering
- ▶ Dumpster Diving
- ▶ Skimming
- ▶ "Spam"- Spyware
- ▶ Dishonest Employee
- ▶ Pharming
- ▶ Phishing
- ▶ Counterfeit Cards/Checks



---

---

---

---

---

---

---

---

## UNKNOWN EMAILS

- ▶ Also known as "SPAM".
- ▶ Could launch hackers software (Spyware).
- ▶ Could cause victim to respond to fraud scheme (i.e. "Phishing").
- ▶ Could cause victim to give up personal info when making a "purchase".
- ▶ Best practice is to delete unknown or suspicious looking emails.

---

---

---

---

---

---

---

---

## Example of an Unknown Email



**Attention! New self-spreading virus!**

Be careful, a new self-spreading virus called "RTSW.Smash" spreading very fast via e-mail and LAN networks. It's about two million people infected and it will be more.  
 To avoid your infection by this virus and to stop it, we provide you with full information how to protect yourself against it and also including free remover. You can find it in the attachment.  
 © 2004 Networks Associates Technology, Inc. All Rights Reserved

Opening this file will  
 launch illicit program




---

---

---

---

---

---

---

---

## "PHARMING"

- ▶ Computer hacker using a malicious code acquires domain or host name information for a legitimate website and then redirects traffic to another identical looking (bogus) website.
- ▶ Usually banking or retail websites.
- ▶ Most often used to steal passwords, PIN numbers or bank information.

---

---

---

---

---

---

---

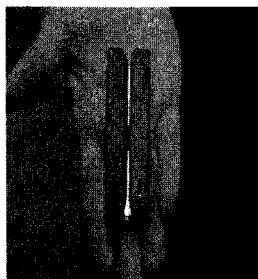
---







# SKIMMING



- ▶ Suspect uses a "wedge" to store information contained on credit card strip.
- ▶ Downloads info later to computer.
- ▶ Uses info to create counterfeit cards with your personal information.

---

---

---

---

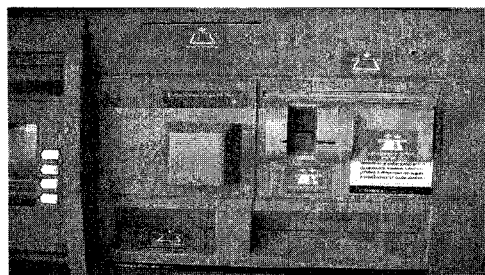
---

---

---

---

## Standard ATM machine?



---

---

---

---

---

---

---

---



False front is attached to ATM with card reader >>> to copy magnetic strip info on your card

---

---

---

---

---

---

---

---



Look at the pamphlet holder on the left >>

---

---

---

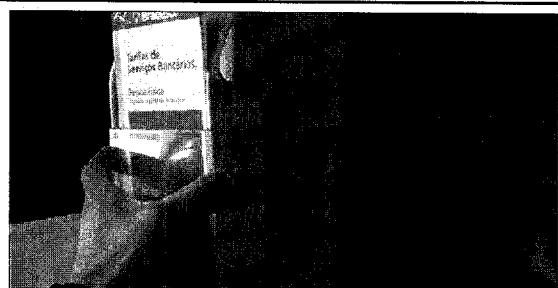
---

---

---

---

---



Note the hole in the side >>

---

---

---

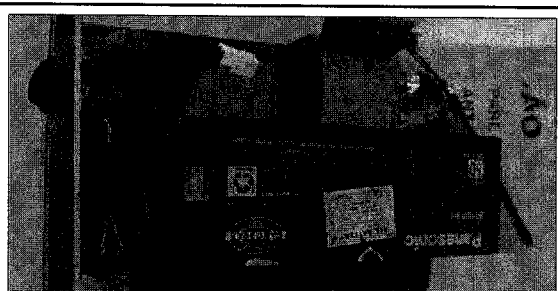
---

---

---

---

---



Camera/transmitter housed inside >>

---

---

---

---

---

---

---

---

Camera can view keypad and monitor and send wireless picture up to 200 meters.



---

---

---

---

---

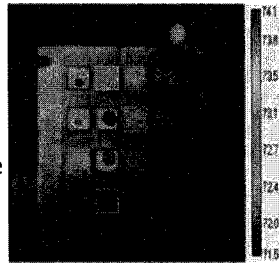
---

---

---

### Digital Robbery Thermal Imaging Allows ATM Theft From a Distance

- ▶ ATM pins can be stolen using a thermal imaging camera.
- ▶ When ATM users press keys to enter their PIN, they leave behind a residual heat from their fingers.



---

---

---

---

---

---

---

---

### “ TOOLS OF THE TRADE ”



---

---

---


---

---

---

---

---



**Consumers' Rights for Unauthorized Debit and Credit Card Use**

---

---

---

---


---

---

---

---

- ▶ Fair Credit Reporting Act (FCRA) governs consumers' right for fraudulent use of credit cards.
- ▶ Electronic Funds Transfer Act (EFTA) governs consumers' right for fraudulent use of debit cards.
- ▶ Consumer protection is stronger for credit cards:  
 Charge-back rights;  
 Credit dispute rights;  
 Credit line available now.




---

---

---

---

---

---

---

---

**Debit and Credit Cards Not Equal**

<p><u>Debit Cards:</u>          If you report within 2 days of discovery, loss is limited to \$50;</p> <p>If you report between 3 - 60 days, loss limited to \$500;</p> <p>After 60 days, no protection for fraudulent use of card!</p>	<p><u>Credit Cards:</u>          Regardless of report date, loss is limited to \$50.</p> <p>If credit card company has a zero liability policy, you still must report losses within 60 days of the fraudulent charges.</p>
---	--

---

---

---

---

---

---

---

---

### Business Precautions

- ▶ Positive Pay bank feature.
- ▶ Dual signature requirement on checks.
- ▶ No signature stamp.
- ▶ Review bank statements and credit card statements monthly.
- ▶ Separation of accounting duties.
- ▶ Regular employee (ethics) training.
- ▶ Anti-virus software on computers (cellphones).
- ▶ Check business credit reports regularly.
- ▶ Consider business credit monitoring.

---

---

---

---

---

---

---

---

### Corporate Responsibility

- ▶ Businesses maintain personal identifying information for clients and employees.
- ▶ Information kept in writing and on databases.
- ▶ Many cases of employees stealing this information to sell for profit or for this personal gain.
- ▶ Hackers often gain access to databases.
- ▶ Businesses have a responsibility to notify law enforcement and FTC if they are aware that any personal identifying information could have been compromised

---

---

---

---

---

---

---

---

### Safeguarding Information

- ▶ Keep only what personal information is necessary.
- ▶ Conduct background checks on all potential employees.
- ▶ Shred sensitive material.
- ▶ Utilize anti-virus software.
- ▶ Limit access of sensitive information.
- ▶ Regularly educate and train employees on security issues.
- ▶ Require strong passwords.
- ▶ Have a plan to respond to security incidents.

---

---

---

---

---

---

---

---

- ▶ Promptly remove mail from mailbox and deposit outgoing mail in secure receptacles.
- ▶ Empty your purse/wallet of extra credit or ID cards including your social security card.
- ▶ Make a list/copy of all items in your wallet and keep in secure location.
- ▶ Examine all credit card and bank statements each month.
- ▶ Do not respond to unknown or "phishing" emails.
- ▶ Report loss or stolen cards.




---

---

---

---

---

---

---

---

- ▶ Make inquiries on unexpected bills.
- ▶ If providing financial information over the Internet, ensure the information is encrypted and the site is secure (https:)
- ▶ Never give out personal information over the phone.
- ▶ Always shield your hand and the screen when using the ATM machine, even if no one is around.
- ▶ Consider placing a fraud alert on your account with all three major credit bureaus.
- ▶ Never leave transaction receipts behind.
- ▶ Order and review your credit report once a year ([www.annualcreditreport.com](http://www.annualcreditreport.com))

---

---

---

---

---

---

---

---

**IF YOU BECOME A VICTIM:**

- ▶ Get organized and keep written detailed records in a notebook (company, date, time)
- ▶ If business, make one person responsible for contacting creditors and handling issues .
- ▶ Dispute and close all fraudulent accounts that were opened by notifying credited by phone and in writing. Keep copies of all letters mailed.
- ▶ Seek support from family & friends
- ▶ It may take weeks or months to fix the problem!!!




---

---

---

---

---

---

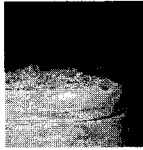
---

---



### IMPORTANT CONTACTS

- ▶ Equifax.....1-800-525-6285
- ▶ Experian..... 1-888-397-3742
- ▶ Transunion.....1-800-680-7289
- ▶ FTC..... 1-877-FTC-HELP  
www.ftc.gov
- ▶ IFCC.....www.ifccfbi.gov
  - For victims of fraud on the Internet



---

---

---

---

---

---

---

---

### REMEMBER . . .

- ▶ Alertness, common sense and good judgment will greatly reduce your risk of becoming a victim of identity theft.
- ▶ Monitor your credit reports regularly.
- ▶ Utilize good anti-virus software.
- ▶ If something sounds too good to be true, it is!

---

---

---

---

---

---

---

---

## Questions???

---

---

---

---

---

---

---

---

Detective Jackelyn Weibel  
Allegheny County District Attorney's Office  
1444 Hillside Avenue  
Pittsburgh, PA 15216  
(412) 388-5300  
Jweibel@da.allegheny.pa.us

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---