FEDERAL BUREAU OF INVESTIGATION

Cyber Division
Cyber Criminal Section
Financial Threat Focus Cell

SSA Jason L. Nestelroad

July 27, 2010

FEDERAL BUREAU OF INVESTIGATION

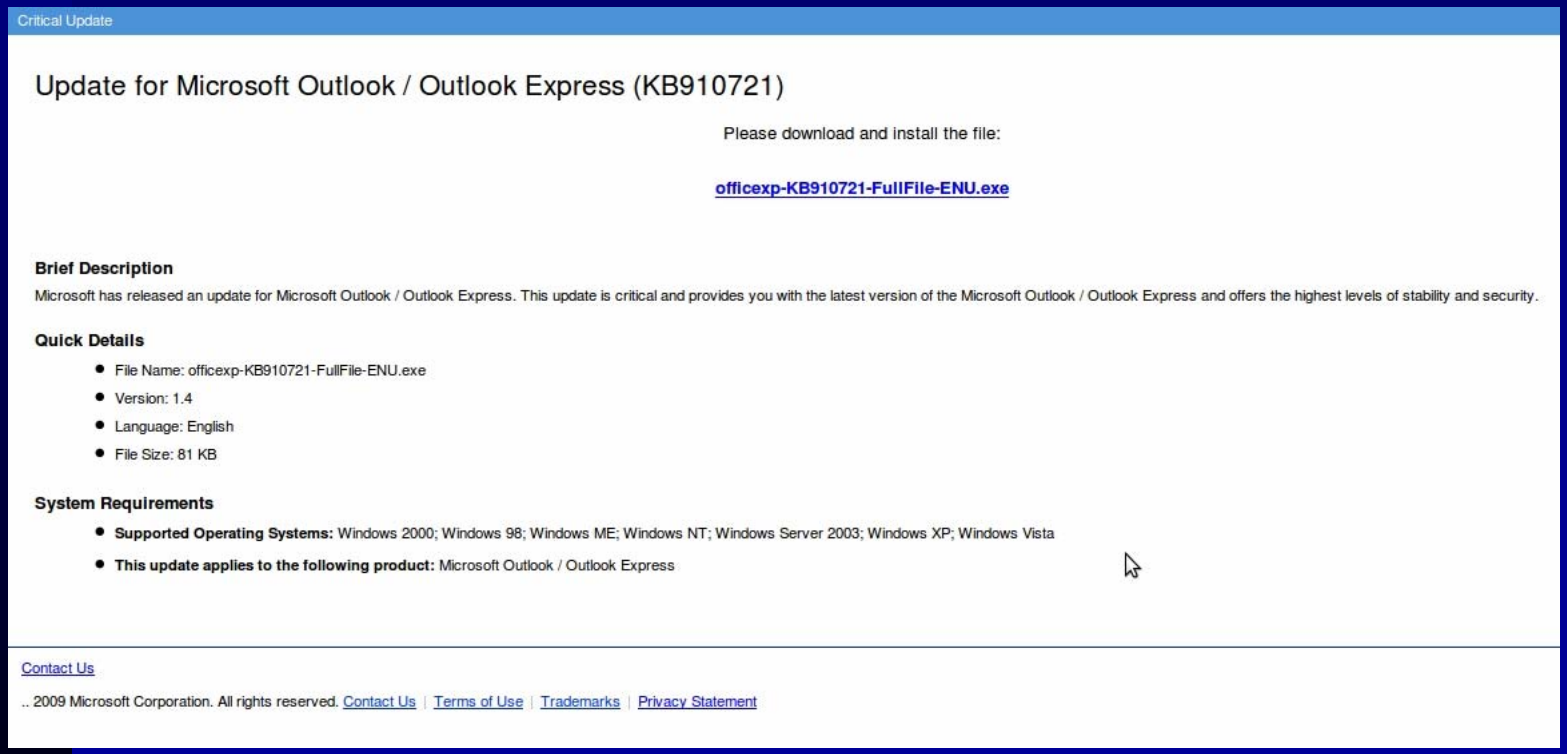
ACH Online Banking Scheme Overview

- Small to medium sized businesses are being targeted
  - CFO / Accountants receive phishing e-mails
- Malware installed
  - Keyloggers
  - Users credentials obtained
- ACH credits sent to US money mules
  - Forwarded on to Russia and Eastern Europe

FEDERAL BUREAU OF INVESTIGATION

Examples of Phishing Emails

- Microsoft Critical Update, Bank of America, Chase, Facebook



Critical Update

Update for Microsoft Outlook / Outlook Express (KB910721)

Please download and install the file:

officexp-KB910721-FullFile-ENU.exe

Brief Description

Microsoft has released an update for Microsoft Outlook / Outlook Express. This update is critical and provides you with the latest version of the Microsoft Outlook / Outlook Express and offers the highest levels of stability and security.

Quick Details

- File Name: officexp-KB910721-FullFile-ENU.exe
- Version: 1.4
- Language: English
- File Size: 81 KB

System Requirements

- **Supported Operating Systems:** Windows 2000; Windows 98; Windows ME; Windows NT; Windows Server 2003; Windows XP; Windows Vista
- **This update applies to the following product:** Microsoft Outlook / Outlook Express

Contact Us

.. 2009 Microsoft Corporation. All rights reserved. Contact Us | Terms of Use | Trademarks | Privacy Statement


VICTIMS
Banks/Financial Institutions
Subjects
CORPORATE ACCOUNTS
Vishing
Smishing
Phishing
Stock Fraud
Secure ID Keyloggers
ACH Payments
Money Mules
WESTERN UNION
MoneyGram International
SARs via FinCEN
Ukraine
Russia
United States

FEDERAL BUREAU OF INVESTIGATION

Money Mule Recruitment

- CareerBuilder.com/ Monster.com
- Work from Home Scams sent via phishing emails
- Exchange students / Visas
- Professional Front Companies
  - Web Sites / Logins
  - In person meetings
  - Bonuses for quick response

FEDERAL BUREAU OF INVESTIGATION

Front Companies – How they look legit

- Legitimate looking websites
- Websites with employee logins
- Meeting employees in person
- Providing bonuses/incentives for quick transactions

HOME | ABOUT US | SERVICES | PRODUCTS | CAREERS | PARTNERS | CONTACTS

17.09.2008
New warehouse.
We are proud to announce that today we are opening our new warehouse in Riga, Latvia. All of our facilities are supported by a cost-efficient transportation system that fully integrates warehousing and transportation functions.

11.05.2008
New service announced.
We would like to introduce to you our new service - Residential Delivery. Air Parcel Express provides extraordinary customer service and use state-of-the-art technology online, plus we use the newest moving trucks in our fleet to provide you with the most efficient and cost-effective home delivery solution in the industry.

24.12.2007
2007's results.
At the end of 2007 we have offices and representatives in North America (Canada, US) and Europe (UK, France). Our total turnover reached $2m this year and is expected to rise to $4m next year.

Air Parcel Express is pleased to offer you choices in business service that are in a high demand in the world shipping market. The services we offer meet a wide range of requirements, cost and quality. We continually increase the spectrum of our proposals to guarantee you complete satisfaction from our mutual agreement.

International Business Services
With mail forwarding from Air Parcel Express, you can instantly reach the largest consumer market in the world. Want to create the illusion of a business presence in the country? We make it possible with United States mailing address. Don't want your valued customers to incur the cost of shipping to your international headquarters? Use your Air Parcel Express address as an intermediary. Want us to distribute your product to clients with a US postmark? We can do that, too. Air Parcel Express will work together with you to become a valued member of your supply chain. Contact us with your needs so we can help craft a business solution for your firm today.

Domestic Business Services
In today's global economy, it is necessary for your employees to travel the globe. If you have the employees that are frequently traveling, you owe them a convenience of Air Parcel Express account. Contact us today so we can help you to craft a solution to fit your company.

Individuals Living Abroad
Whether you are an expatriate, travel for business, or are frequently abroad for pleasure, Air Parcel Express will make sure your mail gets to you in a cost effective and timely manner. We know it is a hassle to receive important packages and bills while you are away from home; with that in mind, we offer automatic forwarding options that take the worry out of leaving home for an extended period.

FEDERAL BUREAU OF INVESTIGATION

Current Stats and Trends

- Approximately $150 million in attempted loss – over $58 million actual

- Approximately 5500 money mules identified

FEDERAL BUREAU OF INVESTIGATION

Threat Focus Cell Activities

- Targeting subjects overseas as well as major money mules and front companies here in the U.S. –follow the money and the malware / case coordination

- Collaboration with finance sector to inform financial institutions and third party vendors

- Collaboration with business sector and Infragard to inform small and medium sized businesses about the threat

FEDERAL BUREAU OF INVESTIGATION

Threat Focus Cell Activities

- Addressing the Threat

1. Criminal actors
2. Infrastructure
3. Cash out organization
4. Money mules

HIGH-TECH HEIST
2,100 ATMs Worldwide Hit at Once

11/16/09

It was a highly sophisticated and cleverly orchestrated crime plot. And one unlike any we've ever seen before.

It culminated a year ago this month—on November 8, 2008—when a wave of thieves fanned out across the globe nearly simultaneously. With cloned or stolen debit cards in hand—and the PINs to go with them—they hit more than 2,100 money machines in at least 280 cities on three continents, in such countries as the U.S., Canada, Italy, Hong Kong, Japan, Estonia, Russia, and the Ukraine.

When it was all over—incredibly within 12 hours—the thieves walked off with a total of more than $9 million in cash. And that figure would've been more, had the targeted ATMs not been drained of all their money.

This individual, one the suspected "cashers" at an ATM in the Atlanta area, is still at large. Contact our office in Atlanta at (404) 679-9000 if you have any information on him or the case. Details

The alleged masterminds of this slick scheme—prosecutors charged earlier this month following an extensive FBI investigation assisted by other federal agencies and our partners around the globe—were three 20-something Eastern Europeans and an unnamed person called simply "Hacker 3."

Working together, the four hackers cooked up "perhaps the most sophisticated and organized computer fraud attack ever conducted," according to Acting U.S. Attorney Sally Quillian Yates of the Northern District of Georgia.

- It started when a 28-year-old Moldovan man learned of a vulnerability in the computer network of major credit card processing company based in Atlanta. With an eye toward exploiting it, he passed that information to a hacker living in Estonia.
- The Estonian conducted "reconnaissance" on the network vulnerability and shared what he learned with a hacker in Russia.
- With the help of the three other hackers at varying times, the Russian busted into the electronic network, reverse-engineered the PIN codes from the encrypted system, and raised the limits on the amount of money that could be withdrawn from the prepaid payroll debit cards. (These cards, used by many companies, enable employees to withdrawal their salaries from an ATM.)
- In addition to providing computer support, Hacker 3 managed the network of thieves around the world—called "cashers"—who used a total of 44 counterfeit cards to withdrawal the $9 million. The Estonian also managed his own cashing group.
- As the cashers went to work, the Russian took the lead in monitoring the victim company's database to track the illegal withdrawals. With the Estonian, he later deleted or tried to delete files on the computer network to cover their tracks.
- When the ATM thefts were complete, Hacker 3—with the help of the Estonian—gathered and divvied up the proceeds. The cashers got to keep 30 to 50 percent of the money they stole; the rest went to the four hackers.

Fortunately, the company reported the breach immediately, and we quickly got to work. Our ensuing case was made with a great deal of international cooperation and even led to joint investigations overseas. Suspected cashers, for example, have also been identified and arrested in Estonia and Hong Kong.

The case is a testament to both the globalized nature of crime in today's world and the international reach of the FBI, which depends more and more on a network of 61 overseas offices worldwide to protect the U.S. from a range of national security and criminal threats.

Department of Justice Press Release

For Immediate Release
November 10, 2009

United States Attorney's Office
Northern District of Georgia
Contact: (478) 752-3511

International Effort Defeats Major Hacking Ring
Elaborate Scheme Stole over $9.4 Million from Credit Card Processor

ATLANTA, GA—VIKTOR PLESHCHUK, 28, of St. Petersburg, Russia; SERGEI TŠURIKOV, 25, of Tallinn, Estonia; and OLEG COVELIN, 28, of Chişinău, Moldova, along with an unidentified individual, have been indicted by a federal grand jury on charges of conspiracy to commit wire fraud, wire fraud, conspiracy to commit computer fraud, computer fraud, and aggravated identity theft. IGOR GRUDIJEV, 31, RONALD TSOI, 31, EVELIN TSOI, 20, and MIHHAIL JEVGENOV, 33, each of Tallinn, Estonia, have been indicted by a federal grand jury on charges of access device fraud.

Acting United States Attorney Sally Quillian Yates said of the case, "Last November, in just one day, an American credit card processor was hacked in perhaps the most sophisticated and organized computer fraud attack ever conducted. Today, almost exactly one year later, the leaders of this attack have been charged. This investigation has broken the back of one of the most sophisticated computer hacking rings in the world. This success would not have been possible without the efforts of the victim, and unprecedented cooperation from various law enforcement agencies worldwide."

In Washington, D.C., Assistant Attorney General of the Criminal Division Lanny A. Breuer said, "The charges brought against this highly sophisticated international hacking ring were possible only because of unprecedented international cooperation with our law enforcement partners, particularly between the United States and Estonia. Through our close cooperation, both nations have demonstrated our commitment to identifying sophisticated attacks on U.S. financial networks that are directed and operated from overseas and our commitment to bringing the perpetrators to justice."

FBI Atlanta Special Agent in Charge Greg Jones said, "Through the diligent efforts of the victim company and multiple law enforcement agencies within the United States and around the world, the leaders of a technically advanced computer hacking group were identified and indicted in Atlanta, sending a clear message to cyber-criminals across the globe. Justice will not stop at international borders but continue with the on-going cooperation between the FBI and other agencies such as the Estonian Central Criminal Police and the Netherlands Police Agency."

FEDERAL BUREAU OF INVESTIGATION

Who are these subjects/hackers?

- Average age is anywhere between 16 and 30
- Predominately white males of Eastern European descent
- Well educated, organized and intelligent
- Just how sophisticated are they?

FEDERAL BUREAU OF INVESTIGATION

Mitigation

- Know your customer
- Reporting incidents to law enforcement
- Separate PC for online banking transactions
- Dual authentication – call back or two party verification, true out-of-band

EMERGING TRENDS

- Telecommunications Matters related to Financial Industry
  - Telephonic Denial of Service (TDOS)
  - Revenue Sharing related to Call Centers
  - Mobile Phone - Vulnerabilities
  - Remote Mobile Payment Services – M-Pesa

- Check Clearing for the 21st Century Act (Check 21)
  - Digital Check Images allow for remote deposit

Telecommunications – TDOS & Revenue Sharing

- Sustained calls to a customer's home or cellular telephone
  - Thwart FI/Brokerage Firm attempts for "Out of Band Authentication"
  - Subjects take over phone abandend cell phone number and port it out to VoIP
- Revenue Sharing
  - Automated calls
    - White Noise
    - Dual-tone multi-frequency signaling (DTMF) – Menu System

Telecommunications – Mobile Phones

Smart Phone Vulnerabilities:

- Physical access
- Browse internet
- Receive SMS text
- **Applications**

Over-all Goals of Research:

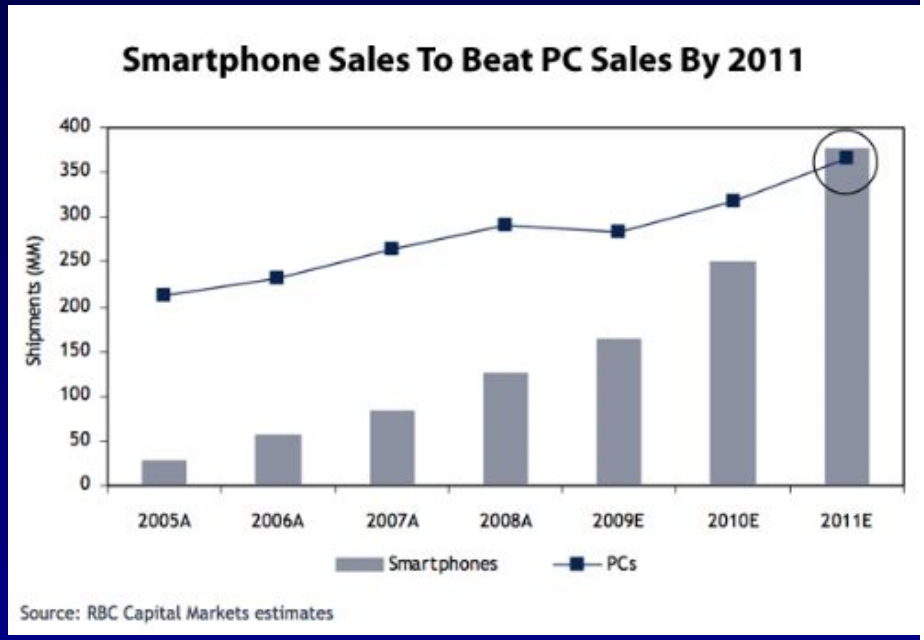
1. How smart phone applications are being exploited
2. What sensitive information is targeted
3. Anticipate future threats or trends
4. Determine how financial partners, retail partners, telcos, and consumers may reduce risk

Courtesy: NCFTA Analyst Roxanne C. Ruminski

Why Research Smart Phones?

- Popularity increasing
- More applications are available
- Reliance upon smart phones increasing
- Operating systems becoming more complex, allowing more options for hacking

  (For example: Rootkits)



Top Five Converged Mobile Device Vendors, Shipments, and Market Share, Q4 2009 (Units in Millions)

Vendor	4Q09 Unit Shipments	4Q09 Market Share	4Q08 Unit Shipments	4Q08 Market Share	4Q09/4Q08 Growth
1. Nokia	20.8	38.2%	15.1	38.5%	37.7%
2. Research In Motion	10.7	19.6%	7.6	19.4%	40.8%
3. Apple	8.7	16.0%	4.4	11.2%	97.7%
4. Motorola	2.5	4.6%	1.6	4.1%	56.3%
5. HTC	2.4	4.4%	2.2	5.6%	9.1%
Others	9.4	17.2%	8.3	21.2%	13.3%
Total	**54.5**	**100.0%**	**39.2**	**100.0%**	**39.0%**

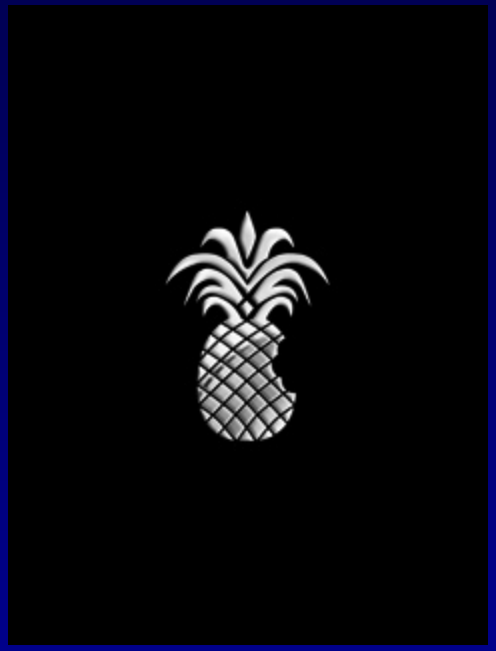
Sources:
Above RBC Capital Markets and to left Linusfordevices.com

Understanding the Process

SMART PHONE	TELCO	DOWNLOAD APPLICATIONS	APPLICATIONS	HACKING METHODS	HACKING PURPOSE
 iPhone	at&t	iPhone App Store	Social Networking	▪Viruses pushed through internet server or SMS text	▪PII
 Droid	at&t verizon Sprint T-Mobile Additional teleco companies	DroidApps Or directly to website, (pay with credit card)	Finances	▪Spoofing femtocells	▪Personal and/or business contacts
 Blackberry		BlackBerry App World Or directly to website, pay on phone bill	The Weather Channel Information	▪Eavesdropping	▪Cookies
			NHL Hobbies	▪Malware based attacks	▪Username password
					▪Pin number
					▪Denial of service
					▪Push viruses

Specific Emerging Vulnerability

- Jailbroken iPhones allow users to download applications and/or illegal or pirated apps otherwise not available on iPhone App Store.
- Accepts any SIM without restriction



Booting screen of a jailbroken iPhone.

Hacking Competition: March 2010

Pwn2Own contest at the CanSecWest security conference March 24th, 2010:

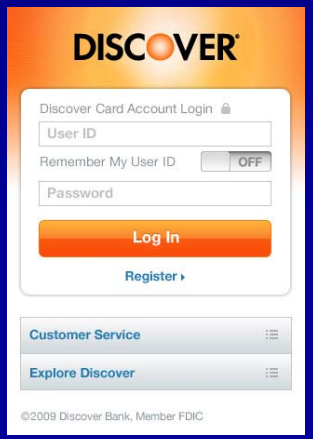
Technology Targets included vulnerabilities affecting the following mobile phones:

Apple iPhone 3 GS
RIM Blackberry Bold 9700
A Nokia device running Symbian S60 (likely the E62)
A Motorola phone running Android (likely the Droid)

Ralf Philipp Weinmann of the University of Luxembourg and Vincenzo Iozzo of German company Zynamics were able to grab key data in an iPhone. The researchers used a vulnerability in Safari that pulled the SMS database he explained. Data included deleted messages, contacts, pictures, and iTunes music files. The joint hackers shared a $15,000 prize, and each took ownership of an iPhone.

Alerting Financial Partners

If you ask us to "remember" your user ID, we will also create a permanent cookie for this purpose. In addition, DFS uses a temporary cookie file to maintain your session as you move from page to page on the Mobile Service. The cookie is deactivated when you conclude your session. Because this cookie is stored only in your mobile device's temporary memory, it is deleted when you turn off your mobile device. Most mobile devices allow you to modify your preferences to be notified when a cookie is set, or to reject all cookies. If you choose to reject our cookies, some areas of our Mobile Service may not function properly.



Safaricom | Products & Services

Home | Abou

M-PESA

Send money to your loved
Safe, fast, convenie
Register FREE at M-

About Us | Products & Servic

You are here → Home → Products&Services → M-PESA | Sear

- Safaricom
- Business Solutions
- What's New!
- Products&Services
  - Safaricom Terms & Conditions
  - PrePay
  - PostPay
  - Data and Messaging
  - M-PESA
    - M-PESA Resource Center
    - How to Register for M-Pesa
    - M-PESA Services
    - M-PESA Tariff
    - International Money Transfer (IMT)
    - M-PESA Agents

M-PESA

Send PESA By Phone. FAST, SAFE & AFFORDABLE

M-PESA is a Safaricom service allowing you to transfer money using a mobile phone. Kenya is the first country in the world to use this service, which is offered in partnership between Safaricom and Vodafone. M-PESA is available to all Safaricom subscribers (Prepay and Postpay), even if you do not have a bank account. Registration is FREE and available at any M-PESA Agent countrywide. The M-PESA application is installed on your SIM card and works on all makes of handsets.

Board of Governors of the Federal Reserve System

Frequently Asked Questions about Check 21

Print

The Check Clearing for the 21st Century Act (Check 21) was signed into law on October 28, 2003, and became effective on October 28, 2004. Check 21 is designed to foster innovation in the payments system and to enhance its efficiency by reducing some of the legal impediments to check truncation. The law facilitates check truncation by creating a new negotiable instrument called a substitute check, which permits banks to truncate original checks, to process check information electronically, and to deliver substitute checks to banks that want to continue receiving paper checks. A substitute check is the legal equivalent of the original check and includes all the information contained on the original check. The law does not require banks to accept checks in electronic form nor does it require banks to use the new authority granted by the Act to create substitute checks.

The Federal Reserve Board has released the final rule to implement Check 21, including the model disclosure language for depository institutions to use in notifying consumers of their rights under the law.

» *USAA Deposit@Mobile*

Deposit checks when you want, where you want, with this first-of-its-kind mobile application. No need to drive to the bank, wait in line or mail in your deposit. It's free, secure and as easy as snapping a picture. And your USAA bank account is credited instantly.**

USAA Deposit@Mobile for the iPhone® debuted in August, with more than 75,000 members depositing $234 million in 2009. It's also available for Android® users, and similar apps are in development for BlackBerry® and other smart phones. USAA Mobile remains one of the top-rated financial apps on iTunes and has been downloaded more than 373,000 times.

Find out more at **USAA.com**/mobile or download the app from the Apple App Store or Google's® Android Market.

WHAT YOU'LL NEED:

1. Eligibility for USAA property and casualty insurance
2. A USAA checking or savings account
3. A USAA credit card or loan, or be qualified for one
4. An iPhone or Android phone with the free USAA Mobile App

**Deposits may not be available for immediate withdrawal. Bank products provided by USAA Federal Savings Bank, Member FDIC.

HOW TO USE USAA DEPOSIT@MOBILE:

ENTER AMOUNT
After logging in and selecting your account, enter check amount.

CAPTURE FRONT AND BACK
Take pictures of the front and back of your endorsed check.

SUBMIT
Verify all information, then submit.

CONFIRMATION
Receive confirmation of deposit.

FEDERAL BUREAU OF INVESTIGATION

Cyber Division
Cyber Criminal Section
Financial Threat Focus Cell

SSA Jason L. Nestelroad

July 27, 2010