



GSA SmartPay Conference

# Information Security & Identity Theft

Maureen Garlock  
Vice President, Citi





Success is in the Cards

11<sup>th</sup> Annual GSA SmartPay Conference

Phoenix, Arizona  
July 28<sup>th</sup> - July 30<sup>th</sup>, 2009



# Techniques for Establishing a Successful Audit Process

---

## 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
- Must be scanned to receive CLP credits
  - For each course
- Unanswered Questions
  - Q-Cards & Ballot Boxes
  - Answer to be emailed after the conference - within 45 days



# Information Security & Identity Theft

---

## Goals & Objectives

---

**This session is designed to assist you in achieving the following goals:**

- Gaining an understanding of the definition and types of information security
- Identifying the various types of fraud and how their statistics in the marketplace
- Outlining tools and resources available to manage fraud prevention



# Agenda

---

1. Information Security Overview
2. Fraud in the Marketplace
3. Types of Fraud
4. Staying Informed
5. Fraud Early Warning at Citi
6. Fraud Prevention Tips



---

# 1. Information Security Overview

---

# Information Security & Identity Theft

---

## What is Information Security?

---

- **A collective set of policies, standards, processes and procedures that limits or controls access to, and use of, information to authorized users**
  - Information Security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption
- **Are information security methodologies new?**
  - Julius Caesar is credited with the invention of the Caesar cipher c50 B.C. to prevent his secret messages from being read should a message fall into the wrong hands
  - WW II brought about significant advancements in Information Security in that formalized classification of data based upon sensitivity of information and who could have access to the information was introduced
  - The rapid growth and wide spread use of electronic data processing and electronic business conducted through the Internet fueled the need for better methods of protecting these computers and the information they store, process and transmit

# Information Security & Identity Theft

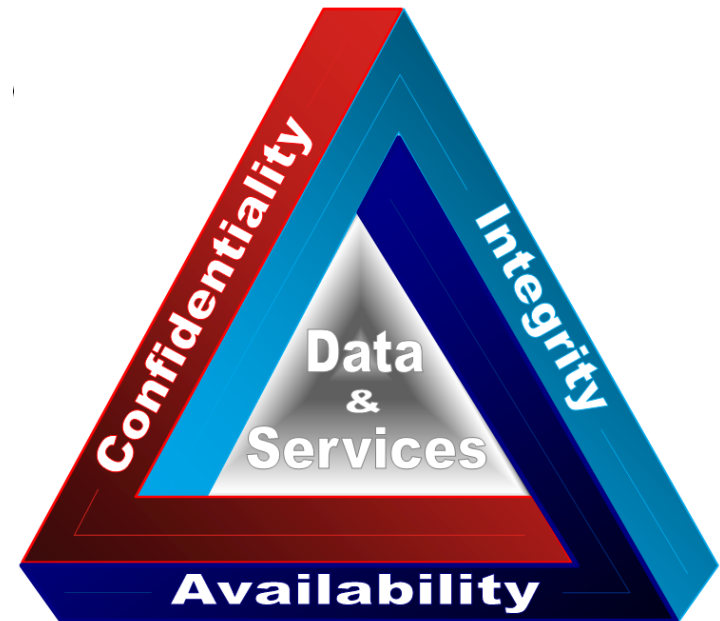
---

## What is Information Security? (continued)

---

### Information Security Core Principles

- Confidentiality
  - Holding sensitive data in confidence, limited to an appropriate set of individuals or organizations
- Integrity
  - Data can not be created, changed, or deleted without authorization
- Availability
  - The information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed
  - The opposite of availability is denial of service (DOS)



# Information Security & Identity Theft

---

## How much electronic data does Citi manage?

---

Citi manages 1 Petabyte of electronic data

(1 Petabyte is the equivalent of 15 million CDs)



---

## 2. Fraud in the Marketplace

---

# Information Security & Identity Theft

---

## Fraud in the Marketplace – In the News

---

*“Consumers Report \$239 Million Lost To Cyber Fraud In '07”*

*Washington Post April 4, 2008*

*“A recent study shows that credit card fraud hit one in twenty users and identity theft affected one in fifty people during past year” myIDfix.com*

*“Identity theft is the fastest growing crime in America. The average victim spends 175 hours and \$1000.00 repairing the damage. “myIDfix.com*

*“Every 79 seconds, a thief steals someone’s identity, opens accounts in the victim’s name and goes on a buying spree.” CBSnews.com*

*“U.S. Study Shows 8.3 Million Victims of Identity Theft in 2005” ftc.gov*

*“\$652B lost annually by US businesses to fraud and in more than 40% of these cases, not a penny is recovered.” gtnews.com*

# Information Security & Identity Theft

## Fraud in the Marketplace - Statistics

- Surveys from 2003 to 2006 showed a decrease in the total number of victims but an increase in the total value of identity fraud to \$56.6 billion in 2006
- The average fraud per person rose from \$5,249 in 2003 to \$6,383 in 2006
- Only 15% of victims learn about the theft through proactive action The average time spent by victims resolving the problem is about 40 hours
- 73% of respondents indicated the crime involved the thief acquiring a credit card

CY	Total No. of Complaints	Complaints Reporting Amount Paid	Percentage of Complaints Reporting Amount Paid	Amount Paid Reported	Average Amount Paid <sup>1</sup>	Median Amount Paid <sup>2</sup>
2004	410,709	310,299	76%	\$568,702,566	\$1,833	\$262
2005	437,906	285,255	65%	\$683,484,366	\$2,396	\$349
2006	428,319	364,500	85%	\$1,187,305,506	\$3,257	\$500

<sup>1</sup>Average is based on the total number of consumers who reported amount paid for each calendar year: CY-2004 = 310,299; CY-2005 = 285,255 ; and CY-2006 = 364,500. One hundred eighty-four consumers reported an amount paid of \$1 million or more during CY-2006; 42 and 49 consumers for CY-2004 and CY-2005, respectively.

<sup>2</sup>Median is the middle number in a set of numbers so that half the numbers have values that are greater than the median and half have values that are less. Calculation of the median excludes complaints with amount paid reported as \$0.

# Information Security & Identity Theft

## Fraud in the Marketplace – Statistics (continued)

### Fraud Complaints by Consumer Age *Calendar Years 2004 through 2006*

Consumer Age Range	CY - 2004		CY - 2005		CY - 2006	
	Complaints	Percentages <sup>1</sup>	Complaints	Percentages <sup>1</sup>	Complaints	Percentages <sup>1</sup>
19 and Under	9,076	3%	8,028	3%	2,663	2%
20-29	66,134	20%	65,343	20%	23,372	16%
30-39	76,757	24%	72,341	23%	29,117	21%
40-49	74,872	23%	74,379	23%	33,060	23%
50-59	57,302	18%	59,094	18%	28,868	20%
60-69	22,484	7%	23,767	7%	11,710	8%
70 and Over	16,882	5%	16,948	5%	12,897	9%
<i>Total Reporting Age</i>	<i>323,507</i>		<i>319,900</i>		<i>141,687</i>	

<sup>1</sup>Percentages are based on the total number of consumers reporting their age in fraud complaints for each calendar year: CY-2004 = 323,507; CY-2005 = 319,900; and CY-2006 = 141,687. 33% of consumers reported this information during CY-2006, 79% and 73% for CY-2004 and CY-2005, respectively.

# Information Security & Identity Theft

---

## Fraud in the Marketplace - Identity Theft Statistics

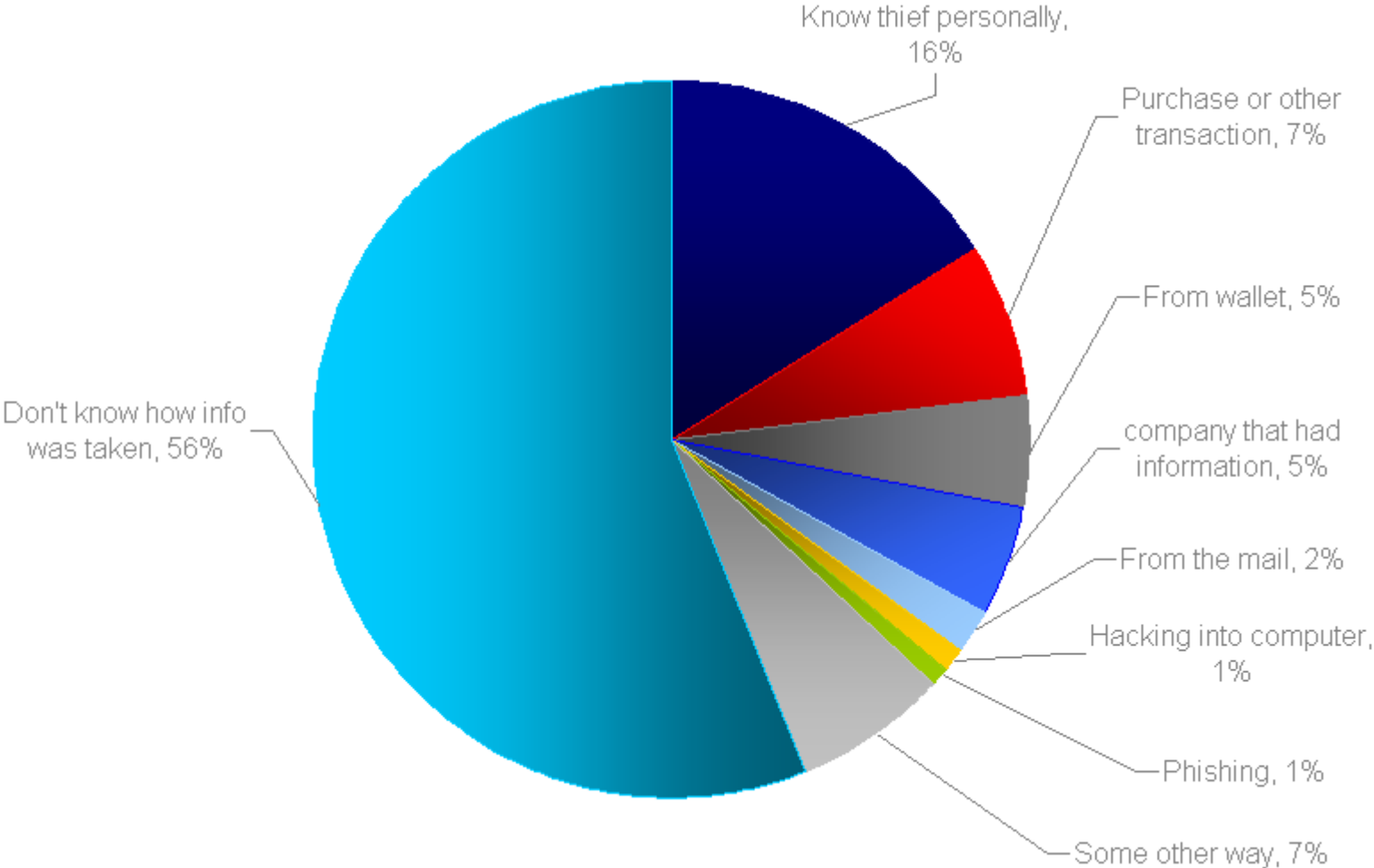
---

- According to the FBI, the number of victims will increase by 500,000-700,000 each year
- Every 79 seconds an identity is stolen in this country
  - By the end of this session, more than 53 people will become victims of identity theft
- 28% of identity theft was due to a lost or stolen credit card



# Information Security & Identity Theft

## Fraud in the Marketplace - Cases of Known Identity Theft

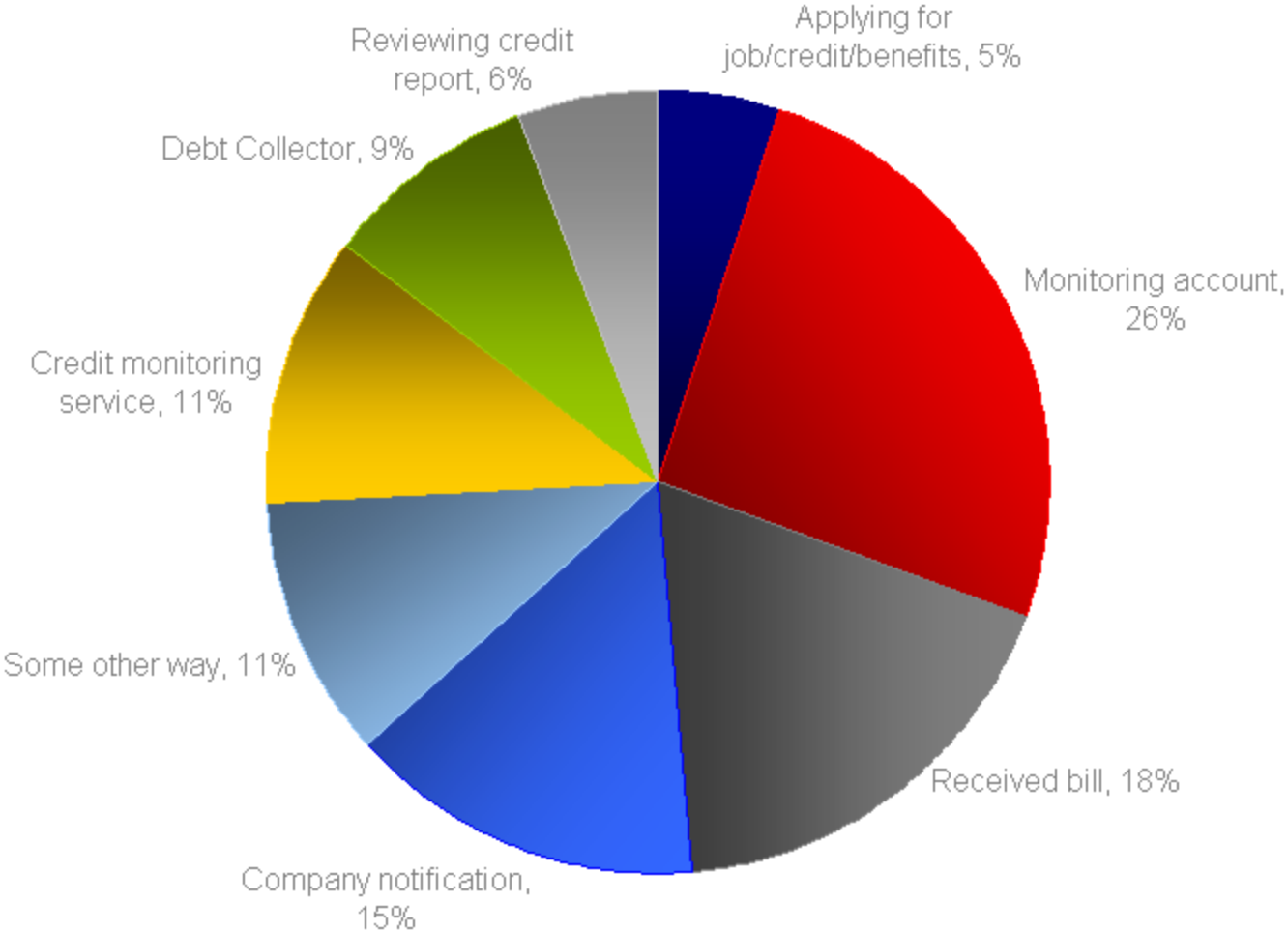


Source: 2006 Identity Theft Survey Report



# Information Security & Identity Theft

## Fraud in the Marketplace - Ways Victims Discovered Identity Theft

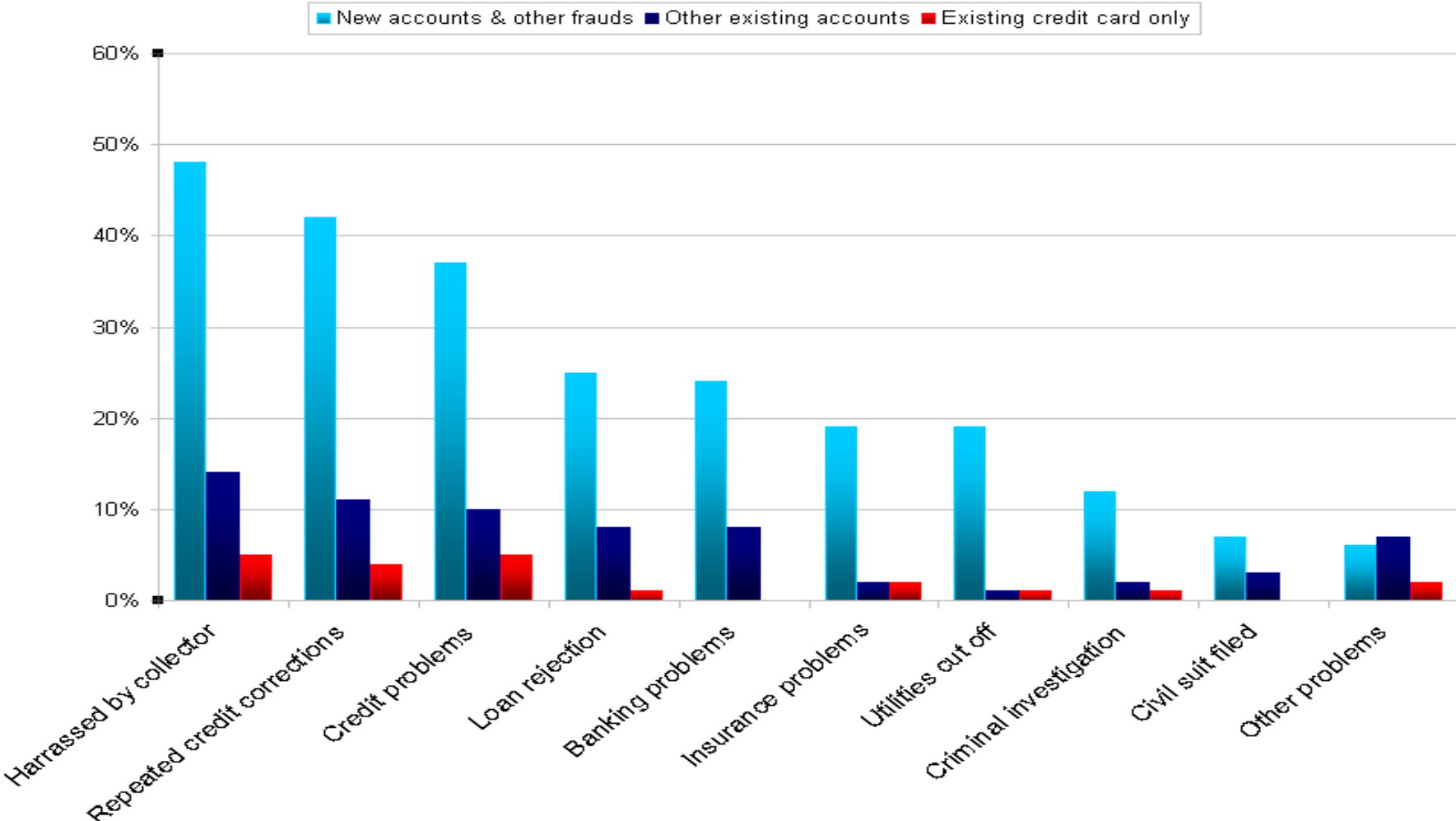


Source: 2006 Identity Theft Survey Report



# Information Security & Identity Theft

## Fraud in the Marketplace - How Identity Theft Affects You



---

## 3. Types of Fraud

---

# Information Security & Identity Theft

---

## Types of Fraud

---

- Types:
  - Hijacking existing accounts and deposits
  - Creating new alternate identities
- How can someone steal my identity?
  - Stealing records
  - Trash (Dumpster Diving)
  - Credit Reports
  - Theft of wallet, purses
  - Electronic scams (as discussed)



# Information Security & Identity Theft

---

## Types of Fraud – Social Engineering

---

- A facet of Information Security aimed at manipulating people
- Creating a false sense of trust in order to...
  - Gain insider access
  - Obtain sensitive information
  - Bypass an organization's existing physical security controls



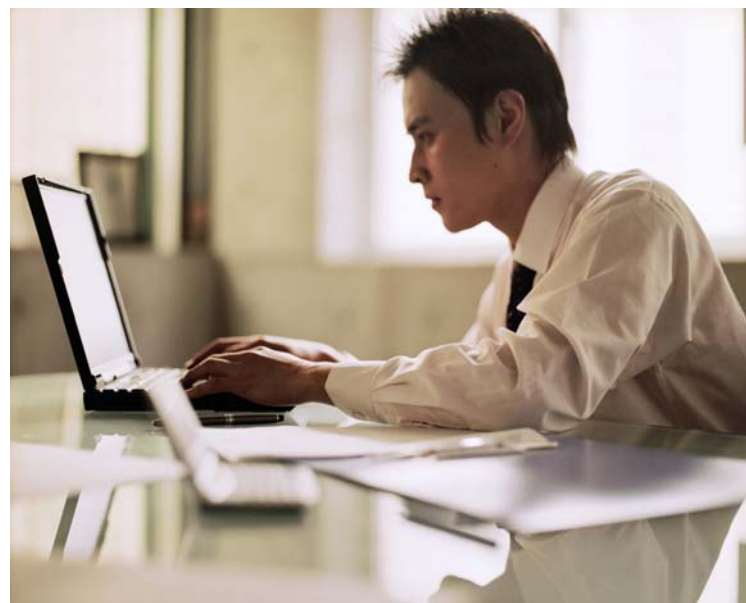
# Information Security & Identity Theft

---

## Type of Fraud – Social Engineering (continued)

---

- Psychological Subversion
  - Establishing a relationship with an insider to gain access to continuing stream of information
- Masquerading
  - Impersonating people with legitimate access or a need to know to gain access
- Shoulder Surfing
  - Stealing information by watching a legitimate user type in a password
- Tailgating
  - Entering secure locations by following behind someone with legitimate access
- Dumpster Diving
  - Finding improperly discarded information



# Information Security & Identity Theft

---

## Types of Fraud – Phishing Scams & Fraudulent Emails

---

- Phishing is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information
- Millions of fraudulent e-mail messages are sent that appear to come from Web sites you trust, like your bank or credit card company, and request that you provide personal information
- Often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites
- March 6, 2008 Headline from [www.darkreading.com](http://www.darkreading.com):

### *Surge of Phishing Kits Hits the Net*

Researchers are investigating an unusually high volume of free phishing kits – over 400 – now in the wild

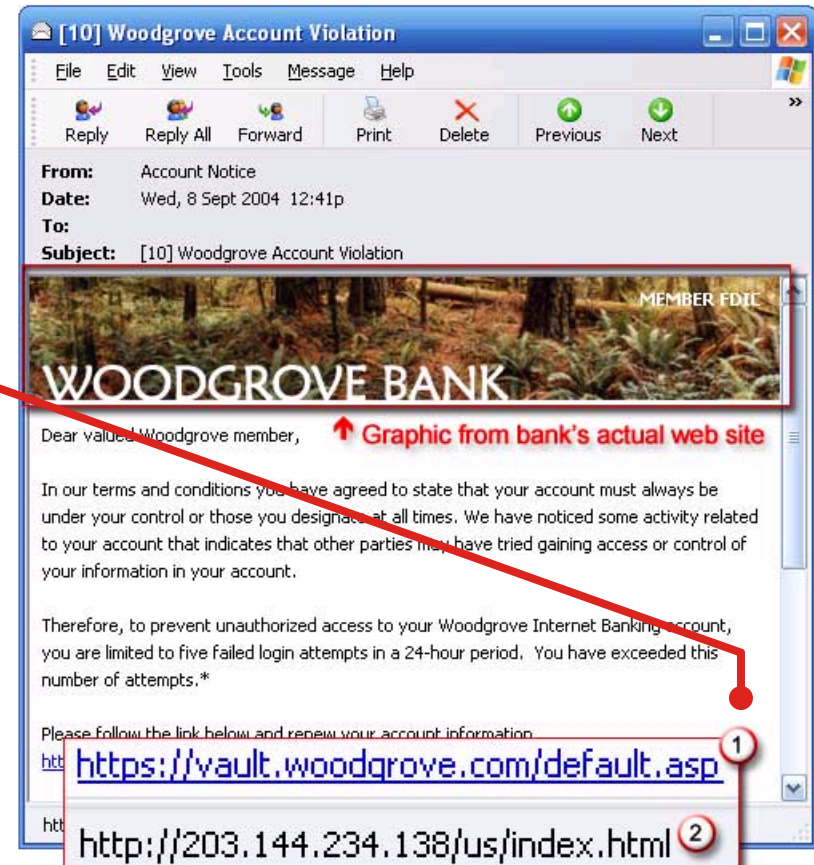
# Information Security & Identity Theft

## Types of Fraud – Phishing Scams & Fraudulent Emails (continued)

What does phishing look like?

1. Resting (but not clicking) the mouse pointer on the link reveals the real Web address

2. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign



# Information Security & Identity Theft

---

## Types of Fraud – Identifying Email & Phishing Scams

---

- "Verify your account"
  - Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail
- "If you don't respond within 48 hours, your account will be closed"
  - Conveys a sense of urgency and might even claim that your account has been compromised
- "Click the link below to gain access to your account"
  - HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site
  - Links may contain all or part of a real company's name and are usually "masked"
- May also use URLs that **resemble** the name of a well-known company:
  - www.mic**o**soft.com
  - www.mir**o**soft.com
  - www.**verify**-microsoft.com

# Information Security & Identity Theft

---

## Types of Fraud – Internet Thievery & Electronic Scams

---

- How can I spot a true website from a fake?
  - Look for the lock or key icon at the bottom of the browser
  - If the site has changed since your last visit, be suspicious
  - A list of popular financial sites that use a secure page for logins is maintained on [pharming.org](http://pharming.org)
  - Check spelling, grammar, and punctuation
    - If there are errors chances are you may have been phished
  - Hover over suspicious links to find masked URL's (as in the previous example)
  - A reputable business will never ask you to verify account information online
  - Did you initiate the contact?
- What to do?
  - Report suspicious incidences to Citi immediately

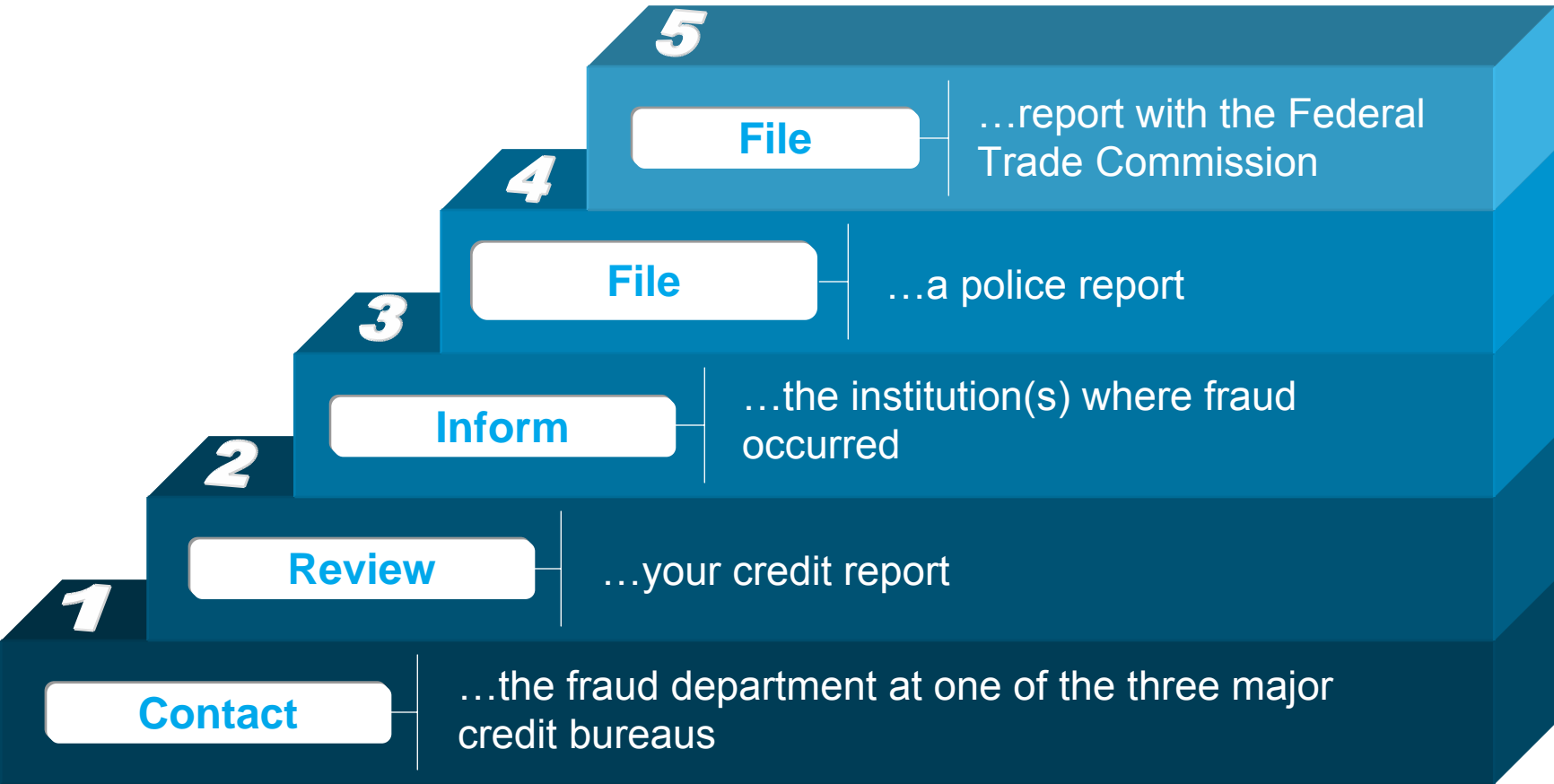
# Information Security & Identity Theft

---

## Types of Fraud – What if I am a Victim?

---

**Five steps to minimize damage/maximize control:**



---

## 4. Staying Informed

---

# Information Security & Identity Theft

---

## Staying Informed - Resources

---

- Federal Trade Commission Identity Theft Clearing House
  - [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)
  - 1-877-438-4338
- Credit Bureaus
  - Equifax – [www.equifax.com](http://www.equifax.com)
  - Experian – [www.experian.com](http://www.experian.com)
  - TransUnion – [www.transunion.com](http://www.transunion.com)
- Free Credit Reports
  - [www.annualcreditreport.com](http://www.annualcreditreport.com)



# Information Security & Identity Theft

---

## Staying Informed – Resources (continued)

---

- [www.fbi.gov](http://www.fbi.gov)
- [www.lookstoogoodtobetrue.com](http://www.lookstoogoodtobetrue.com)
- [www.ic3.gov](http://www.ic3.gov)
- [www.ftc.gov](http://www.ftc.gov)
- [www.darkreading.com](http://www.darkreading.com)
- State governments / task forces
- Newspapers / Magazines
- ...and many other resources are available



---

## 5. Fraud Early Warning (FEW) at Citi

---

# Information Security & Identity Theft

---

## Fraud Early Warning (FEW) at Citi – Our Mission

---

- Identify
  - Lost / Stolen
  - Never received reissued or new card
  - Counterfeit activity
  - Credit Master attacks
  - Points of compromise
- Monitor high risk transactions indicative of unusual behavior
- Reduce fraud losses
  - Prevent and minimize the fraudulent activity
  - Detect unusual behavior in the early stages of fraud and reduce the impact to our customers



# Information Security & Identity Theft

---

## Fraud Early Warning (FEW) at Citi – Fraud Types & Definitions

---

	Type	Definition
1	<b>Lost</b>	Cardholder misplaced / lost card
2	<b>NRI</b>	Never received reissued or new card
3	<b>Card Not Present</b>	Transactions conducted over the internet or by phone (MOTO)
4	<b>Stolen</b>	Cardholder is victim of theft
5	<b>Altered / Counterfeit</b>	Cardholder is in possession of card; a copy has been made and used by the criminal. <i>Manual vs. Skimming</i>
6	<b>Account Takeover</b>	Fraudster is able to assume / obtain personal information in order to request an additional card

---

## 6. Fraud Prevention

---

# Information Security & Identity Theft

## Fraud Prevention - 4 Strategic approaches to fighting fraud...



---

## 7. Prevention Tips

---

# Information Security & Identity Theft

---

## Prevention Tips

---

- Identify fraud usage patterns, MCC trends, suspicious merchants
- Identify and shut down test points
- Identify and shut down credit master fraud runs
- Work with Citi partners to identify CPP's (common purchase points – point of compromise)
- Install “priorities” to flag accounts that meet the criteria
- Determine “risk” to prioritize accounts for FEW analysts
- Constant review of effectiveness



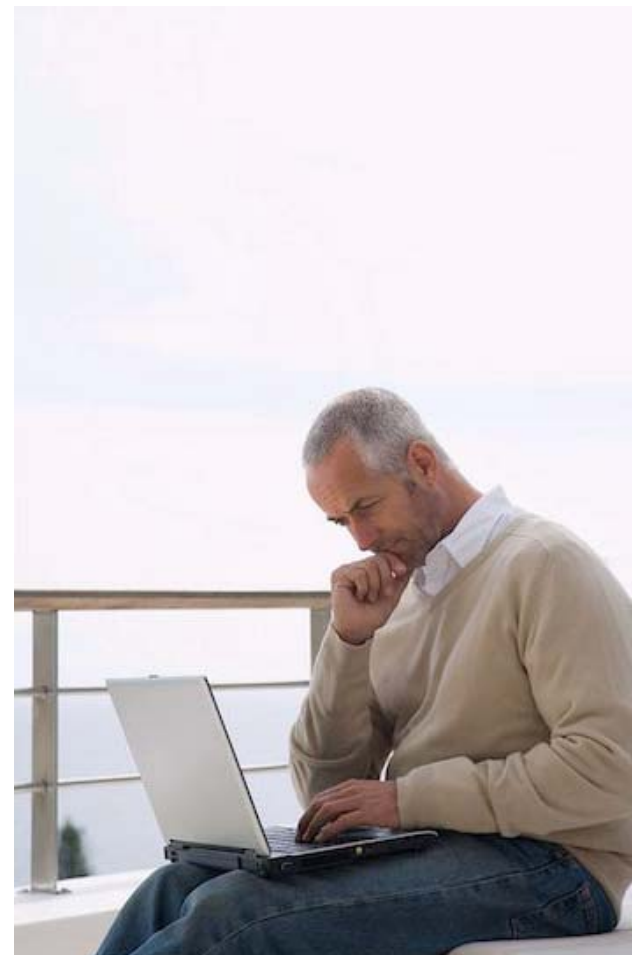
# Information Security & Identity Theft

---

## Prevention Tips for You & Your Cardholders

---

- Never leave cards in an unlocked desk or cabinet
- Do not leave receipts/statements/reports unattended
- Be aware of your surroundings when providing card information to another person
- Review statements/account activity regularly
- Immediately contact the card provider if you do not recognize activity
- Avoid letting merchants take your card out of your line of sight if possible
- Keep your account information current
- Do not keep PIN with card
- Change password(s) frequently



# Information Security & Identity Theft

---

## Prevention Tips – For Program Coordinators

---

- Internal process to receive cards / distribute to cardholders
- Use employee's correct verification when submitting applications
- Never leave new / reissued / canceled cards in an unlocked desk or cabinet
- Do not leave reports / statements lying around
- Report potential compromise immediately
- Assist in educating cardholders that the card is for authorized use only
- Utilize card restrictions (MCC, Transaction Limits, etc)
- Report cancelled cards for terminated employees immediately

# Information Security & Identity Theft

---

## Summary

---

**This session was designed to assist you in achieving the following goals:**

- Gaining an understanding of the definition and types of information security
- Identifying the various types of fraud and how their statistics in the marketplace
- Outlining tools and resources available to manage fraud prevention



# 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 U.S. tax treatment or U.S. 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 which 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 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.

© 2009 Citibank, N.A. All rights reserved. Citi, Citi Arc Design, CitiDirect, Citimanager, Citibank Custom Reporting System, 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.



