Identity Theft Trends and Prevention

Greg Munson, CISSP, CISM
Senior VP, Citigroup Information Security
A Winning Hand: Solutions, Savings and Sustainability with GSA SmartPay

The 13th Annual GSA SmartPay Training Conference, Las Vegas
Identity Theft Trends and Prevention

House Rules

To ensure the best possible learning experience for participants, please adhere to the following house rules:

• Turn cell phones and pagers to vibrate
• Hold questions to end of session
• Ensure your participant badge is scanned to receive CLP credits
  − For each course
  − Must leave room and re-enter
• Take advantage of opportunities to provide feedback
  − Please select the Citi Q&A icon on any Citi PC at the conference
  − Answers to be e-mailed after the conference within 60 days
Identity Theft Trends and Prevention

Goals & Objectives

This course is designed to assist you in achieving the following objectives:

• Defining What Is Meant by “Identity”
• Detecting Identity Theft
• Preventing Identity Theft
• Understanding Current Trends
Identity Theft Trends and Prevention

Agenda

- Overview of Identity Theft
- Techniques
- Key Trends
- Preventing Identity Theft
1. Overview of Identity Theft
Identity Theft Trends and Prevention

What is Your Identity?

I Know Who I Am. Do You?

• **Official Identity**: Defined by the state
  - Driver's License, Passport, Birth Certificate, Social Security Number, etc.
  - Unique; can only be altered by state authority

• **Digital Identity**: Defined by You
  - Personal – Facebook Profile
  - Professional – LinkedIn Profile
  - Location – Global Positioning System (GPS)
  - Online – e-mail address(es)
  - Not unique; can be altered by you

• **Summary**: Your **Official Identity** is designed to exert state control over what you do, who you are, or where you go. **Digital Identity** is designed primarily to sell “you” something
Identity Theft Trends and Prevention

Overview

What is identity theft?

- Current federal law defines identity theft as a federal crime when someone knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.
- Translation: When a criminal has enough of your personal information to impersonate you, to commit fraud with existing accounts or to open and use new accounts in your name.
Identity Theft Trends and Prevention

Overview

How big is the problem?

• The Federal Trade Commission estimates that 9 to 10 million American identities are stolen every year
• The average time spent by victims resolving a problem is about 330 hours
• Individual costs range from $30 to thousands of dollars
• Corporate costs are not clear but can be in the thousands of dollars per record

Identity theft ring busted in New York

“Using financial information purchased from crooked bank insiders, a ring of thieves compromised the checking accounts of nearly 350 New York-based corporations, religious institutions, hospitals and schools, as well as city and state government agencies, to steal millions of dollars.”

Source: SC Magazine
Identity Theft Trends and Prevention

Overview

Why do identity thieves want your information?

Identity theft remains a low-risk, high-reward crime, and not every motive is financial. Credit card fraud is still one of the most common forms of identity theft. The general types and motives of identity theft include:

- **Commercial**: Using a business name to obtain credit or steal phone/utilities services
- **Criminal**: To hide or disguise criminal activity
- **Financial**: To obtain goods and services or to launder money
- **Identity cloning**: Completely assuming someone else’s identity (especially for illegal immigration purposes or terrorism)
- **Medical**: Using stolen information to obtain medical care or drugs
Identity Theft Trends and Prevention

Overview

But identity theft is more of a problem for the banks, right?

Wrong. Consider the story of Michelle Brown, a victim of identity fraud who testified before a US Senate Committee Hearing on Identity Theft.

“Over a year and a half from January 1998 through July 1999, one individual impersonated me to procure over $50,000 in goods and services. Not only did she damage my credit, but she escalated her crimes to a level that I never truly expected: She engaged in drug trafficking. The crime resulted in my erroneous arrest record, a warrant out for my arrest, and eventually, a prison record when she was booked under my name as an inmate in the Chicago Federal Prison.”
Identity Theft Trends and Prevention

2. Techniques
Identity Theft Trends and Prevention

Techniques

How does identity theft commonly occur?

**Low-tech attacks:**
- Dumpster diving
- Stolen wallets/purses

**“Middle-tech” attacks:**
- Phishing, social engineering, bought and sold in black markets
- Trojan horse and zombie software from Internet attacks take control of your PC

**High-tech attacks:**
- ATM skimming, discarded hard drives, hacking, Radio Frequency Identification Devices (RFID)

And don’t forget accidental data disclosures by companies…
Identity Theft Trends and Prevention

Techniques

Would you have spotted this ATM skimming device?

The real card reader slot. The capture device

The side cut out is not visible when on the ATM.
3. Key Trends
Identity Theft Trends and Prevention

Trends

**Trend 1:** Ever-Increasing Regulation and Litigation
- ID Theft “Red Flag” rules
- Data breach disclosure rules: Are they helping?

**Trend 2:** The Business Side of Identity Theft
- Organized crime goes corporate

**Trend 3:** More Sophisticated Attacks
- Creative attacks

**Trend 4:** Social Media Is the New Privacy Sieve
- Giving away too much information
Identity Theft Trends and Prevention

Trends

Trend 1: Ever-Increasing Regulation and Litigation

The ID Theft “Red Flags” Rules

- Sponsored by the Federal Trade Commission. The act was passed in January 2008, active enforcement began June 1, 2010
- Requires creditors and financial institutions to implement identity theft prevention programs
- Requires institutions to identify and detect behaviors that could indicate identity theft
- Requires a response and mitigation to identity theft threats
- Sets a requirement to update the identity theft prevention program periodically
- Long-term effectiveness of this program is TBD
Trend 1: Ever-Increasing Regulation and Litigation (continued)

Plenty of Data Breach Disclosure Rules

• Almost every state has their own data breach notification laws
• Federal legislation is pending
• But are these laws helping? Not according to a 2008 Carnegie Mellon study:

“We find only a marginal effect of law. We estimate that the passage of law has reduced identity theft rate by about 2%.”

“Do Data Breach Disclosure Laws Reduce Identity Theft?”
Sasha Romanosky, Rahul Telang, Alessandro Acquisti
Heinz School of Public Policy and Management, Carnegie Mellon University
Identity Theft Trends and Prevention

Trend 2: The Business Side of Identity Theft

• Bulk ID theft is a multi-billion-dollar business but risk is also increasing for the criminals
• Stolen identities have become commodities that are bought and sold in covert marketplaces, resulting in a glut of data
• Officer titles and business-style hierarchies have developed
• According to the Verizon 2009 Data Breach Investigations Report: The value associated with selling stolen credit card information dropped from between $10 and $16 per record in mid-2007 to less than $0.50 per record today
• But the top underground product is the “full info card,” including name, passport, Social Security number, credit cards, date of birth and mother’s maiden name. Price for this package can reach $1,000
Trend 3: More Sophisticated Attacks

• ID theft rings are international
• Closing a financial account isn’t always enough
• Sophisticated attack tools: Zeus, Private Banker
• Multifactor authentication defense only raises the bar
• Even phishing attacks have become more sophisticated
  — “Spear phishing”
  — Whaling
  — SMiShing and Vishing
Identity Theft Trends and Prevention

Trends

Trend 4: Social Media Is the New Privacy Sieve

• Users volunteer too much information (vacations schedules, GPS locations)
• Twitter & Facebook leak more information about you than you think
• Adjusting privacy settings does not always work as advertised
• Fake user identities are being used to trick users into giving up even more information
• Rogue Facebook “widgets” like Secret Crush can introduce spyware
• Malware like the koobface virus can take over your account
• Social media tools are vulnerable to phishing attacks
• Twitter-style shortened web links like Bit.ly and TinyURL can disguise malware sites
Identity Theft Trends and Prevention

4. Preventing Identity Theft
Identity Theft Trends and Prevention

ID Theft Prevention Tips

Ten ways to safeguard your identity

1. Regularly review billing statements and credit reports
2. Use a crosscut shredder on ALL financial documents
3. Be cautious on the Internet
4. Use strong passwords and change them often, do not write them down
5. Watch for “Skimmers” at ATMs and other points of sale
6. Keep an inventory of important cards, numbers, contacts
7. Don’t store sensitive information on PC Drives, PDAs, etc.
8. Use fraud alerts and credit freezes
9. Keep track of your credit card in restaurants and retail stores
10. Protect your personal information (Social Security #, etc.)

* Fact: Most victims of ID theft have no idea *how* their information was stolen
Identity Theft Trends and Prevention

ID Theft Prevention Tips

What information is considered “sensitive”?

- Social Security Numbers
- Bank account or credit card numbers
- Mother’s maiden name
- Driver’s license number
- Insurance policy numbers (medical and auto)
- Date of birth
- State or employee identification number
- Passwords and Personal Identification Numbers (PINS)
- Sometimes even simple information like home address…
What else can I do to protect myself?

- Sign up for proactive credit and/or Identity monitoring services
- Run anti-spyware and anti-virus protection on your computer
- Keep personal computers, laptops and any electronic devices that can access the internet or wireless communication networks patched and up-to-date
- Use a single credit card online and monitor statements carefully
- Don’t forget your traditional home mailbox
- Be aware of the latest scams, but also use your common sense:
  - You did not win a lottery you never entered
  - Some rich guy overseas does not need your help “moving” money
  - Credit card companies do not “verify” your information via email
Identity Theft Trends and Prevention

ID Theft Prevention Tips

What should I do if I have a problem…

• Citi Identity Theft provides free assistance 24 X 7 for Citi bank or credit card customers who suspect they may be victims of identity theft.

• If you suspect your PC or laptop has been compromised, bring to an authorized vendor to debug and restore your key files, applications and operating system.

• For any suspicious transactions, immediately contact bank, credit card, or the business and express your concerns in order to minimize your potential financial liability. Make sure you maintain a record of this contact.
Identity Theft Trends and Prevention

ID Theft Prevention Tips

Citi Identity Theft:


Citi Identity Monitor:

Identity Theft Trends and Prevention

ID Theft Prevention Tips

Summary: Remember These Three Things

- When browsing the Internet, “If you Didn’t Pick It, Don’t Click It”
- Do not send any personal or financial information via email
- Monitor your financial activities on a regular basis – at least monthly
Identity Theft Trends and Prevention

Greg Munson

All Audiences
Thank you for attending!

Visit the Citibank Welcome Center
- Level 3 Foyer – West
- National Industries for the Blind will have a display of products
- Conference Slide Show – come see yourself shine!

Visit the Citibank One-on-One Lab – Lido Room 3101 A/B

Visit the Citibank Mini Sessions – Lido Room 3001 A/B

Citi Q&A Link – Tell us your thoughts
Identity Theft Trends and Prevention

Schedules available at the Welcome Center

2011 Track Schedule Brochures
Identity Theft Trends and Prevention

Interactive Training Events – DoD

Citi offers on-site training at no cost for agencies meeting the required minimum participant level of 20 or more as set forth in the GSA SmartPay2 Master Contract.

- Regional Citi Training Locations
  - Norfolk, VA
  - Washington, DC
  - Visit [www.defensetravel.dod.mil/passport](http://www.defensetravel.dod.mil/passport) to view and register for these sessions

- Upcoming Training
  - Visit [www.defensetravel.dod.mil/passport](http://www.defensetravel.dod.mil/passport) to view and register for these sessions

- On-site at your base or installation
  - 20-participant minimum
  - Visit [www.citimanager.com/dodhome](http://www.citimanager.com/dodhome) and under Resources to download the On-site Training Request Form

- Distance Learning – Video Conferences

Please e-mail us at CommCard.Training@citi.com and a Citi training coordinator will work with you directly for on-site or Distance Learning sessions.
Citi offers Computer Based Training (CBT) via the Citi Commercial Card Learning and System Support (CLASS) in CitiManager.

- Visit [home.cards.citidirect.com](http://home.cards.citidirect.com) and from the Web Tools tab select the CLASS link.

Please contact your Account or Client Manager if you are interested in setting up a training session. Training can be conducted at a Citi Training Location, on-site at your office or via the Web.

- Regional Citi Training Locations
  - Norfolk, VA
  - Washington, DC
I. Terms & Disclosures

IRS Circular 230 Disclosure: Citigroup Inc. and its affiliates do not provide tax or legal advice. Any discussion of tax matters in these materials (i) is not intended or written to be used, and cannot be used or relied upon, by you for the purpose of avoiding any tax penalties and (ii) may have been written in connection with the "promotion or marketing" of any transaction contemplated hereby ("Transaction"). Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor.

Any terms set forth herein are intended for discussion purposes only and are subject to the final terms as set forth in separate definitive written agreements. This presentation is not a commitment to lend, syndicate a financing, underwrite or purchase securities, or commit capital nor does it obligate us to enter into such a commitment. Nor are we acting in any other capacity as a fiduciary to you. By accepting this presentation, subject to applicable law or regulation, you agree to keep confidential the existence of and proposed terms for any Transaction.

Prior to entering into any Transaction, you should determine, without reliance upon us or our affiliates, the economic risks and merits (and independently determine that you are able to assume these risks) as well as the legal, tax and accounting characterizations and consequences of any such Transaction. In this regard, by accepting this presentation, you acknowledge that (a) we are not in the business of providing (and you are not relying on us for) legal, tax or accounting advice, (b) there may be legal, tax or accounting risks associated with any Transaction, (c) you should receive (and rely on) separate and qualified legal, tax and accounting advice and (d) you should apprise senior management in your organization as to such legal, tax and accounting advice (and any risks associated with any Transaction) and our disclaimer as to these matters. By acceptance of these materials, you and we hereby agree that from the commencement of discussions with respect to any Transaction, and notwithstanding any other provision in this presentation, we hereby confirm that no participant in any Transaction shall be limited from disclosing the US tax treatment or US tax structure of such Transaction.

We are required to obtain, verify and record certain information that identifies each entity that enters into a formal business relationship with us. We will ask for your complete name, street address, and taxpayer ID number. We may also request corporate formation documents, or other forms of identification, to verify information provided.

Any prices or levels contained herein are preliminary and indicative only and do not represent bids or offers. These indications are provided solely for your information and consideration, are subject to change at any time without notice and are not intended as a solicitation with respect to the purchase or sale of any instrument. The information contained in this presentation may include results of analyses from a quantitative model that represent potential future events that may or may not be realized, and is not a complete analysis of every material fact representing any product. Any estimates included herein constitute our judgment as of the date hereof and are subject to change without any notice. We and/or our affiliates may make a market in these instruments for our customers and for our own account. Accordingly, we may have a position in any such instrument at any time.

Although this material may contain publicly available information about Citi corporate bond research, fixed income strategy or economic and market analysis, Citi policy (i) prohibits employees from offering, directly or indirectly, a favorable or negative research opinion or offering to change an opinion as consideration or inducement for the receipt of business or for compensation and (ii) prohibits analysts from being compensated for specific recommendations or views contained in research reports. So as to reduce the potential for conflicts of interest, as well as to reduce any appearance of conflicts of interest, Citi has enacted policies and procedures designed to limit communications between its investment banking and research personnel to specifically prescribed circumstances.

© 2011 Citibank, N.A. All rights reserved. Citibank, Arc Design, CitiDirect, CitiManager, Citibank Custom Reporting System, and Citibank Electronic Reporting System, are trademarks and service marks of Citigroup Inc. or its affiliates and are used and registered throughout the world.

In January 2007, Citi released a Climate Change Position Statement, the first US financial institution to do so. As a sustainability leader in the financial sector, Citi has taken concrete steps to address this important issue of climate change by: (a) targeting $50 billion over 10 years to address global climate change: includes significant increases in investment and financing of alternative energy, clean technology, and other carbon-emission-reduction activities; (b) committing to reduce GHG emissions of all Citi owned and leased properties around the world by 10% by 2011; (c) purchasing more than 52,000 MWh of green (carbon neutral) power for our operations in 2006; (d) creating Sustainable Development Investments (SDI) that makes private equity investments in renewable energy and clean technologies; (e) providing lending and investing services to clients for renewable energy development and projects; (f) producing equity research related to climate issues that helps to inform investors on risks and opportunities associated with the issue; and (g) engaging with a broad range of stakeholders on the issue of climate change to help advance understanding and solutions.

Citi works with its clients in greenhouse-gas-intensive industries to evaluate emerging risks from climate change and, where appropriate, to mitigate those risks.