2012 GSA SmartPay Conference
“Fine Tune Your Payments Program with GSA SmartPay”
Identity Theft Trends and Prevention

House Rules

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

• Turn electronic devices to vibrate
• No video-taping or audio recording is allowed
• Hold questions to end of session
• Ensure your participant badge is scanned to receive CLP credits
  - For each course
• 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

Schedules Available at the Welcome Center

2012 Track Schedule Brochures
Identity Theft Trends and Prevention

Reminders

- Visit the Citibank Welcome Center—Governor’s Lobby
- Visit the Citibank One-on-One Lab—Governor’s Chambers D&E
- Citi Q&A Link—Tell us your thoughts
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) 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.
Identity Theft Trends and Prevention

Interactive Training Events–GSA

Citi offers Computer-Based Training (CBT) via the Citi Commercial Card Learning and System Support (CLASS) in CitiManager.

- Visit **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
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

1. Overview of Identity Theft
2. Techniques
3. Key Trends
4. Preventing Identity Theft
1. Overview of Identity Theft
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, generally by determining what you purchase, where you shop digitally or simply things you “like”
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 (continued)

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 estimates are $7.2MM per data breach and $214 per compromised 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
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
- **Political**: Organized “hacktivists” use identity information to gain access to sensitive organizations or post confidential documents
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 or “cross-swiping” credit card during a valid transaction

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

High-tech attacks:
- ATM/card reader 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 (continued)

Would you have spotted these skimming devices?

The real card reader slot.

The capture device.

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

3. Key Trends
Identity Theft Trends and Prevention

Trends 2012

Trend 1: Web-Based Vulnerabilities and Attacks on the Rise
• Increased sophistication, availability and lower cost of attack automation

Trend 2: Rise of Mobile Computing and Apple/Mac Vulnerabilities
• Malware? We have an App for That!
• Mobile Computing and i-devices

Trend 3: Social Media Is the New Privacy Sieve
• Giving away too much information
• Rise in “spearfishing”—targeted attacks

Trend 4: Rise in “Political“ Cyber Crime and Recent Successes
• The rise of “hacktivists”: LulzSec, Anonymous, Wikileaks
• The fall of fake antivirus
• Spam reduction
• Successful prosecution of major offenders
Trend 1: Web-Based Vulnerabilities and Attacks on the Rise

- According to Sophos Labs 2012 Security Threat Report, more than 30,000 websites are infected every day (a 50% increase from 2011) and 80% of those infected sites are legitimate. Eighty-five percent of all malware, including viruses, worms, spyware, adware and Trojans, comes from the web. Today, drive-by downloads have become the top web threat, and in 2011 we saw one drive-by malware, Blackhole, rise to number one. Blackhole is a crimeware kit that provides sophisticated coding to corrupt legitimate websites in order to distribute malware.

- Cybercriminals constantly launch attacks designed to penetrate your digital defenses and steal sensitive data. And almost no online portal is immune to threat or harm. The most recent development is the introduction of Polymorph malware—malware that can “reinvent” itself after each use to prevent detection by AV.
Identity Theft Trends and Prevention

Trends 2012 (continued)

Trend 1: Web Vulnerabilities and Attacks—How Do They Work?

Here are just a few of the techniques cybercriminals commonly use to distribute malware on the web:

- Social engineered click-jacking tricks users into clicking on innocent-looking webpages
- Spearphishing sites mimic legitimate institutions, such as banks, in an attempt to steal account login credentials
- Malvertising embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites
- Compromised legitimate websites host embedded malware that spreads to unsuspecting visitors
- Drive-by downloads exploit flaws in browser software to install malware just by visiting a webpage

Malicious code typically installs spyware or malware by exploiting known vulnerabilities in your browser or associated plug-ins. These malware threats include:

- Fake antivirus to extort money from the victim
- Keyloggers to capture personal information and account passwords for identity or financial theft
- Botnet software to subvert the system into silently joining a network that distributes spam, hosts illegal content or serves malware
Identity Theft Trends and Prevention

Trends 2012–Rise of Mobile Computing

How did we get here?

1st cell phone call 1973
1st person-to-person SMS message 1993
1st Internet use on a cell phone 1999
1st Windows tablet PC launched 2001
1st BlackBerry launched 2002
1st iPhone launched 2007
1st Android OS launched 2008

20 years between 1st cell phone call and 1st SMS
6 years between 1st SMS and 1st Internet use on a cell phone
1 year between 1st iPhone and 1st Android OS
Identity Theft Trends and Prevention

Trends 2012 (continued)

Trend 2: Rise of Mobile Computing and Apple/Mac Vulnerabilities

- Mobile computing—clients demand mobile banking, point of sale, check processing and other financial capabilities on their i-devices, Smartphones and tablets

- 1.6 billion mobile devices sold in 2010—increase of 72%

- According to 2012 Sophos Security Threat Report:
  - 87% of users unaware that smartphones can transmit confidential payment information such as credit card details without the user being prompted
  - 67% do not use keypad locks or passwords
  - 65% worry more about security on their laptop or desktop PC than their mobile device
Identity Theft Trends and Prevention

Trends 2012 (continued)

The rise of Mac malware

- In 2011, the emergence of malware for the Mac upstaged Windows malware. There’s no doubt that the Windows malware problem is much larger than the Mac threat, but the events of 2011 show Mac users that the malware threat is genuine. Fake antivirus schemes such as MacDefender, Mac Security, MacProtector and MacGuard all came to light this year, and we’re seeing scammers use techniques such as fake antivirus and SEO poisoning to infect Macs, as they’ve been doing for years with Windows.

- History of Mac Malware 2006 - 2011
  - 2006 Leap, the first virus for Mac OS X
  - 2007 OpenOffice, BadBunny and RSPlug financial malware
  - 2008 Fake antivirus, backdoors and Jahlav
  - 2009 Apple releases rudimentary virus protection
  - 2010 Backdoors, cross-platform attacks and free antivirus
  - 2011 MacDefender fake antivirus and SEO poisoning
Trend 3: Social Media Is the New Privacy Sieve

- Users volunteer too much information (vacation schedules, GPS locations)
- Twitter, Facebook, YouTube, LinkedIn, Google, leak more information about you than you think—“likejacking”
- 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
- Social media tools are vulnerable to phishing attacks
- Twitter-style shortened web links like Bit.ly and TinyURL can disguise malware sites
- A major source of information used in “spearfishing” and “whaling”
Identity Theft Trends and Prevention

Trends 2012 (continued)

Trend 3: Social Media Is the New Privacy Sieve (continued)

How it enables targeted attacks

- Cybercriminal uses Identity information, including professional associations, corporate title, personal tastes and habits, friends and “linked” Internet accounts from various social media in order to customize a social engineering attack that appears genuine.
- Attack is generally in the form of an e-mail, an attached file or more recently, an online survey with attached offer.
- Often the attack may simply be used to gather additional information to move “up the ladder” to a “whale” (CEO, Department Chairman, Senator/Congressman, etc.).
- According to Cisco, spearfishing is 40 times more effective than mass attacks. Losses in 2011 are estimated at $150MM, triple that of 2010.
- Activity has increased 650% in the period 2006 - 2010.
Identity Theft Trends and Prevention

Trends 2012 (continued)

Trend 4: Rise in “Political“ Cyber Crime and Recent Successes

• LulzSec and Anonymous sowed chaos by leaking documents and attacking websites

• LulzSec successfully targeted attacks on RSA (major security and cyber key provider), Lockheed Martin, Sony, PBS, the US Senate, CIA, FBI affiliate InfraGuard and others. DNS attack affected 77 million Sony Playstation users.

• Cyber criminals are becoming more professionalized through the availability of commercial crimeware kits.

• Increasingly, data breaches of political and sensitive data and denial of service attacks are more common than financial information breaches (except in the mobile space) as banks develop better protections—Multi-Factor Authentication, PSI standards, Red Hat regulations and other sophisticated prevention and detection tools.

• Decentralized hacker groups can be reduced but are difficult to eliminate.
Identity Theft Trends and Prevention

Trends 2012 (continued)

Trend 4: Recent Successes (continued)

• Increased user awareness has reduced “fake anti-virus” success, as well as the June 2011 FBI arrest of a cybergang responsible for tricksing nearly 1 million individuals into purchases of $72MM in “fake” AV. Fake AV still represents 5.5% of all infections in 2011

• Google removed over 100 malicious apps from the Android market in 2011. However, in a one-day span before the removal, over 10,000 malware apps were downloaded

• In March 2011, Operationb107 knocked out major global spammer Rustock (known for viagra and pharmaceutical spams). Result was a 30% drop in global spam

• Additional 20% drop in spam due to September 2010 closure of underground spamming network Spamit.com
Identity Theft Trends and Prevention

4. Preventing Identity Theft
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…
Identity Theft Trends and Prevention

Identity Theft Prevention—Protect Yourself at All Times

- **Awareness**—Where are you vulnerable
- **Defense**—Strengthen your protections
- **Actively secure your Weak Points**

Where and how am I and my PC vulnerable to Attack? What has changed Recently? What patches are available for my most used programs?

Are my passwords protected? Do I have AV and antispyware installed? Am I monitoring my sensitive information?

Have I patched my software in a timely manner? Have I turned on patch alerts for all major SW vendors and packages? Have I checked that my security settings are as “tight” as they need to be?
Ten ways to safeguard your identity

1. Regularly review billing statements and credit reports.
2. Use a crosscut shredder on ALL financial documents.
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.
6 Tips to Mitigate Risk of Data Loss and Control of Your PC

1. Keep your computer up-to-date with the latest security patches, not just Microsoft but Adobe, Firefox, etc.

2. Delete e-mail with suspicious-looking content or attachments immediately. View e-mail as plain text and disable JavaScript, Flash and preview features.

3. Manage your downloads folder at the end of each session. Delete what you don’t need to keep and save the rest somewhere that makes sense on your computer.

4. Keep Flash, Java and JavaScript disabled in your web browser and PDF viewer, except for sites or documents that really need it.

5. Use security software that is up to date and that includes not just antivirus and firewall protection, but HIPS and web services too. And if your computer slows down as a result, don’t turn off active scanning; instead, try different security software.

6. Purge your email and web browser caches from time to time. Some e-mail programs give you the option to “rebuild archive” or “update database,” to purge caches. Web browsers allow you to purge caches manually, or automatically when you exit the browser.
What else can I do to protect myself?

- Sign up for proactive credit and/or identity monitoring services
- Run antispyware and antivirus 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 e-mail
What should I do if I have a problem?

- Citi Identity Theft provides free assistance 24/7 for Citibank or credit card customers who suspect they may be victims of identity theft.

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

- For any suspicious transactions, immediately contact the 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 (continued)

Citi Identity Theft:


Citi Identity Monitor:

Identity Theft Trends and Prevention

ID Theft Prevention Tips (continued)

Summary: Remember These Three Things

- When browsing the Internet or viewing e-mail from unknown source:
  
  “If You Didn’t Pick It, Don’t Click It”

- If an unknown or unasked for window appears on your screen and it will not disappear or returns after normal close

  **Shut down/re-boot PC. Power down is most effective.**

- Set your major software programs (Microsoft Office, Adobe, Google) to provide you with software Update Notifications. These are primarily current security “patches” that are downloadable for free.
Identity Theft Trends and Prevention

Survey

Please take the course survey online by visiting:
www.gsasmartpayconference.org/survey
or by using the link sent to you via email from Feedback Systems.

Surveys can be taken through any mobile device.
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.

efficiency, renewable energy & mitigation