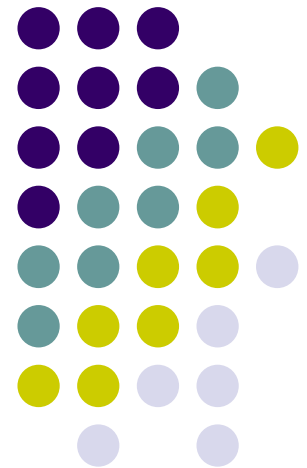


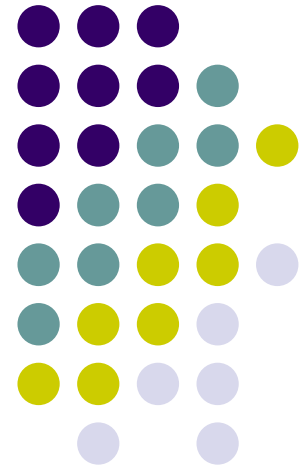
The President's Task Force on Identity Theft and The FTC's Role in Identity Theft

Joanna P. Crane
Federal Trade Commission



The views expressed are those of the speaker and not necessarily those of the FTC or any other person.

FTC's Responsibilities Under ID Theft Act

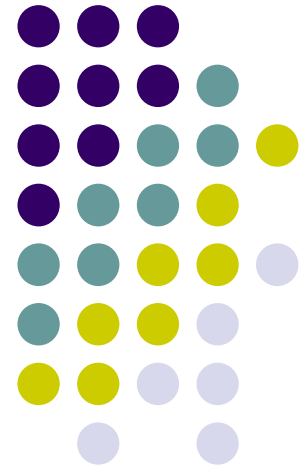


Establish centralized complaint and consumer education service for victims



- Section 5 of the Identity Theft and Assumption Deterrence Act of 1998 required the FTC to create the “centralized complaint and consumer education service for victims of identity theft” for the federal government
 - Receive complaints from victims
 - Provide information and assistance to victims
 - Log them and refer them as appropriate to law enforcement and the 3 major CRAs

Victim & Consumer Resources



Hotline & Website Advise Consumers and Victims, Take Complaints, Answer Inquiries

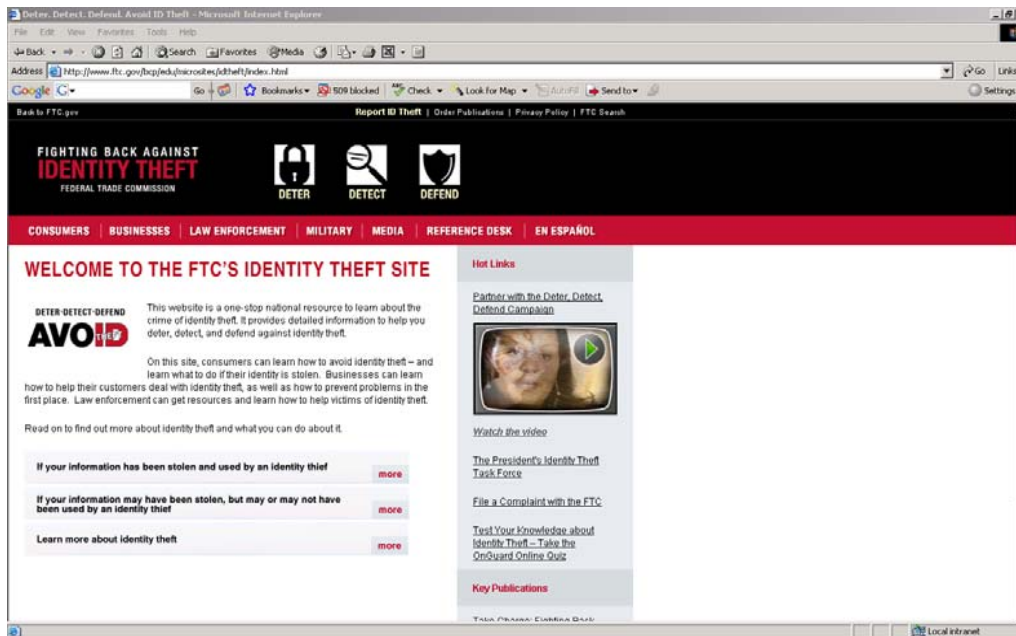


- Toll-free phone number for victims
1-877-ID THEFT (438-4338)
- www.ftc.gov/idtheft
 - Printable Universal ID Theft Complaint Form
- www.onguardonline.gov
 - Combat internet fraud, protect personal information
- FTC does not investigate the complaints of specific individuals
 - Monitors complaint database for trends, brings civil actions where pattern or practice of violations appears



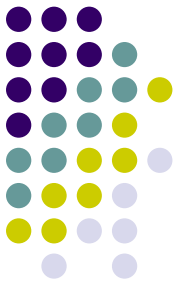
FTC's Identity Theft Website

- www.ftc.gov/idtheft



- Online Complaint form
- ID Theft Affidavit Online

FTC's OnGuardOnline Website



The screenshot shows the OnGuardOnline.gov website in a Windows Internet Explorer browser window. The address bar displays <http://www.onguardonline.gov/#>. The website features a blue header with the OnGuardOnline logo and navigation links for TOPICS, GAMES, VIDEOS, TOOLS, and ABOUT US. A search bar is also present. The main content area includes a sidebar with the text: "OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information." Three main content boxes are displayed: "TOPICS" (Learn Experts' Top Tips for Computer Security), "GAMES" (Test your Cyber Smarts with Interactive Quizzes), and "VIDEOS" (Watch Videos about Online Safety). Below these are three promotional sections: "Show of Hands" (a poll about FOIA requests), "What Do You Think?" (a poll about FOIA requests), and "How To Spread The Word!" (a section about promoting safe computing). The footer contains links for Order Publications, Share this Page, Privacy Policy, File a Complaint, Contact Us, and Site Map, along with the slogan "STOP • THINK • CLICK™".

OnGuardOnline
YOUR SAFETY NET™

EN ESPAÑOL

TOPICS GAMES VIDEOS TOOLS ABOUT US

SEARCH

OnGuardOnline.gov
provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

TOPICS
Learn Experts' Top Tips for Computer Security

GAMES
Test your Cyber Smarts with Interactive Quizzes

VIDEOS
Watch Videos about Online Safety

Show of Hands:
The best way to get a free copy of your credit report is to file a Freedom of Information Act (FOIA) Request.

What Do You Think?
 I do that all the time.
 Umm...no. Duh.

VOTE

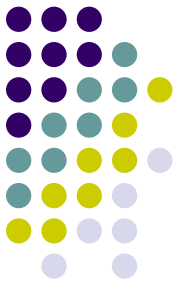
How To Spread The Word!
How Can You Promote Safe Computing? Partner with OnGuard Online!

- ▶ [OnGuard Online Game Buttons](#)
- ▶ [OnGuard Online Buttons & Banners](#)
- ▶ [OnGuard Online Games](#)

Order Publications Share this Page Privacy Policy File a Complaint Contact Us Site Map

STOP • THINK • CLICK™

Model Letters, Forms for Victims at FTC IDT Web Site



Tools For Victims - Deter, Detect, Defend, Avoid ID Theft - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media

Address http://www.ftc.gov/bcp/edu/microsites/idtheft/tools.html

Back to FTC.gov Report ID Theft | Order Publications | Privacy Policy | FTC Search

FIGHTING BACK AGAINST IDENTITY THEFT
FEDERAL TRADE COMMISSION

DETER **DETECT** **DEFEND**

CONSUMERS | **BUSINESSES** | **LAW ENFORCEMENT** | **MILITARY** | **MEDIA** | **REFERENCE DESK** | **EN ESPAÑOL**

TOOLS FOR VICTIMS

While dealing with problems resulting from identity theft can be time-consuming and frustrating, most victims can resolve their cases by being assertive, organized, and knowledgeable about their legal rights. These tools are designed to assist you in resolving disputes related to identity theft and in asserting your legal rights.

ID Theft Complaint Form:
The FTC is the federal clearinghouse for identity theft complaints. The complaints we receive from victims are available to other federal, state and local law enforcement officials nationwide. The standardized printed [ID Theft Complaint](#) can be used in conjunction with a police report to create an [Identity Theft Report](#) that will help victims recover more quickly. Specifically, an Identity Theft Report can be used to permanently [block fraudulent information](#) from appearing on your credit report and also make sure that these [debts do not reappear](#) on your credit report. An Identity Theft Report can prevent a company from continuing to [collect debts](#) that result from identity theft, or selling them to others for collection. It's also needed to place an [extended fraud alert](#) on your credit report.

ID Theft Affidavit:
The [ID Theft Affidavit](#) may be required for a variety of purposes, including to absolve you of the debt when an identity thief opens a new account in your name, or to obtain application or transaction records from a company the identity thief dealt with. If you do not need to obtain any application or transaction records, and need only to have a specific debt absolved, you may want to ask the company whether they will accept the Identity Theft Report alone. The Identity Theft Report is a more detailed version of the ID Theft affidavit, and as discussed above, entitles you to additional protections.

Sample Letter to Request Fraudulent Transaction or Account Information:
You can use this [sample letter](#) to request information from businesses the identity thief dealt with. This information can be useful to you to show that the thief, rather than you, made the transaction, and to law enforcement by providing information about the thief such as his or her address.

Chart Your Course of Action: Use this form to record the steps you've taken to report the fraudulent use of your identity. Keep this list in a safe place for reference.

Sample Letter to Credit Reporting Company:
Use this [sample letter](#) to request that the consumer reporting companies block fraudulent information from appearing on your credit report. Click [here](#) for additional information.

Hot Links

[Use Our Materials In Your Community](#)



[Watch the video](#)

[The President's Identity Theft Task Force](#)

[File a Complaint with the FTC](#)

[Victims' Statement of Rights](#)

[Test Your Knowledge about Identity Theft - Take the OnGuard Online Quiz](#)

Key Publications

[Take Charge: Fighting Back Against Identity Theft \(PDF 4.9MB\)](#)

[Information Compromise and the Risk of Identity Theft: Guidance for Your Business \(PDF 132KB\)](#)

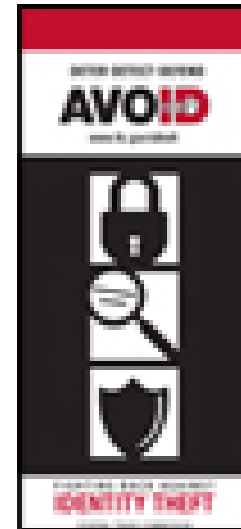
Protecting Personal Information: A Guide for Business (PDF 3.47MB)

Start | Inbox - Microsoft Outlook | FTC's Perspective | Tools For Victims - Det... | Local intranet | 4:20 PM



Consumer Educational Materials

- Take Charge: Fighting Back Against Identity Theft
- AVOID ID Theft:
Deter, Detect, Defend



www.ftc.gov/bulkorder

Training Materials: Deter, Detect, Defend, Defend Education Kits



TALKING ABOUT IDENTITY THEFT:
A HOW-TO GUIDE

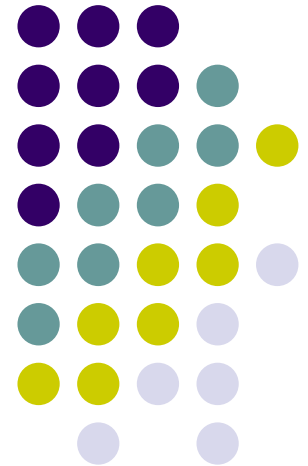


DETER · DETECT · DEFEND

AVOID THEFT

www.ftc.gov/idtheft

Law Enforcement Resources

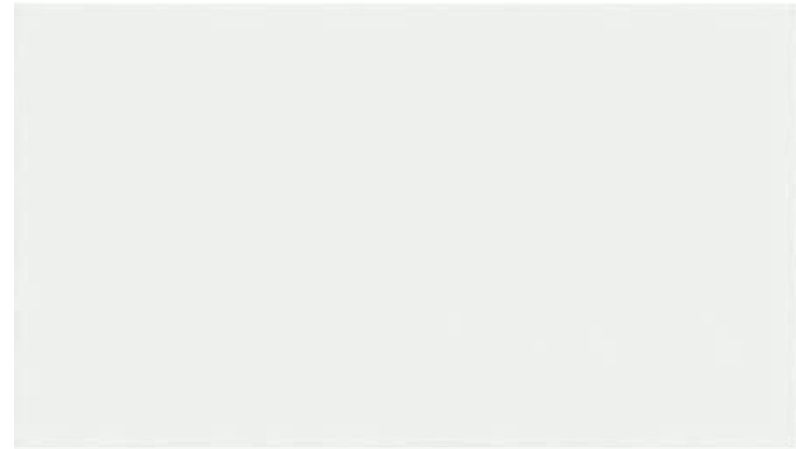


FTC's Complaint Database

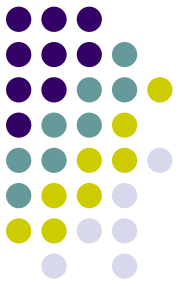


Identity Theft Data Clearinghouse

- Federal government's centralized database of identity theft victim complaints
 - Available for **FREE** through the Consumer Sentinel Network
 - Over 1.6 million searchable complaints
- Contents
 - victim contact information
 - suspect information: name, address, phone, relationship to the victim
 - description of crime, details
 - what financial institutions were involved
 - police report number, department name, contact information



The Clearinghouse – How It Helps Investigators



- Initiate new investigations
 - Multiple victims report same suspect name or address.
 - Additional addresses and phone numbers related to those leads.
- Strengthen ongoing investigations and prosecutions
 - Additional victims and witnesses
 - Additional addresses and phone numbers used by suspect
 - Additional defrauded companies

Clearinghouse Tools



- **Scheduled Search** – “set it and forget it”
 - Create a query on any piece of information
 - Run query overnight - if there is a hit, you will receive an email with link
- **Alert** – Deconfliction - place an alert on any piece of information to let other LEOs know you are investigating
- **Contacts** – CS members, USPIS contacts, bank contacts, etc.

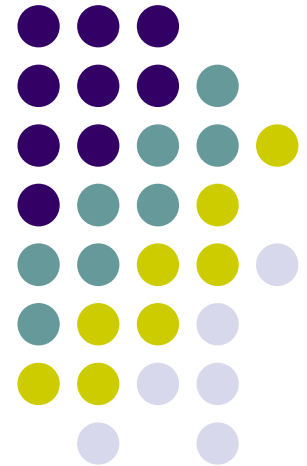
CD-ROM for Law Enforcement



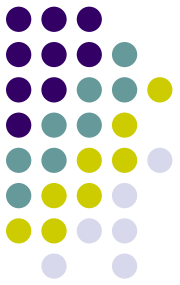
- Contains useful information about fighting identity theft:
 - first steps victims should take
 - how to get business records without a subpoena

The President's Identity Theft Task Force

Created by Executive Order in May 2006
Strategic Plan delivered to President April 2007
Implementation Report Issued in September
2008



President's ID Theft Task Force Recommendations

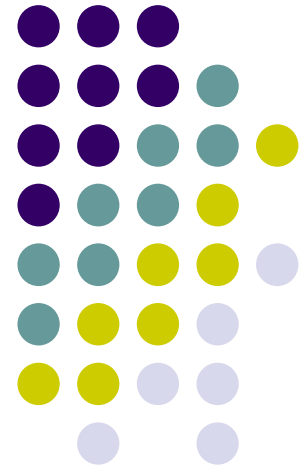


The Three-Part Strategy



- Prevention: Keep sensitive consumer data out of the hands of identity thieves
- Remediation: Help victims recover
- Deterrence: Prosecute and punish those who commit the crime and thereby deter future criminal conduct

Prevention: Keeping Consumer Data Out Of The Hands Of Criminals

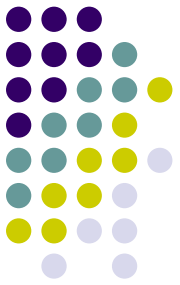


Improve Data Security in Public Sector



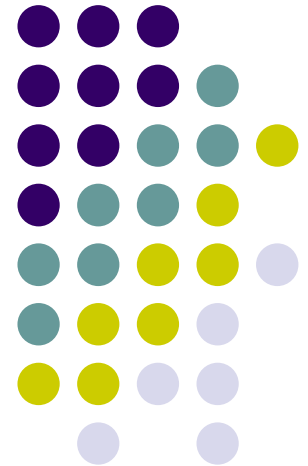
- Decrease the Unnecessary Use of Social Security Numbers in the Public Sector by Developing Alternative Strategies for Identity Management
 - OMB Guidance Issued June 2007
- Educate Federal Agencies on How to Protect Data; Monitor Their Compliance with Existing Guidance
 - OMB Guidance Issued May 2007, Annual Certification Required
- Ensure Effective, Risk-Based Responses to Data Breaches by Federal Agencies
 - OMB Guidance issued in September 2006 and May 2007

Improve Data Security in Private Sector



- Establish National Standards for Private Sector Data Protection Requirements and Breach Notice Requirements
 - FTC Providing Ongoing Legislative Support & Counsel
- Develop Comprehensive Record on Private Sector Use of Social Security Numbers
 - FTC Report Issued in December 2008
- Better Educate the Private Sector on Safeguarding Data
 - FTC Guidance Issued in March 2007
- Initiate Investigations of Data Security Violations
 - 26 cases completed since 2006
- Initiate a Multi-Year Public Awareness Campaign
 - Enlist Private Outreach Partners

Remediation: Helping Victims Repair Their Lives



Training and Individual Assistance



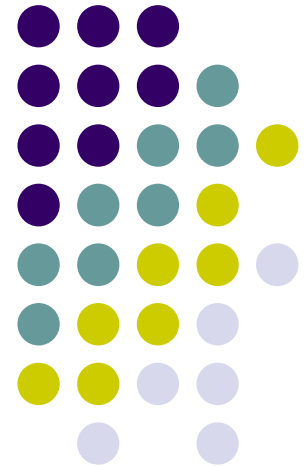
- Provide Specialized Training About Victim Recovery to Those who Offer Direct Assistance to Identity Theft Victims
 - Train law enforcement officers – ongoing seminars
 - Design nationwide training for victim assistance counselors and pro bono attorneys
 - Create and distribute an ID Theft Victim Statement of Rights – June 2007
- Fund New Avenues for Individualized Assistance to Identity Theft Victims
 - Grant money for NGOs distributed by DOJ

Statutory and Regulatory Issues

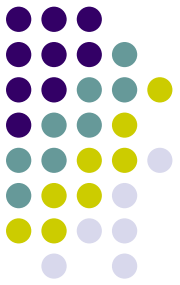


- Amend Criminal Restitution Statutes to Ensure That Victims Recover the Value of Time Spent in Trying to Remediate the Harms Suffered
 - The Identity Theft Enforcement and Restitution Act was passed in 2008
- Assess National System That Allows Victims to Obtain an Identification Document for Authentication Purposes

Deterrence: Prosecuting and Punishing Identity Thieves



Identity Theft Trends



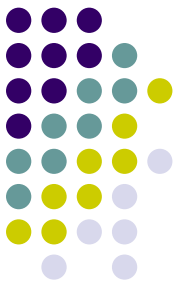
- Significant Criminal Groups and Organizations
 - Steady increase in involvement of groups and organizations of repeat offenders or career criminals in identity theft
 - Foreign organized criminal groups are increasingly engaged in computer- or Internet-related identity theft schemes
 - Organized groups in Europe and Asia use sophisticated tools to deceive Internet users into disclosing personal data, such as:
 - Keyloggers
 - Spyware
 - Botnets

Domestic Prosecution Approaches and Initiatives



- Increase Prosecutions of Identity Theft
- Enhance Training for Law Enforcement Officers and Prosecutors
- Enhance Information Sharing Between Law Enforcement and the Private Sector
 - Enhance ability of law enforcement to receive information from financial institutions
- Increase Coordination with Foreign Law Enforcement

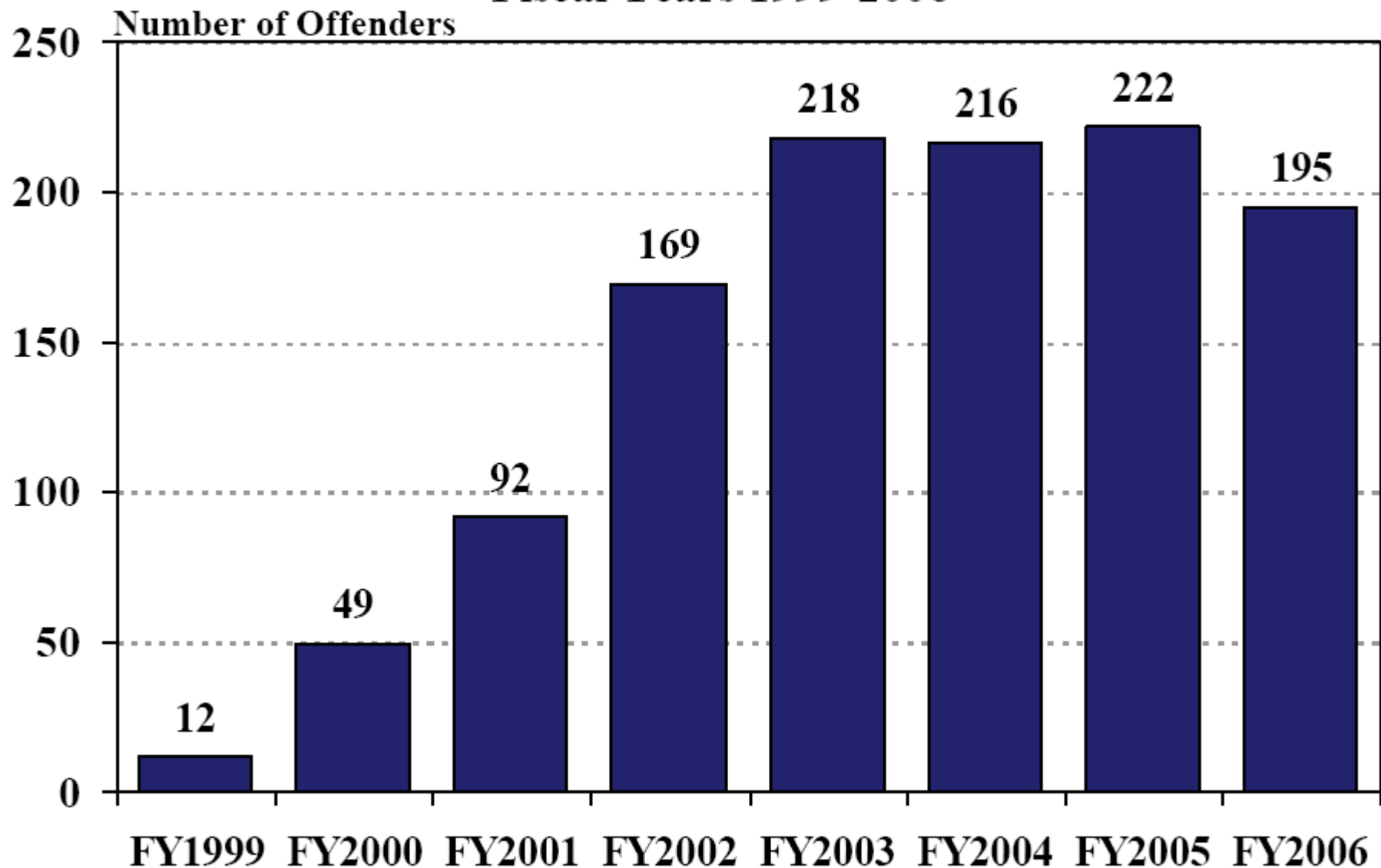
Increase Prosecutions of Identity Theft



- Create or Make Increased Use of Interagency Working Groups and Task Forces Devoted to Identity Theft
 - Federal authorities lead or co-lead more than 90 task forces or working groups dedicated (in whole or part) to identity theft
 - U.S. Attorneys' Offices lead 17 identity theft task forces and working groups
 - FBI leads four identity theft task forces
 - Secret Service leads 29 Financial Crimes Task Forces and 24 Electronic Crimes Task Forces
 - Postal Inspection Service leads 14 Financial Crimes Task Forces or Working Groups
- Support State Prosecution of Identity Theft

Trend in 18 U.S.C. § 1028(a)(7) Convictions

Fiscal Years 1999-2006



SOURCE: U.S. Sentencing Commission 1999-2006 Datafiles, USSCFY99-USSCFY06.

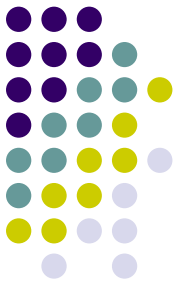
Chart includes offenders with at least one count of conviction under 18 U.S.C. § 1028(a)(7).

Law Enforcement Training



- Enhance Training for Law Enforcement Officers and Prosecutors
 - More than 20 regional identity theft training seminars for state and local law enforcement since 2002
 - Approximately 3,000 officers trained
 - No charge for seminar attendance
 - More planned for FY 2007-2008

Enhance Information Sharing Between Law Enforcement and the Private Sector



- Law enforcement works best with early notice...
- ... but companies often reluctant to report
 - Embarrassment, loss of customer trust
- Federal, state, and local law enforcement report success from outreach
 - Regional initiatives, Electronic Crime Task Forces, InfraGard
 - Key is continuous maintenance of relationship and trust
- Federal and state data breach legislation
 - Key question for law enforcement: Continue investigating or pull the plug and allow customers to be told?

Increase Coordination with Foreign Law Enforcement



- Encourage Other Countries to Enact Suitable Domestic Legislation Criminalizing Identity Theft
- Encourage Other Nations to Accede to the Convention on Cybercrime
- Identify Safe Havens for Identity Thieves and Target Those Countries for Diplomatic and Enforcement Initiatives
- Enhance U.S. Government's Ability to Respond to Appropriate Foreign Requests for Evidence in Criminal Cases Involving Identity Theft
- Assist, Train, and Support Foreign Law Enforcement
- Participate in Operational Law Enforcement Networks

Facilitate Investigation and Prosecution of International Identity Theft



- Support the Council of Europe's Convention on Cybercrime
 - The Convention is the first multilateral instrument to address the spread of criminal activity on computer networks
 - It includes criminal offenses that relate to stealing and exploiting personal information
 - It ensures that all countries that are parties to it have the ability to assist effectively in transnational identity theft cases

Assist, Train, and Support Foreign Law Enforcement



The US Department of Justice:

- Trains foreign prosecutors, legislators, judges, and law enforcement agents, often under the auspices of multilateral organizations
- Conducts bilateral cybercrime training programs with individual countries
- Leads hands-on exercises that bring together law enforcement agents from different countries

The U.S. Secret Service:

- Provides classroom training instruction on identity theft at International Law Enforcement Academies (ILEAs)



Most Important: Working Together

- Partnerships with State, Local, and International Law Enforcement
 - Identity theft must be fought at all levels
 - State and local law enforcement on front lines in investigating and receiving complaints
 - Standard ID Theft Complaint helps data sharing
 - Federal government can assist
 - International/interstate investigations
 - Training and resources for local and international investigators/prosecutors
 - Creating interagency working groups and task forces that include state and local representatives, to ensure appropriate investigation and prosecution

Takedown of Major International ID Theft Ring Through International Cooperation

NetworkWorld.com Community - Mozilla Firefox

File Edit View History Bookmarks Yahoo! Tools Help

http://www.networkworld.com/community/comment/reply/30741

Most Visited Getting Started Latest Headlines

AVG "TJX BJS: Search Total Protection AVG Info Get More

NETWORKWORLD News | Blogs & Columns | Subscriptions | Videos | Events | More

Google Custom Search Search

Security LANs & WANs VoIP Infrastructure Mgmt Wireless Software Data Center SMB Careers Toolshed Communities

NEW Buyer's Guides Tests White Papers Webcasts Solution Centers

[TJX identity theft saga continues: 11 charged with pilfering millions of credit cards](#)

Submitted by [Layer 8](#) on Tue, 08/05/08 - 6:48pm.

The Justice Department charged 11 people in connection with the massive credit and debit card number theft from various retailers, including [TJX](#), BJs and OfficeMax.

The group charged were involved in the [theft](#) of more than 40 million credit and debit card numbers that officials said they is the largest [identity-theft](#) case ever prosecuted by the Department of Justice.

In an [indictment](#) returned today by a federal grand jury in Boston, [Albert "Segevec" Gonzalez](#), of Miami, was charged with computer fraud, wire fraud, access device fraud, aggravated identity theft and conspiracy for his role in the scheme. Charges were also brought on related charges against Christopher Scott and Damon Patrick Toey, both of Miami, the DOJ said. Gonzalez was previously arrested by the Secret Service in 2003 for access device fraud. During the course of this investigation, the Secret Service discovered that Gonzalez, who was working as a confidential informant for the agency, was criminally involved in the case. Because of the size and scope of his criminal activity, Gonzalez faces a maximum penalty of life in prison if he is convicted of all the charges alleged in the Boston indictment.

Others from Estonia, China and Belarus were also charged.

The indictment alleges that during the course of the sophisticated conspiracy, Gonzalez and his co-conspirators obtained the credit and debit card numbers by "wardriving" and [hacking](#) into the wireless computer networks of major retailers - including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks, the DOJ said.

The indictment alleges that after they collected the data, the conspirators concealed the data in encrypted computer servers that they controlled in Eastern Europe and the United States. They allegedly sold some of the credit and debit card numbers, via the Internet, to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. Gonzalez and others were allegedly able to conceal and launder their fraud proceeds by using anonymous Internet-based currencies both within the United States and abroad, and by channeling funds through bank

Welcome, visitor. [Register](#) [Log in](#)

Advertisement:



September 21-23, 2009 | San Diego, CA

If you're launching the Next Big Thing, you need a big venue

DEMOfall 09 Apply to Launch
The Launchpad for Emerging Technology

rollover to find out how **xerox**

Introducing the new **ColorQube MFP**.
Solid ink saves money and



Joanna Crane
jcrane@ftc.gov

The views expressed are those of the speaker and not necessarily those of the FTC or any other person.