

---

# Identity Theft: An Overview

Georgia FBLA Leadership Conference  
Athens GA

March 16, 2007

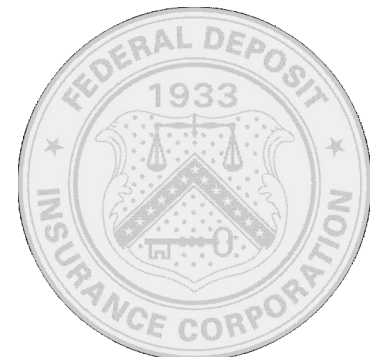




# Presenter

---

- Thomas Stokes
  - Community Affairs Officer
  - Division of Supervision and Consumer Protection
  - Atlanta, GA



# Agenda

---

- Background
- How ID theft is perpetrated
- Consumer protection laws
- Savvy Surfing
- Project Suggestions
- Resources





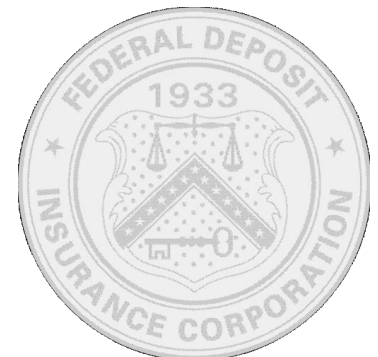
# Background



# Background

---

- Identify Theft – is taking your personal information without your knowledge (e.g., your name, social security number or password) to make purchases and stiff you with the bill!

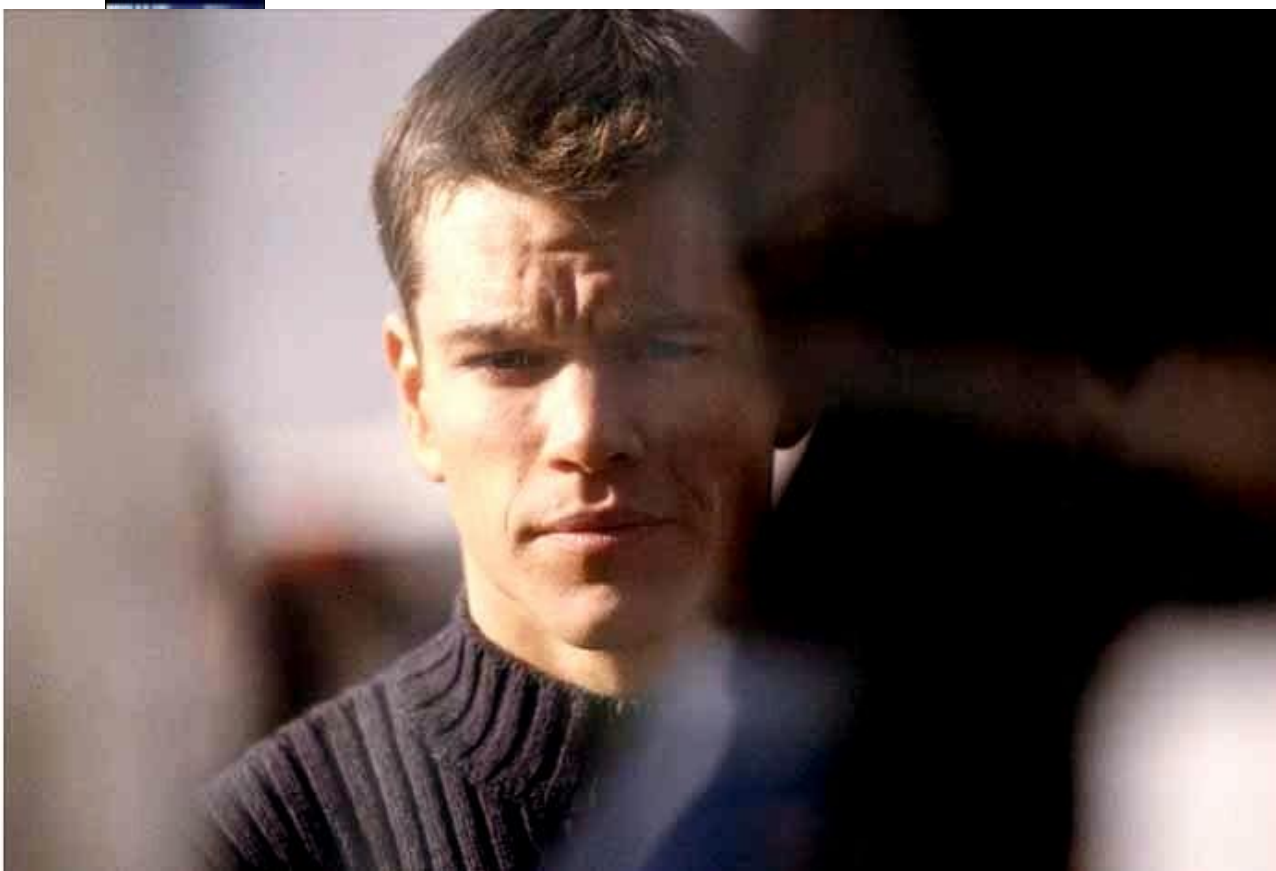


# Background

---

- ID theft is increasingly being committed by highly structured criminal organizations
- Cyber Thieves exploit electronic commerce & online databases facilitate ID theft
- Concern about ID theft may be slowing the growth of online banking and e-commerce  
(Gartner May 2005/The Conference Board June 2005)





# How ID Theft is Perpetrated



# How ID Theft is Perpetrated

---

- Account hijacking
- Phishing
- Hacking
- Spyware
- Reselling personal information



# How ID Theft is Perpetrated

---

- Goal is to steal consumer's identity
- Database hacking provides access to customer list
- Data validation are automated ways to trick systems into providing information



# ID Theft is 2-Step Process

---

- Sensitive information is stolen
- Stolen identity becomes a product for resale or personal use
- Merchant and original consumer victimized by virtual shopping
- Lost \$\$\$ to merchant and potential years of credit clean-up for original consumer



# ID Theft Marketplace

---

- Criminals are using the Web to sell the sensitive personal information they steal:
  - Carderplanet.com
  - Darkprofits.com
  - Shadowcrew.com
- These sites sold credit card and bank account numbers and counterfeit ID cards.
- Responsible for 1.7 million stolen credit cards and \$4.3 million in losses between 8/02-10/04 (WSJ 7/13/05)



# ID Theft Marketplace

---

- These sites were shut down in October 2004 by U.S. Secret Service's "Operation Firewall"
- 28 people arrested
- Suspects were located in 6 foreign countries and 8 states
- New sites are popping up
- IDdefense is tracking 20 new Russian-language sites (WSJ 6/1/05)



# Physical Theft

---

- Mail theft
- Dumpster diving
- Shoulder surfing
- Skimming



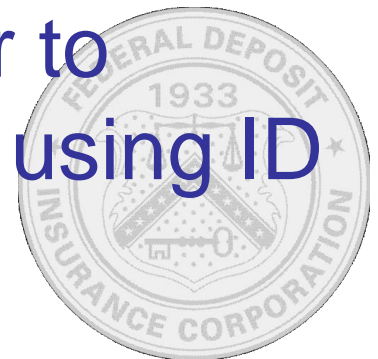
# Portable Skimmer



# Phishing

---

- Use of fraudulent e-mails and phony web sites to fool recipients into divulging confidential information used to commit ID theft
- Financial services companies are most frequent targets
- Fraudulent e-mail instructs customer to hyperlink to spoofed web site, log in using ID & password to “fix” a problem



# Phishing

---

- [www.annualcreditreport.com](http://www.annualcreditreport.com)
- Set up by 3 major credit reporting agencies in accordance with FACTA to provide consumers with their free credit reports
- Over 100 impostor websites exist to collect sensitive information





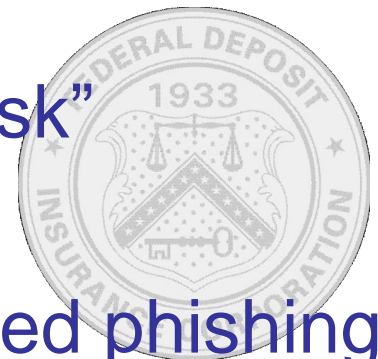
- Use of real stolen information to target you by name and trick you into providing more information.
- Thieves are trying to get social security numbers, pins and passwords.



# Hacking

A vertical image of a blue circuit board is positioned on the left side of the slide, partially overlapping the "Hacking" title. A thick blue horizontal line runs across the slide below the title.

- CardSystems Solutions, Inc.
  - Merchant credit card processor
  - Hacker broke in April 2004, discovered May 05
  - Hacker came from IP addresses in London, India, Malaysia, and New Jersey
  - 12 million accounts “at risk”
  - 263,000 accounts considered “high risk”
  - Unauthorized charges have occurred
  - Information being used for personalized phishing



# Spyware

- Keystroke loggers can be surreptitiously loaded on home PCs or PCs in Internet cafes



- When users access certain sites, logger collects user name, passwords and other data.



# Spyware

---

- Virus e-mail or spyware attachments on gambling, porn, near porn and lesser known free game or music download sites can capture keystroke information and transmit to cyber thieves
- March 2005, Brazilian police arrested leader of hacker gang
- Stole more than \$37 million from bank accounts
- E-mailed keystroke loggers to victims
- Sent 3 million infected e-mails per day (Sydney Morning Herald 3/18/05)





# FDIC ID Theft Study

---

- Strengthen educational programs to help consumers avoid scams
- Continuing emphasis on information sharing between financial services industry, technology providers, and government would help to mitigate risks



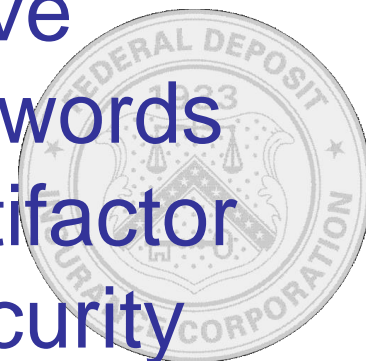


# Supplement's Updated Findings

---

Technology Supervision Branch

- As part of required risk assessment, banks should analyze need for more secure customer authentication
- If product allows access to sensitive customer information, use of passwords should be supplemented with multifactor authentication or other layered security





---

# Consumer Protection





## ELECTRONIC FUND TRANSFER ACT

**If there has been an unauthorized use of an ATM card, debit card or other electronic banking device, this limits the consumer's liability.**





# Free Consumer Reports- FACT Act, §211(a)

---

- Consumers are entitled to one free credit report from each of the credit reporting agencies during any 12 month period





## FAIR CREDIT BILLING ACT

**Establishes procedures for correcting errors on credit card bills. This also allows for a consumer to dispute a purchase made with the card.**





# Savvy Surfing

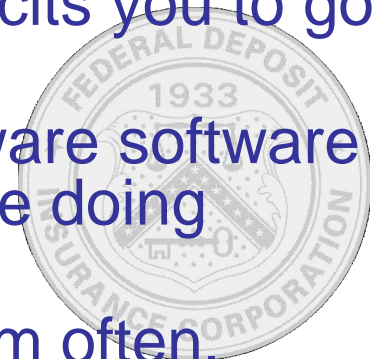
I'm all right, Trin....but I think  
you're gonna have to drive.



# Savvy Surfing

---

- Don't download free content from gambling, porn, near porn or obscure free game and free music websites.
- Never log personal information on an on-line site you don't know or feel comfortable in using.
- Delete unknown e-mail and delete again.
- If your software permits, create a separate folder for unknown e-mail with attachments. Do a frequent delete purge of that folder.
- Be cautious in responding to any e-mail that solicits you to go to a webpage to log on.
- Use updated anti-virus, anti-spam and anti-spyware software and make sure the school and public libraries are doing likewise. Ask them!
- If you do have any on-line accounts – check them often.





---

# Project Suggestions



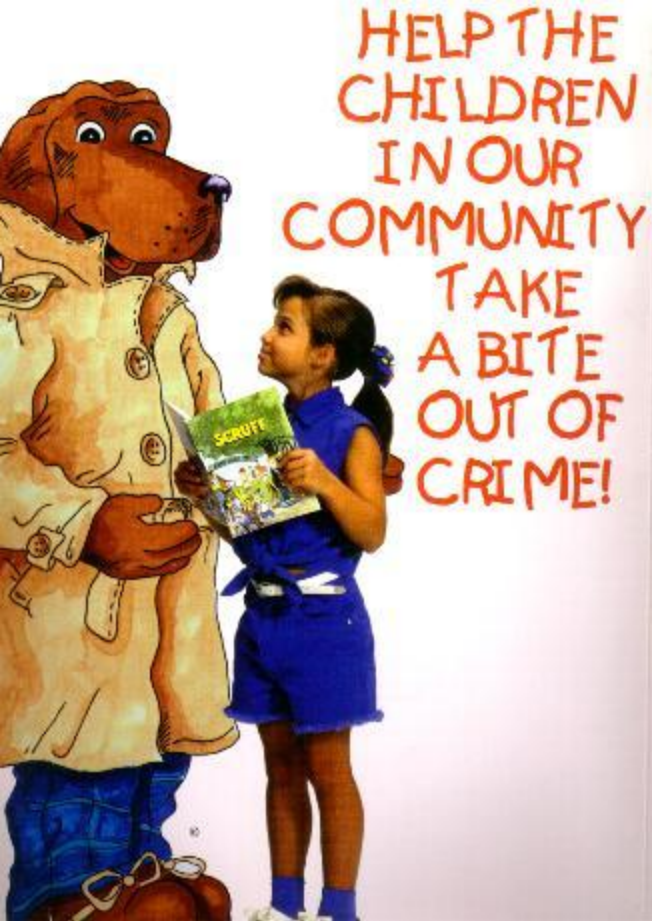
DODGE  
THIS!!

Technology Supervision Branch



# Design an ID Theft Poster





**Publish a desktop children  
book on junior cyberwatch**



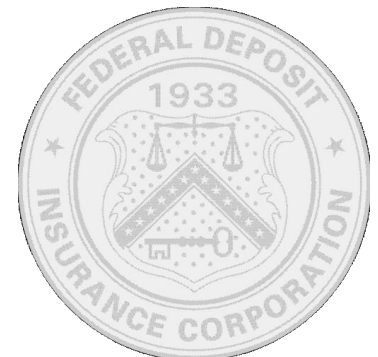
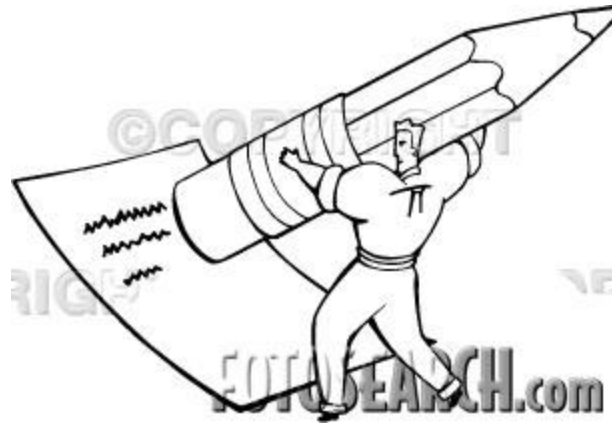


# Design a webpage or online newsletter on cyber security





**Plan and develop a program to educate your parents, school, your school's sponsor and other local businesses to use eraser software before donating old computers.**





## Resources

[www.fdic.gov/quicklinks/consumers.html](http://www.fdic.gov/quicklinks/consumers.html)

[www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/)

[www.stopidentitytheft.org](http://www.stopidentitytheft.org)





**THANK YOU**

