



# Identity Theft: A Prosecutor's Perspective

Jonathan J. Rusch  
Special Counsel for Fraud Prevention  
Criminal Division, Fraud Section  
United States Department of Justice  
Washington, DC 20530  
Liberty Alliance Identity Theft Prevention Workshop  
Chicago, Illinois  
July 17, 2005



# Overview

- A Working Definition of Identity Theft
- Federal Prosecutions of Identity-Theft Cases
- Trends and Themes in Federal Identity-Theft Prosecutions
- Identity-Theft Statutes and Guidelines
- Future Cooperation

The title is centered and surrounded by five light purple circles. One circle is positioned behind the word 'Working', another behind 'Definition', and a third behind 'of'. Below the title, there are three more circles: two solid purple circles on the left and one hollow purple circle on the right.

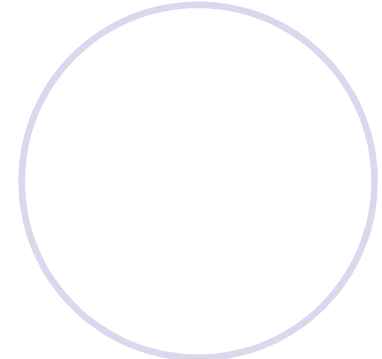
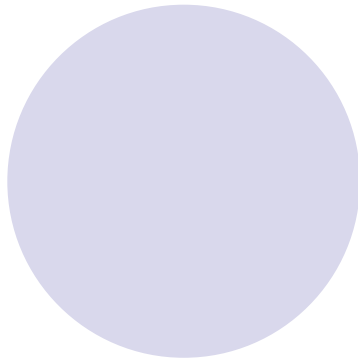
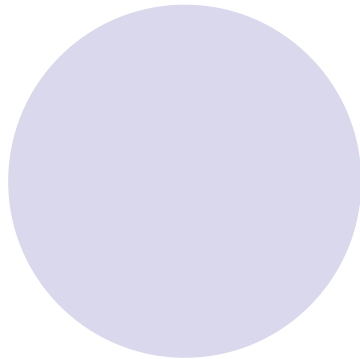
# A Working Definition of Identity Theft



# Definition

- All types of crime in which someone, without authorization, obtains, transfers, or uses another person's personal data in some way that involves fraud or deception, typically for economic gain
  - Identity theft - may be committed for various purposes (e.g., fraud, terrorism), but involves use of another real person's identity
  - Identity fraud - may involve use of wholly fictitious identity or another's real identity for fraud scheme
- Wide variety of criminal statutes applicable to identity theft and fraud
  - Wire fraud, access-device fraud, identity theft

# Federal Prosecutions of Identity-Theft Cases



# Federal Phishing Prosecutions - Examples

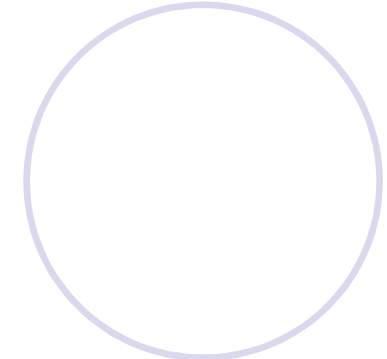
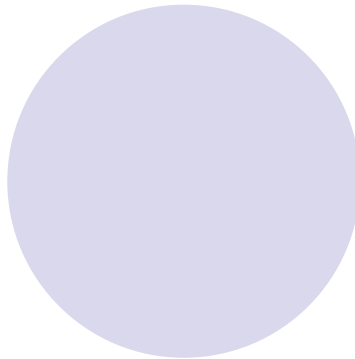
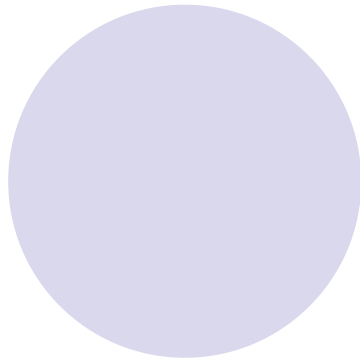
- U.S. v. Carr (E.D. Va., sentenced January 2004)
  - Defendants used spoofed AOL emails, website
  - Lead defendant, 55, sentenced to 46 months imprisonment, second defendant to 37 months imprisonment
- U.S. v. Paperniak (N.D. Cal., pleaded guilty February 3, 2004)
  - Defendant, 20, used spoofed PayPal emails and webpages and sent keyloggers to PayPal users
- U.S. v. Chacin (N.D. Cal., sentenced May 3, 2004)
  - Defendant, 21, used spoofed eBay emails and webpages
  - Sentenced to 33 months imprisonment
- U.S. v. Hill (S.D. Tex., sentenced May 17, 2004)
  - Defendant, 20, used spoofed eBay and AOL emails and webpages
  - Sentenced to 46 months imprisonment
- U.S. v. Defelippi (W.D.N.Y., pleaded guilty May 10, 2005)
  - Defendant, 23, created numerous spoofed websites
  - Plea agreement anticipates that Defelippi sentence will be between 71 and 95 months imprisonment, due in part to plea to aggravated identity theft

# Other Federal Identity-Theft Prosecutions

## – Card Skimming and ATM Fraud

- Since 2003, Federal Prosecutions of Skimming Cases in Dallas, Los Angeles, Miami, New Haven, New Orleans (Among Others)
- Example: U.S. v. Codarcea (D.N.H., second superseding indictment returned July 6, 2005)
  - Defendant (Romanian national living in Quebec) and coconspirators allegedly used concealed devices at Bank of America ATM facilities in Massachusetts and New Hampshire to secretly obtain account data and PINs when bank customers used their ATM cards at the ATM facilities
  - Unauthorized cash withdrawals totaled approximately \$365,000

# Trends and Themes in Federal Identity-Theft Prosecutions



# Involvement of Professional Criminals in Phishing and Carding

- U.S. v. Vega (N.D. Cal., extradited June 2004)
  - Defendant allegedly used Internet chat rooms to traffic in credit-card data of thousands of individuals that had been illegally obtained from sources around the world, including credit card processors and merchants
  - Defendant also allegedly an operator of website where stolen and counterfeit credit-card account data bought and sold
- U.S. v. Mantovani et al. (D.N.J., indicted Oct. 28, 2004)
  - 19 individuals from across the United States and in several foreign countries allegedly conspired with others to operate "Shadowcrew"
  - Shadowcrew.com a website with approximately 4,000 members that was dedicated to facilitating malicious computer hacking and the dissemination of stolen credit card, debit card and bank account numbers and counterfeit identification documents, such as drivers' licenses, passports and Social Security cards
  - Account numbers and other items allegedly sold by approved vendors who had been granted permission to sell by operators and moderators of the Shadowcrew site after completing a review process
  - Shadowcrew members allegedly trafficked in at least 1.7 million stolen credit-card numbers and caused more than \$4 million in losses

# Diversification of Means of Acquiring Personal Data

- U.S. v. Defelippi (W.D.N.Y., pleaded guilty May 10, 2005)
  - From 2001 to 2004, defendant ran illegal business where he would purchase or obtained through phishing stolen credit card information, such as account numbers, names and Social Security numbers, from individuals located in Eastern Europe
  - Defendant purchased information relating to more than 9,000 credit cards from various illegal websites
  - Defendant used credit-card data to produce false credit cards using special manufacturing equipment he had obtained, made false Massachusetts driver's licenses, then sold these documents and shipped them interstate
  - Defendant also used false credit cards and identification documents he produced to buy items, such as computers, then sold items on eBay and shipped them interstate to purchasers

# Use of Keyloggers



- U.S. v. Paperniak (N.D. Cal., pleaded guilty February 3, 2004)
  - Phisher use of keyloggers with PayPal users
- U.S. v. Salcedo (W.D.N.C., sentenced Dec. 15, 2004)
  - Defendants secretly compromised wireless network at Lowe's retail store in Southfield, Michigan, and gained unauthorized access to Lowe's central computer system in North Wilkesboro, North Carolina and to computer systems located in Lowe's stores around the country
  - Defendants then installed on computer system of several Lowe's stores a computer program designed to capture credit-card information of customers conducting transactions with those stores
  - Defendant sentenced to 9 years imprisonment
- U.S. v. Jiang (S.D.N.Y., sentenced Feb. 28, 2005)
  - Defendant, 24, installed keylogging software on computer terminals located at Kinko's stores throughout Manhattan to collect computer usernames and passwords of Kinko's customers
  - Used the confidential information he obtained to access, or attempt to access, bank accounts belonging to other persons, and fraudulently to open online bank accounts
  - Defendant sentenced to 27 months imprisonment

# Compromise of Corporate Insiders – Third-Party Service Organizations

- United States v. Cummings (S.D.N.Y., criminal complaint unsealed Nov. 25, 2002)
  - Defendant a help-desk employee at company that provided computerized access for banks and other entities to credit reports from three leading credit bureaus
  - Defendant sold credit reports to others
  - More than 30,000 victims, estimated losses of \$50 million to \$100 million
  - Lead defendant sentenced in 2005 to 14 years imprisonment

# Compromise of Corporate Insiders – Retail Services

- U.S. v. Dean (C.D. Cal., sentenced Feb. 27, 2004)
  - 24-year-old college student got credit-card and other data for more than 50 people, from girlfriend who worked at amusement park and processed requests for annual passes
  - Student used credit-card data to make online purchases from Ticketmaster and several airlines; bought tickets for various events and sold them, often for well below face value
  - Sentenced to 33 months imprisonment, \$13,965 restitution to Ticketmaster and Southwest Airlines
- U.S. v. Moore (D. Conn., sentenced May 18, 2004)
  - Defendant, owner of company that installed home security systems, took customers' personal information to apply for and get multiple credit cards in victims' names and SSNs
  - Defendant provided own home address or company's address so account statements went to him and not victims
  - Defendant also used victims' data to buy Chevy S-10 pickup trucks, Mercedes-Benz S420, fishing boat (and auto insurance on cars)
  - Sentenced to 43 months imprisonment, \$209,669 restitution

# Identity-Theft Statutes and Guidelines

The title is centered and surrounded by five circles. One circle is white with a light purple outline and is positioned behind the word 'Theft'. Two solid light purple circles are located below the word 'Theft'. Two more solid light purple circles are positioned behind the words 'Statutes' and 'and'. A final white circle with a light purple outline is located below the word 'Guidelines'.

# Identity Theft (18 U.S.C. 1028(a)(7))

- Offense
  - Knowing transfer, possession, or use, without lawful authority, of a means of identification of another person with the intent to commit, or aid and abet, or in connection with any unlawful activity that constitutes a federal offense or a state or local felony
- Statutory Terms
  - “Means of identification” – Any name or number that may be used, alone or with any other information, to identify a specific individual [18 U.S.C. § 1028(d)(4)]
    - Includes name, Social Security number (SSN), date of birth, driver’s license, passport number, biometric data, access devices (e.g., credit-card numbers)

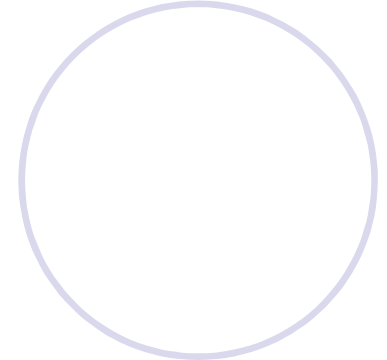
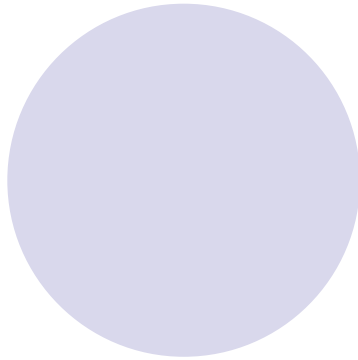
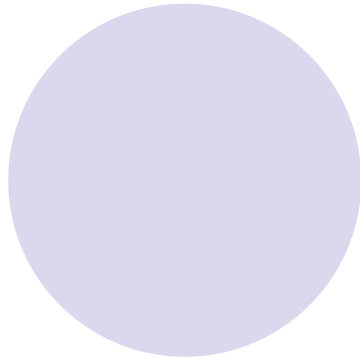
# Aggravated Identity Theft (18 U.S.C. 1028A)

- Ensures a two-year sentence over and above any sentence otherwise applicable in wide range of federal offenses, including fraud
- For terrorism-related offenses, ensures a five-year sentence over and above any sentence otherwise applicable in underlying terrorism-related offenses

# Federal Sentencing Guidelines

- Specific enhancement for certain kinds of identity theft-related conduct (e.g., production of unauthorized access devices) upon conviction in federal court
- Discretionary increase possible where, for example –
  - Offense caused substantial harm to victim's reputation or credit record, or victim suffered substantial inconvenience related to repairing reputation or credit record
  - Defendant essentially assumed victim's identity

# Suggestions for Future Cooperation



# Cooperation at All Levels of Government

- International

- United Nations Crime Commission Expert Group on Fraud and Criminal Misuse of Identity, 2005-
  - Report to identify best practices for private sector and law enforcement
- Expanded outreach to foreign ISP associations and CERTs
  - EuroISPA, Asia & Pacific Internet Association

- National, Regional, Local

- Development of contacts and relationships with –
  - Regional law enforcement task forces devoted to identity theft
  - Specific agencies (e.g., United States Attorneys, FBI, Secret Service, Postal Inspection Service)

# Contact Information



- [Jonathan.Rusch2@usdoj.gov](mailto:Jonathan.Rusch2@usdoj.gov) [E-Mail]
- 202-514-0631 [Office]
- 202-514-7021 [Fax]
- 10<sup>th</sup> Street & Constitution Avenue, Bond Building, Room 4300, Washington, DC 20530 [Mail]