





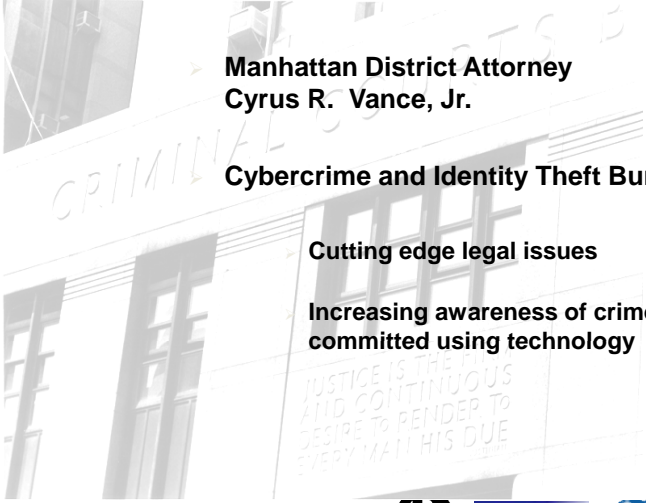
ABA Professional Development

ABA/ABA Money Laundering Enforcement Conference

November 13-15, 2011
Washington, DC




Cybercrime and Identity Theft Bureau






Manhattan District Attorney
Cyrus R. Vance, Jr.

Cybercrime and Identity Theft Bureau

- Cutting edge legal issues
- Increasing awareness of crimes committed using technology



Cyrus R. Vance, Jr.
District Attorney



Facts about Manhattan

- **1,585,873** people
- **23** square miles
- 28.8 million visitors in 2010



Cybercrime and Identity Theft Bureau

- 10 full time Assistant District Attorneys
- 70 additional Assistant District Attorneys
- Cases range from assistance on homicides and sex crimes to development of hacking, intrusion and large scale cyber fraud identity theft rings



Cybercrime and Identity Theft Bureau

- Summary arrests by NYPD
- Mining of arrests/patterns develop
- FINCEN access
- SAR review team
- Forensic lab
- In house investigators



CRIMINAL JUSTICE



Pool of Cases

- Over 100,000 crimes prosecuted/year
- We review 200-300 cases/month
- Cybercrime and identity theft are among the fastest growing crimes in the U.S.
- Some Manhattan police precincts report that identity theft is their most frequently reported crime. Ironically, while incidents of violent crime have largely decreased in New York, prosecutions for cybercrime and identity theft have grown at an alarming rate – up about 50% in the past five years.



CRIMINAL JUSTICE



Cybercrime and Identity Theft Bureau

- Track cases and find important links between them
 - invaluable tool in discerning criminal patterns and typologies, and in identifying criminal organizations that would otherwise go undetected.
- Full-time and other major case ADAs conduct intensive, long-term investigations and prosecutions of national and international criminal organizations as part of our Investigation Division. This mission includes developing long-term malware, hacking and intrusion investigations as well as sophisticated cyber-frauds.



Trends

- Gangs
- Malware
- Insiders
- Check fraud
- Purchasing of personal identifying information from web based portals
 - S3 Apple case
 - Sale of PII based on amount of credit limit



Trends

- Social Networking
- p2p
- Gaming
- Mobile Banking
- Digital currencies
- Prepaid access
 - Green Dot cards
 - Gift cards



Communications Stats

- Three billion phone calls are made every day in the US, which breaks down to 34,722 per second
- 150 Million Landlines (2008)
- In 2008 there were 270 Million cell phone subscribers
- Cell phone usage in the US has increased yearly
- 1.4 Trillion text messages were sent in 2008
 - 4.1 billion a day
- 107% increase from 2007
- In 2007 it was estimated that 183 billion emails were sent per day



Cell Phone Forensics in 2011



Defending Liberty
Pursuing Justice

CRIMINAL
JUSTICE



American
Bar Association
ABA Professional Development

Pump Up The Volume

NY CTY DA HTAU PHONE INTAKES

2008 - **639** Phones

2009 – **772** Phones

2010 – **861** Phones

October 2010 - **70** Phones (40 New cases)

18 Related to Homicide Investigations (Roughly 26%)



Defending Liberty
Pursuing Justice

CRIMINAL
JUSTICE



American
Bar Association
ABA Professional Development



Computers

- **2008**- 456 hard drives taken in by HTAU
- **2009**- 549 hard drives
- **2010**- 577 hard drives



CRIMINAL
JUSTICE



Case examples

- Western Express- cyber ring laundering money through digital currencies
- ACH Russian Fraud- on-line banking leads to malware leads to laundering
- People v. Osahon- credit report cyber fraud



CRIMINAL
JUSTICE



WESTERN EXPRESS

- •“WE I” First Indictment (check cashing -4 defendants –WE and high managerial agents)
- •“WE II” Second and Current Indictment (18 defendants –WE and high managerial agents + 14 of their customers –carding and digital currency)



CRIMINAL JUSTICE



NY CTY DA

USSS



- DOJ-OIA, HCPO (NJ), NYSP, LA Co DA (CA), DEA
- NYS BANKING DEPARTMENT
- FINANCIAL INSTITUTIONS



CRIMINAL JUSTICE





WESTERN EXPRESS



 Stolen credit card #s
 used to buy merchandise,
 reseller uses egold to make
 payment
 Reseller puts good for sale
 on ebay


 **CRIMINAL JUSTICE**
 Defending Liberty Pursuing Justice

 American Bar Association
 ABA Professional Development

WE- Initial Investigation

- *2005: Report of identity theft –stolen CC*
- •*Drop in Manhattan*
- •*Drop paid for merchandise with Egold*
- •*Traced Egold indirectly to Western Express*
- •*Western Express located in Manhattan*
- •*Financial analysis of Western Express*

 **CRIMINAL JUSTICE**
 Defending Liberty Pursuing Justice

 American Bar Association
 ABA Professional Development

Digital Currency

- Western Express was used to launder and convert over \$600,000 in Egold digital currency criminal proceeds into Webmoney digital currency.
- Group communicated through carding Web sites Web sites devoted to trafficking in stolen credit card and personal identifying information.
- They relied on the use of nicknames, false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous digital currency accounts to conceal the existence and purpose of the criminal enterprise



Carders


- “Carding” = trafficking in and using stolen credit card information
- Domestic carders: Forge CCs and go shopping
- Overseas carders: Make millions from fraud in the U.S. without stepping foot into the U.S.
 - -Vend stolen credit card data to U.S. based criminals
- Recruit individuals in the U.S. to receive or resell merchandise purchased via the internet with stolen credit card information



The business

- Located in Manhattan
- Incorporated in New York State
- Business run by Vadim Vassilenko, Yelena Barysheva, and Alexey Baryshev
- Multiple websites, many in Russian
- Multiple advertised services
- **Catered to “carders”**- Individuals who traffic in stolen credit card information





ABA
Defending Liberty
Pursuing Justice

CRIMINAL
JUSTICE

American
Barbers
Association
ABA Professional Development

Western Express' Business Activities

- Websites to drive business
- **Illegal Check Cashing and Money Transmitting**
- \$4,000,000 + (4 year period)
- Mail receiving & Taxpayer ID services
- Resale of stored value cards (gift cards)
- Money orders
- Agent of money transmitters
- Miscellaneous services (Phone cards, Translation)
- **Digital Currency Exchange & Money Laundering:**(Egold, Webmoney, USC)
\$35,000,000 + (5 year period)
 - Egold purchase: \$20,000,000
 - Webmoney purchase: \$15,000,000

Western- 1st Indictment

- February 2006: 1st Indictment
- Indictment of Western Express and principals for Illegal Check Cashing and Illegal Money Transmitting
 - (Vassilenko, his wife Barysheva, his stepson)
- Search warrants by DANY Investigators & USSS, with Hudson Co. NJ, & NYSP
 - 7 locations: NY & NJ. Office, residences, mail receivers
- Recovered roomful of documents & dozens of computers



CRIMINAL
JUSTICE



Western 1

- New York State Banking Law requires check cashers and money transmitters to be licensed by NYS
- Western Express was not licensed by NYS
- Western Express was in the business of depositing checks, and transmitting the proceeds for customers



CRIMINAL
JUSTICE



Charges

- February 2006:
- Indictment for Check Cashing Activity
- Unlicensed Check Cashing NY Banking Law §367(1) (Misdemeanor)
- Unlicensed Money Transmitting NY Banking Law §650(2)(b)(1) (“E” Felony)
- Falsifying Business Records 1stDegreeNY Penal Law §175.10 (“E” Felony)



After WE 1

- Analyzed voluminous evidence and records
- Investigation continued into Western Express and their customers
- Focus on carder customers and digital currency.



Enterprise Corruption Statute

- August 2007: 2nd Indictment
- “Enterprise Corruption”, NY’s RICO law
- 18 defendants (Western Express and customers)
- 173 counts related to stolen credit card data trafficking, larceny, digital currency money laundering, etc



CRIMINAL
JUSTICE



Western Express 2

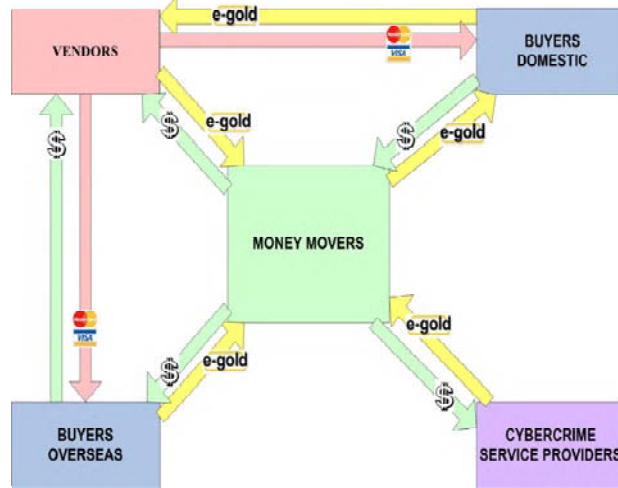
- August 2007 – 2nd Indictment
- Criminal Enterprise (18 members indicted) consisting of:
 - “Money Movers” (Western Express)
 - “Buyers” of stolen credit card information
 - “Vendors” of stolen credit card information
 - “Cybercrime Service Providers”
- Targets: 13 domestic, 5 overseas



CRIMINAL
JUSTICE



Structure of Organized Crime



The defendants

WESTERN EXPRESS CYBERCRIME GROUP ALL DEFENDANTS			
	MONEY MOVER - DEBIT	MONEY MOVER - CREDIT	BUYER - BLUE
1	WESTERN EXPRESS INTERNATIONAL, INC MONEY MOVER & CYBERCRIME SERVICES PROVIDER		10 DOUGLAS LATTA , a/k/a "Kelly Graham", "Real" BUYER (domestic)
2	VADIM VASSILENKO MONEY MOVER & CYBERCRIME SERVICES PROVIDER		11 ANGELA PEREZ , a/k/a "Kelly Graham" BUYER (domestic)
3	YELENA BARYSHEVA MONEY MOVER & CYBERCRIME SERVICES PROVIDER		12 KOSTAS KAPSIS , a/k/a "TheVipir", "Mike Belios" BUYER (domestic)
4	TATIANA GOLOBORODKO a/k/a "Anna Golubenko" MONEY MOVER & CYBERCRIME SERVICES PROVIDER		13 LYNDON ROACH a/k/a "Robert Hanson", "Robert Taylor" BUYER (domestic)
5	EGOR SHEVELEV a/k/a "Eskalibur" VENDOR		14 JERMAINE VANN indicted as JOHN DOE "Chacha" a/k/a "Vanilla", a/k/a "Calvin Davis", "BOP" BUYER (domestic)
6	DZIMITRY BURAK , a/k/a "Graph", a/k/a "Kurochkin" VENDOR & CYBERCRIME SERVICES PROVIDER		15 KEITH CLIMMINGS , a/k/a "Anthony Marshall", "Pincustion" BUYER (domestic)
7	OLEG COVELIN a/k/a Oleg Kovelin a/k/a "DoZ" CYBERCRIME SERVICES PROVIDER		16 JOHN WASHINGTON , a/k/a "thahakid" BUYER (domestic)
8	VIATCHESLAV VASILYEV , a/k/a "TheViver" BUYER (domestic)		17 EDUARD KHOLSTININ , a/k/a "Andrew Ronin", "V.O.R.", "BOP" BUYER (domestic)
9	VLADIMIR KRAMARENKO , a/k/a "Inexwor", "Envisor" BUYER (domestic)		18 ALEXEY YARNE , a/k/a "President" BUYER (domestic)



Challenges

Problems in international cyber investigations

- Identification of targets
- Apprehension of targets
- Extradition of targets



CRIMINAL
JUSTICE



Student Visa Investigation

- Organized cyber crime- 2010
 - Malware placed on the computers of unsuspecting victims (Zeus Trojan)
 - Passwords and usernames compromised
 - Information coordinated from Eastern Europe

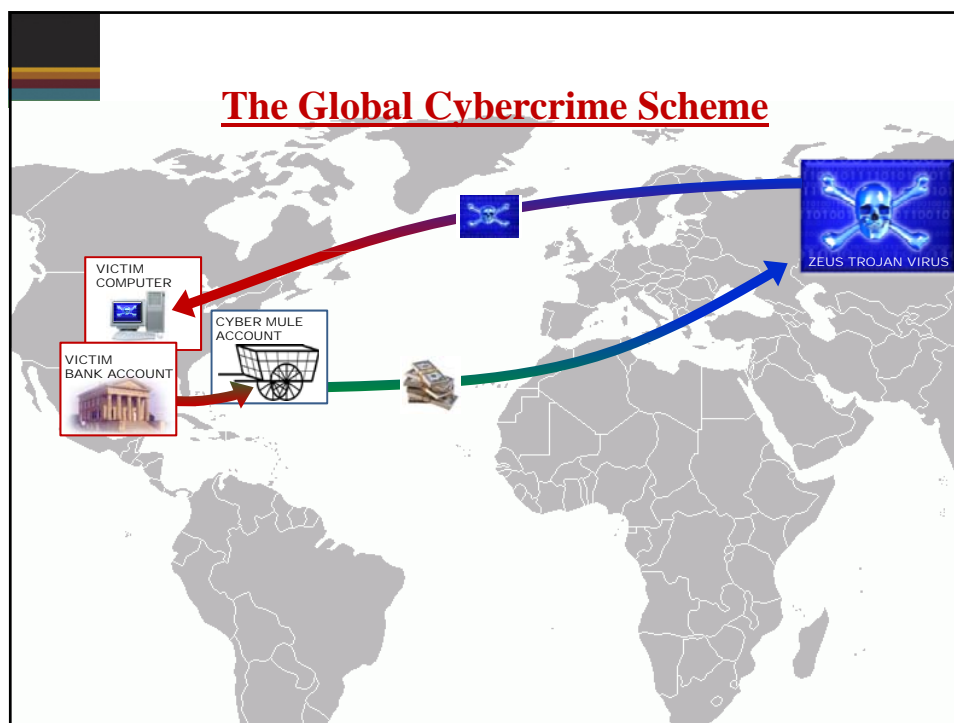


Cyrus R. Vance, Jr.
District Attorney



CRIMINAL
JUSTICE





Student Visa Investigation

- Russians recruited handlers and money mules
 - Russian Social Networking sites
 - In the United States, recruited off of Russian newspapers in Brooklyn
 - Young adults here on J1 Visas

J1 Visa Investigation

- J1 Visa holder would go into bank
- Open account in own name
- Account information then provided to handlers
- \$ moved into J1 Visa account
- \$ withdrawn then by J1 account holder
- \$ given to handler and then wired overseas



CRIMINAL
JUSTICE



Student Visa Investigation

- Summary arrests begin by the NYPD
 - Banks in NYC begin to see pattern
 - Influx of J1 Visa recipients arrested
 - Debriefings
 - Forensics
 - Analysis of arrest data



CRIMINAL
JUSTICE



Student Visa Investigation

- DANY Investigation
 - Over \$850,000 primarily from one major bank
 - 55 defendants indicted total
 - Some literally pulled off of planes heading back to Russia
 - Roomates
 - Charges: Grand Larceny, Money Laundering



CRIMINAL
JUSTICE



Student Visa Investigation

- Victims were spread across the United States
- What can financial institutions do?
 - Worked closely to try and create flags based on the use of J1 visas
 - Cyber security systems of the banks generally not compromised, users were



CRIMINAL
JUSTICE





Thank You!

David Szuchman

Szuchmand@dany.nyc.gov

(212) 335-9610

Questions?

