Issues in Enforcement Collaboration: A Fraud Enforcement Perspective

Jonathan J. Rusch
Deputy Chief for Strategy and Policy
Fraud Section, Criminal Division
U.S. Department of Justice
Atlanta, GA
November 17, 2011

Overview

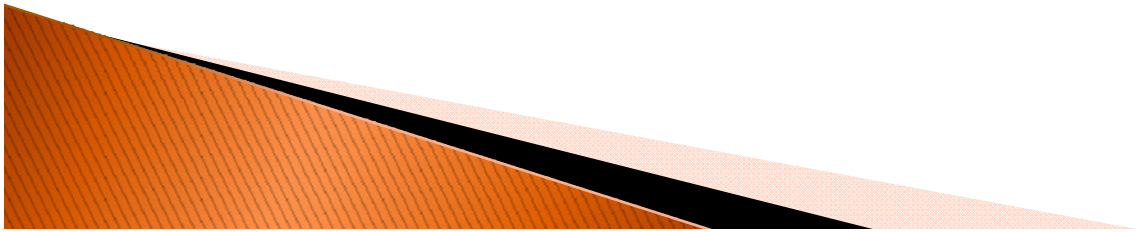
- Key Trends
  Law Enforcement Responses

Key Trends

- Payments Fraud

AFP Payments Fraud and Control Survey (March 2011)

- Organizations Subject to Actual or Attempted Payments Fraud: 71 Percent
  - Revenues under $1 billion: 58 percent
  - Revenues over $1 billion: 82 percent
- 29 Percent of Respondents Reported That Fraud Incidents Increased in 2010 Over 2009
  - 52 Percent: No Change



AFP Payments Fraud and Control Survey (March 2011)

Payment Methods	All Respondents	Revenues <$1 Billion	Revenues > $1 Billion
Checks	93%	84%	95%
ACH Debits	25	26	26
Consumer Credit/Debit Cards	23	19	20
Corporate/Commercial Purchasing Cards	15	19	18
ACH Credits	4	--	11
Wire Transfers	4	2	2

AFP Payments Fraud and Control Survey (March 2011)

- Payments Methods Subject to More Fraud in 2010 Over 2009

Payment Methods	More	About The Same	Less
Checks	30%	50%	20%
Consumer Credit/Debit Cards	18	68	14
Corporate Cards	16	69	15
ACH Debits	15	61	24
Wire Transfers	5	74	21
ACH Credits	3	74	23

AFP Payments Fraud and Control Survey (March 2011)

- Types of Fraud Resulting from Check Use

Fraud Type	All Respondents	Revenues < $1 Billion	Revenues > $1 Billion
Counterfeit Checks (Non-Payroll) Using Organization's MICR Line	68%	64%	71%
Payee Name Alteration	56	50	59
Dollar Amount Alteration	35	34	35
Counterfeit Checks With Company Name but Another Company's Account Data	28	27	28
Loss/Theft/Counterfeit of Employee Paychecks	19	13	21
Other	4	8	3

AFP Payments Fraud and Control Survey (March 2011)

- Frequency of Actual or Attempted ACH Fraud in 2010

Number of Attempts	All Respondents	Revenues < $1 Billion	Revenues > $1 Billion
1-5	65%	71%	63%
6-10	16	14	15
11-15	8	10	7
16-20	3	5	3
20 or More	8	--	12
Median No. of Incidents	4	4	4

Anti-Phishing Working Group, Global Phishing Survey (2H2010)

- At Least 67,677 Phishing Attacks Worldwide
  - Attacks occurred on 42,624 unique domain names
    - 11,769 (28 percent) were registered maliciously by phishers
    - Bulk of the remaining 28,537 domains "compromised" or hacked
  - Malicious use of subdomain registration services nearly doubled in the second half of 2010, and accounted for the majority of phishing in many TLDs
    - Nearly 700 subdomain registration providers, which offer services on more than 3,200 domain names
- Average and Median Uptimes of Phishing Attacks Rose Throughout 2010
  - Average uptime: 73 hours
    - Longest average for any time period in last three years

Internet Crime Complaint Center

- Alerts
  - April 2011
    - Use of compromised online banking credentials of U.S. businesses to send unauthorized wire transfers to Chinese economic and trade companies located near the Russian border
      - March 2010 – April 2011, 20 incidents in which online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies
      - Typical scenario: computer of a person within a company who can initiate funds transfers on behalf of the U.S. business is compromised by either a phishing e-mail or by visiting a malicious Web site; malware harvests the user's corporate online banking credentials
      - As of April 2011, total attempted fraud approximately $20 million; actual victim losses $11 million
  - May 2011:
    - Counterfeit check scams targeting realtors and real estate attorneys

European ATM Security Team (EAST), ATM Fraud Analysis Report (June 2011)

- ATM Skimming Losses in 2H 2010:
  - Domestic issuer losses: €23 million
    - 62 percent decrease from €62 million in 1H2006
  - International losses: €100 million
    - 64 percent decrease from 2H2007
    - Counterfeit EU payment cards are used to make cash withdrawals in countries where all or some of the ATMs are not yet EMV compliant
- "Many EU countries are now reporting that losses in the United States are making up the largest percentage of international losses, where there are no known plans to migrate to EMV."

Key Trends

- Mass-Marketing Fraud

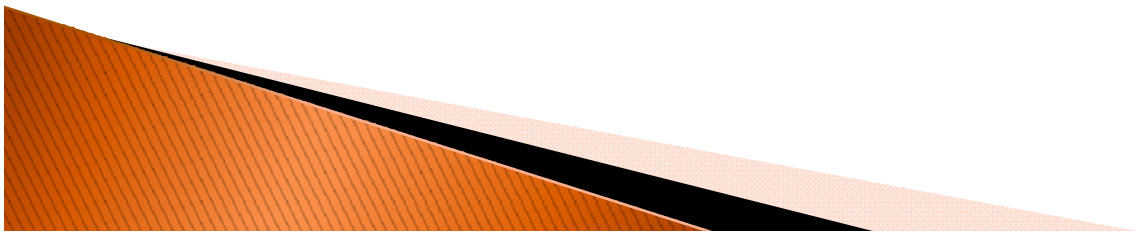
International Trends

- International Mass-Marketing Fraud Working Group, Mass-Marketing Fraud: A Threat Assessment (2010)
  - Mass-Marketing Fraud Increasingly Global in Scope and Effects Over Last Decade
    - Order of magnitude of annual global losses: tens of billions of dollars
  - Mass-Marketing Fraud Has Substantial Impact on Economies and Markets
    - Consumer trust and confidence in legitimate business
  - Large-Scale Criminal Mass-Marketing Fraud Operations Present in Multiple Countries in Most Regions of the World

Example – Europe

Râmnicu Vâlcea – Distinguishing Features

- City of 120,000 in Romania
- Key Node for Internet Fraud
  - "Hackerville"
  - Luxury car dealerships
  - "At least two dozen [money-transfer service] locations lie within a four-block area downtown" (Wired, January 2011)



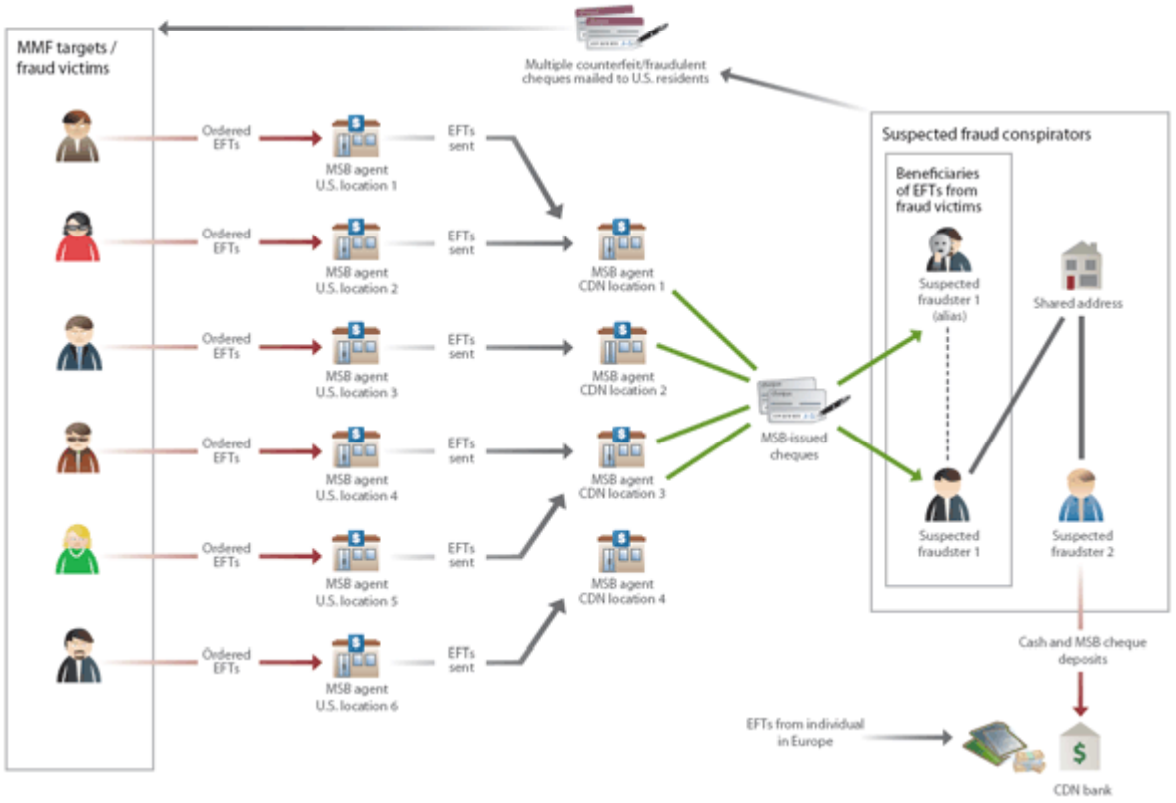
Example – Asia

- June 2011: 598 Suspects Arrested in 160 Locations in Mass-Marketing Fraud Schemes
  - Various telemarketing schemes to induce Chinese and Taiwanese victims to –
    - Purchase goods that were never sent
    - Make funds transfers from bank accounts
    - Pay nonexistent traffic or court summonses
  - Arrests included –
    - 186 in Cambodia
    - 170 in Indonesia
    - 37 in Malaysia

Key Points of Vulnerability

- Mass-Marketing Techniques
  - Internet
  - International Telephone Service
  - Mass Mailing
- Counterfeit Financial Instruments
- Money Transfer Services
- Money Laundering
  - Inspector Nelson Cheng, Hong Kong Police: " . . . money laundering forms an essential component of these fraudulent operations, and the ease with which proceeds can be moved across borders is a primary factor facilitating the success of the operations."

Key Points of Vulnerability



Law Enforcement Responses

- Prosecutions
- Bi- and Multilateral Collaboration

Prosecutions

- U.S. v. Merzi et al. (C.D. Cal., convicted at trial March 26, 2011)
  - Case part of Operation "Phish Phry," a multinational investigation conducted in the United States and Egypt that led to charges against 100 individuals – the largest number of defendants ever charged in a cybercrime case
  - Egyptian-based hackers obtained bank account numbers and related personal identification information from an unknown number of bank customers through phishing
  - Once they accessed the accounts, the individuals operating in Egypt communicated via text messages, telephone calls, and Internet chats with co-conspirators in the United States
    - Through these communications, members of the criminal ring coordinated the illicit online transfer of funds from the compromised accounts to newly created fraudulent accounts
  - Ages of five defendants convicted at trial: 21, 22, 22, 22, 25
  - 41 others previously convicted in federal court

Prosecutions

- U.S. v. Tsastsin et al. (S.D.N.Y., arrested November 8, 2011)
  - Indictment charging seven foreign defendants with engaging in massive click-fraud scheme
    - Defendants allegedly distributed viruses and malware that infected more than 4 million computers in more than 100 countries and grossed at least $14 million
    - At least 500,000 computers in the United States were infected, including computers of NASA, educational institutions, nonprofit organizations, commercial businesses, and private citizens
    - Defendants allegedly sent malware that altered computer settings to reroute users to websites and advertisements
    - Each time that users clicked on or viewed these websites, defendants collected a commission
  - 6 Estonian nationals -- Vladimir Tsastsin, 31; Timur Gerassimenko, 31; Dmitri Jegorov, 33; Valeri Aleksejev, 31; Konstantin Poltev, 28; and Anton Ivanov, 26 -- arrested on Tuesday by Estonian police and border guard
  - Seventh defendant, a Russian national, remains at large

Bi- and Multilateral Collaboration

- International Treaties and Conventions
  - Bilateral Mutual Legal Assistance Treaties
  - United Nations Transnational Organized Crime Convention
  - Council of Europe Cybercrime Convention
- Domestic Processes for Collaboration
  - Foreign Evidence Request Efficiency Act of 2009
    - Expanded authority to execute requests for assistance in foreign investigations and prosecutions of criminal offenses, and prosecution-related proceedings (e.g., forfeiture, sentencing, and restitution)
    - Includes search warrants, warrants for stored wire or electronic communications, orders to compel appearance for testimony
  - FTC SAFEWEB Act
- Transnational Organized Crime Strategies
  - United States, United Kingdom
- Working Groups
  - International Mass-Marketing Fraud Working Group
    - Law enforcement representatives from Australia, Belgium, Canada, Netherlands, Nigeria, United Kingdom, United States
- Training of Foreign Law Enforcement
  - International Law Enforcement Academies
  - 2011 Cybercrime Training in Kenya

Contact Data

- Jonathan.Rusch2@usdoj.gov
- 202-514-0631 [Office]
- 202-514-7021 [Fax]
- 10th Street and Constitution Avenue, N.W., Bond Building, Room 4414, Washington, DC [Mail]