

UNITED STATES ATTORNEY'S OFFICE

Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE Tuesday, June 26, 2012 http://www.justice.gov/usao/nys

CONTACT: <u>U.S. ATTORNEY'S OFFICE</u>

Ellen Davis, Jerika Richardson,

Jennifer Queliz (212) 637-2600

FBI

Tim Flannelly, Jim Margolin

(212) 384-2100

MANHATTAN U.S. ATTORNEY AND FBI ASSISTANT DIRECTOR-IN-CHARGE ANNOUNCE 24 ARRESTS IN EIGHT COUNTRIES AS PART OF INTERNATIONAL CYBER CRIME TAKEDOWN

Two-Year FBI Undercover "Carding" Operation Protected Over 400,000 Potential Cyber Crime Victims and Prevented Over \$205 Million in Losses

Preet Bharara, the United States Attorney for the Southern District of New York, and Janice K. Fedarcyk, the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced today the largest coordinated international law enforcement action in history directed at "carding" crimes – offenses in which the Internet is used to traffic in and exploit the stolen credit card, bank account, and other personal identification information of hundreds of thousands of victims globally. Today's coordinated action – involving 13 countries including the United States – resulted in 24 arrests, including the domestic arrests of 11 individuals by federal and local authorities in the United States, and the arrests of 13 individuals abroad by foreign law enforcement in seven countries. In addition, the federal and local authorities, and authorities overseas, today conducted more than 30 subject interviews, and executed more than 30 search warrants. Today's coordinated actions result from a two-year undercover operation led by the FBI that was designed to locate cybercriminals, investigate and expose them, and disrupt their activities.

Eleven individuals were arrested today, and one last night, in the United States: CHRISTIAN CANGEOPOL, a/k/a "404myth," was arrested today in Lawrenceville, Georgia, MARK CAPARELLI, a/k/a "Cubby," was arrested in San Diego, California; SEAN HARPER, a/k/a "Kabraxis314," was arrested in Albuquerque, New Mexico; ALEX HATALA a/k/a "kool+kake," was arrested in Jacksonville, Florida; JOSHUA HICKS, a/k/a "OxideDox," was arrested in Bronx, New York; MICHAEL HOGUE a/k/a "xVisceral," was arrested in Tucson, Arizona; MIR ISLAM, a/k/a "JoshTheGod," was arrested in Manhattan, New York; PETER KETCHUM, a/k/a "IwearaMAGNUM," was arrested in Pittsfield, Massachusetts; STEVEN HANSEN a/k/a "theboner1," was arrested in Wisconsin, where he is currently serving a prison sentence on state charges. In addition, two minors, whose names will not be made public, were arrested by local authorities in Long Beach and Sacramento, California. HICKS and ISLAM will be presented later today before a magistrate judge in the Southern District of New York. The other federally arrested defendants will be presented before magistrate judges in the corresponding federal districts of arrest.

Another 13 individuals were arrested today in seven foreign countries. Eleven of those individuals were arrested as a result of investigations commenced in foreign jurisdictions based in part on information arising out of the undercover operation and provided by the FBI to foreign law enforcement. Those 11 arrests occurred in: the United Kingdom (6 arrests), Bosnia (2), Bulgaria (1), Norway (1), and Germany (1). Two additional defendants were arrested today in foreign countries based on provisional arrest warrants obtained by the United States in connection with Complaints unsealed today in the Southern District of New York. Those two individuals are: ALI HASSAN, a/k/a "Badoo," who was arrested in Italy; and LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," who was arrested in Japan. Australia, Canada, Denmark, and Macedonia conducted interviews, executed search warrants, or took other coordinated action in connection with today's takedown, including.

Charges were also unsealed in the Southern District of New York against four additional defendants who remain at large.

Manhattan U.S. Attorney PREET BHARARA said: "As the cyber threat grows more international, the response must be increasingly global and forceful. The coordinated law enforcement actions taken by an unprecedented number of countries around the world today demonstrate that hackers and fraudsters cannot count on being able to prowl the Internet in anonymity and with impunity, even across national boundaries. Clever computer criminals operating behind the supposed veil of the Internet are still subject to the long arm of the law.

The allegations unsealed today chronicle a breathtaking spectrum of cyber schemes and scams. As described in the charging documents, individuals sold credit cards by the thousands and took the private information of untold numbers of people. As alleged, the defendants casually offered every stripe of malware and virus to fellow fraudsters, even including software enabling cyber voyeurs to hijack an unsuspecting consumer's personal computer camera. To expose and prosecute individuals like the alleged cyber-criminals charged today will continue to require exactly the kind of coordinated response and international cooperation that made today's arrests possible."

FBI Assistant Director-in-Charge Janice K. Fedarcyk said: "From New York to Norway and Japan to Australia, Operation Card Shop targeted sophisticated, highly organized cyber criminals involved in buying and selling stolen identities, exploited credit cards, counterfeit documents, and sophisticated hacking tools. Spanning four continents, the two-year undercover FBI investigation is the latest example of our commitment to rooting out rampant criminal behavior on the Internet.

Cyber crooks trade contraband and advance their schemes online with impunity, and they will only be stopped by law enforcement's continued vigilance and cooperation. Today's arrests cause significant disruption to the underground economy and are a stark reminder that masked IP addresses and private forums are no sanctuary for criminals and are not beyond the reach of the FBI."

The following allegations are based on the Complaints unsealed today in Manhattan federal court:

Background on "Carding" Crimes

"Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals – including

the account information associated with credit cards, bank cards, debit cards, or other access devices – and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: buy goods or services online; manufacture counterfeit credit cards by encoding them with the stolen account information; manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, and wire fraud.

"Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: exchange information related to carding, such as information concerning hacking methods or computersecurity vulnerabilities that could be used to obtain personal identification information; and to buy and sell goods and services related to carding, for example, stolen credit or debit card account numbers, hardware for creating counterfeit credit or debit cards, or goods bought with compromised credit card or debit card accounts. Carding forums often permit users to post public messages - postings that can be viewed by all users of the site - sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for him or her, or if he or she pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

Individuals who use stolen credit card information to purchase goods on the Internet are typically reluctant to ship the goods to their own home addresses, for fear that law enforcement could easily trace the purchases. Accordingly, carders often seek out "drop addresses" — addresses with which they have no association, such as vacant houses or apartments, where carded goods can be shipped and retrieved without leaving evidence of their involvement in the shipment. Some individuals used carding forums to sell "drop services" to other forum members, usually in exchange for some form of compensation. One frequently used form of compensation is a "1-to-1" arrangement in which the carder wishing to ship to the drop must ship two of whatever items he has carded — one for the provider of the drop to forward to the carder, and the other for the provider of the drop to keep as payment in kind for the carder's use of the drop. Another frequently used compensation arrangement is for the carder and the drop provider to agree to resell the carded items shipped to the drop and to split the proceeds between them.

Background on the Undercover Operation

In June 2010, the FBI established an undercover carding forum, called "Carder Profit" (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things. Since individuals engaged in these unlawful activities on one of many other carding websites on the Internet, the FBI established the UC Site in an effort to identify these cybercriminals, investigate their crimes, and prevent harm to innocent victims. The UC Site was configured to

allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol ("IP") addresses of users' computers when they accessed the site. The IP address is the unique number that identifies a computer on the Internet and allows information to be routed properly between computers.

Access to the UC Site, which was taken offline in May 2012, was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times, new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. The e-mail addresses entered by registered members of the site were collected by the FBI.

Harm Prevented By the Undercover Operation

In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. In so doing, the FBI has prevented estimated potential economic losses of more than \$205 million, notified credit card providers of over 411,000 compromised credit and debit cards, and notified 47 companies, government entities, and educational institutions of the breach of their networks.

The Charged Conduct

As alleged in the Complaints unsealed today in the Southern District of New York, the defendants are charged with engaging in a variety of online carding offenses, in which they sought to profit through, among other means, the sale of hacked victim account information, personal identification information, hacking tools, "drop" services and other services that could facilitate carding activity.

MICHAEL HOGUE, a/k/a "xVisceral," offered malware for sale, including remote access tools ("RATS") that allowed the user to take over and remotely control the operations of an infected victim-computer. HOGUE's RAT, for example, enabled the user to turn on the web camera on victims' computers and spy on them, and to record every keystroke of the victim-computer's user. If the victim visited a banking website and entered his or her user name and password, the key logging program could record that information, which could then be used to access the victim's bank account. HOGUE sold his RAT widely over the Internet, usually for \$50 per copy and boasted that he had personally infected "50-100" computers with his RAT, and that he'd sold it to others who had infected "thousands" of computers with malware. HOGUE's RAT infected computers in the United States, Canada, Germany, Denmark, and Poland, and possibly other countries.

JARAND MOEN ROMTVEIT, a/k/a "zer0," used hacking tools to steal information from the internal databases of a bank, a hotel, and various online retailers, and then sold the information to others. In February 2012, in return for a laptop computer, ROMTVEIT sold credit card information to an individual he believed to be a fellow carder, but who in fact was an undercover FBI agent.

MIR ISLAM, a/k/a "JoshTheGod," trafficked in stolen credit card information and possessed information for more than 50,000 credit cards. ISLAM also held himself out as a member of "UGNazi," a hacking group that has claimed credit for numerous recent online hacks, and as a founder of "Carders.Org," a carding forum on the Internet. Last night, ISLAM met in Manhattan with an individual he believed to be a fellow carder - but who in fact was an undercover FBI agent - to accept delivery of what ISLAM believed were counterfeit credit cards encoded with stolen credit card information. ISLAM was placed under arrest after he attempted to withdraw illicit proceeds from an ATM using one of the cards. Today, the FBI seized the web server for UGNazi.com, and seized the domain name of "Carders.org" – taking both sites offline.

STEVEN HANSEN, a/k/a "theboner1," and ALEX HATALA, a/k/a, "kool+kake," sold stolen "CVVs," a term used by carders to refer to credit card data that includes the name, address, and zip code of the card holder, along with the card number, expiration date, and security code printed on the card. HATALA advertised to fellow carders that he got "fresh" CVV's on a "daily" basis from hacking into "DBs [databases] around the world."

ALI HASSAN, a/k/a "Badoo," also sold "fulls," a term used by carders to refer to full credit card data including cardholder name, address, social security number, birth date, mother's maiden name, and bank account information. HASSAN claimed to have obtained at least some of them by having hacked into an online hotel booking site.

JOSHUA HICKS, a/k/a "OxideDox," and LEE JASON JEUSHENG, a/k/a "iAlert, a/k/a "Jason Kato," each sold "dumps," which is a term used by carders to refer to stolen credit card data in a form in which the data is stored on the magnetic strips on the backs of credit cards. HICKS sold 15 credit card dumps, in return for a camera and \$250 in cash to a fellow carder who, unbeknownst to HICKS, was in fact an undercover FBI agent. HICKS met the undercover agent in downtown Manhattan to consummate the sale. Similarly, JEUSHENG sold 119 credit card dumps, in return for three iPad 2's to a carder who in fact was an undercover FBI agent. JEUSHENG provided his shipping address in Japan to the undercover agent, which in part led to his identification and arrest.

MARK CAPARELLI, a/k/a "Cubby," engaged in a so-called "Apple call-in" scheme, in which he used stolen credit cards and social engineering skills to fraudulently obtain replacement products from Apple, Inc., which he then resold for profit. The scheme involved CAPARELLI obtaining serial numbers of Apple products he had not in fact bought. He would then call Apple with the serial number, claim the product was defective, arrange for a replacement product to be sent to an address he designated, and give Apple a stolen credit card number to charge if he failed to return the purportedly defective product. CAPARELLI sold and shipped four iPhone 4 cellphones that he had stolen through the Apple call-in scheme to an individual whom he believed to be a fellow-carder, but who in fact was an undercover FBI agent.

SETH HARPER, a/k/a "Kabraxis314," and PETER KETCHUM, a/k/a "iwearaMAGNUM," each sold "drop" services to other carders in return for money or carded merchandise. HARPER provided drop addresses in Albuquerque, New Mexico, to which coconspirators sent expensive electronics, jewelry, and clothing, among other things. KETCHUM advertised drop locations "spread across multiple cities" in the United States and allegedly received and shipped carded merchandise including sunglasses and air purifiers, as well as synthetic marijuana.

CHRISTIAN CANGEOPOL, a/k/a "404myth," engaged in illegal "instoring" at Walmart to obtain Apple electronic devices with stolen credit cards. "Instoring" is a term used by carders to refer to using stolen credit card accounts to make in-store, as opposed to online, purchases of

items, using stolen credit card information and matching fake identifications. As part of the alleged scheme, CANGEOPOL and a co-conspirator used stolen credit card data to order electronic devices on Walmart's website; in selecting a delivery option, they opted to have items delivered to various Walmart stores in Georgia; CANGEOPOL then picked up the items using a fake identification; CANGEOPOL and the co-conspirator then resold the carded electronics and split the proceeds.

* * *

The attached chart reflects the name, age, residence, and pending charges against each individual charged in the Southern District of New York.

Mr. Bharara praised the outstanding investigative work of the FBI and its New York Cyber Crime Task Force, which is a federal, state and local law enforcement task force combating cybercrime. Mr. Bharara also commended the U.S. Attorney's offices in the following districts: New Mexico, Arizona, Delaware, Massachusetts, California (Central and Southern districts), Florida (Middle district), Georgia (Northern), as well as the Manhattan District Attorney's Office. He also thanked the following domestic law enforcement partners for their assistance: the New York City Police Department; the Essex, Vermont Police Department; the Eaton, Ohio Police Department; the Butler County, Ohio Sheriff's Office; the Cedar Bluff, Alabama Police Department; the Modesto, California Police Department; the Louisiana State Police; the Suffolk County, New York Police Department; the Bakersfield, California Police Department; the Kern County, California District Attorney's Office; the Long Beach, California Police Department; the Louisville, Kentucky Metro Police Department; and the Nelson County, Kentucky Sheriff's Office.

Mr. Bharara acknowledged and thanked the following international law enforcement agencies: the United Kingdom's Serious Organised Crime Agency, Royal Military Police, Thames Valley Police, Greater Manchester Police, Leicestershire Police, Hertfordshire Police, and Wiltshire Police; the Australian Federal Police; Bosnia's Republika Srpska Ministry of Interior; the Bulgarian Ministry of Interior, General Directorate for Combating Organized Crime; the Danish National Police; the Royal Canadian Mounted Police; the French National High-Tech Crime Unit (OCLCTIC) of the Central Directorate of the Police Judiciaire; the German Bundeskriminalamt (BKA); the Italian Polizia di Stato, Compartimento Polizia Postale e delle Comunicazioni; the National Police Agency of Japan, Tokyo Metropolitan Police Department (Cyber Crimes Control Division), Ministry of Justice of Japan, Tokyo High Prosecutors Office, and the Ministry of Foreign Affairs of Japan; the Macedonian Ministry of Interior, Department Against Organized Crime; and the Norwegian National Police for their efforts. He also thanked the Computer Crime & Intellectual Property Section of the Department of Justice, as well as the Office of International Affairs at the Department of Justice.

This case is being handled by the Office's Complex Frauds Unit. AUSAs James Pastore, Serrin Turner, Timothy Howard, Rosemary Nidiry, Alexander Wilson, and Sarah McCallum, are in charge of the prosecution.

The relevant charging documents can be found on the SDNY website at: http://www.justice.gov/usao/nys/pressreleases/index.html

12-190 ###

List of Arrested Defendants Charged in SDNY Complaints

DEFENDANT	SDNY COMPLAINT #	Residence	Age	CHARGES & MAXIMUM PENALTIES
CHRISTIAN CANGEOPOL, a/k/a "404myth"	12 Mag. 1667	Lawrenceville, Georgia	19	Conspiracy to commit access device fraud (7.5 years in prison)
MARK CAPARELLI, a/k/a "Cubby"	12 Mag. 1640	San Diego, California	20	 Wire fraud (20 years in prison) Access device fraud (10 years in prison)
STEVEN HANSEN, a/k/a "theboner1"	12 Mag. 1641	Kentucky (in prison in Wisconsin)	23	Fraud in connection with identification information (Five years in prison)
SEAN HARPER, a/k/a "Kabraxis314"	12 Mag. 1638	Albuquerque, New Mexico	23	Conspiracy to commit access device fraud (7.5 years in prison)
ALI HASSAN, a/k/a "Mr Badoo," a/k/a "Mr.Badoo," a/k/a "Badoo"	12 Mag. 1565	Milan, Italy	22	 Conspiracy to commit wire fraud (20 years in prison) Conspiracy to commit access device fraud, with object of possession 15 or more access devices (Five years in prison) Aggravated identity theft (Two years mandatory consecutive in prison)
ALEX HATALA, a/k/a "kool+kake"	12 Mag. 1669	Jacksonville, Florida	19	Fraud in connection with identification information (Five years in prison)
JOSHUA HICKS, a/k/a "OxideDox"	12 Mag. 1639	Bronx, New York	19	> Access device fraud (10 years in prison)
MICHAEL HOGUE, a/k/a "xVisceral"	12 Mag. 1632	Tucson, Arizona	21	 Conspiracy to commit computer hacking (10 years in prison) Distribution of malware (10 years in prison)
LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato"	12 Mag. 1605	Tokyo, Japan	23	Access device fraud (10 years in prison)
PETER KETCHUM, JR., a/k/a "iwearaMAGNUM"	12 Mag. 1651	Pittsfield, Massachusetts	21	Conspiracy to commit access device fraud (7.5 years in prison)

JARAND MOEN ROMTVEIT, a/k/a "zer0," a/k/a "zer0iq"	12 Mag. 1656	Porsgrunn, Norway	25	A A A	Access device fraud (possession 15 unauthorized devices) (10 years in prison) Access device fraud (affecting transactions with unauthorized devices) (15 years in prison) Aggravated identity theft (Two years mandatory,
MIR ISLAM, a/k/a "JoshTheGod"		Bronx, New York	18	\ \ \ \	consecutive in prison) Access device fraud (10 years in prison) Access device fraud (affecting transactions with unauthorized devices) (15 years in prison)