

# ASIS Councils NEWSLETTER

## Banking and Financial Services Council

Mr. Larry E. Brown – Chairman  
First Citizens Bank & Trust

Mr. Terry Huskey, CPP – Vice Chair  
Wachovia Corporation

Mr. Kevin O'Brien  
The Bank of New York

Mr. Brian R. Abraham, CPP  
3SI Security Systems

Mr. Robert S. Ballagh Jr, CPP  
CheckFree

Mr. Steven K. Braden  
Capital One Financial Corp

Mr. Michael J. Collins  
Provident Bank

Mr. Robert D. Croskery  
Wells Fargo & Company

Mr. Clark B. Cummings, CPP  
FirstBank

Mr. Randy Dicampii  
Wilmington Trust Company

Mr. Johan D. Du Plooy, CPP  
Risk Diversion Pty Ltd

Mr. R. P. Handren, CPP  
RBC Protection Services

Mr. Alexander Hilton  
Canadian Imperial Bank

Mr. Douglas W. Kohlsdorf, CPP

Mr. W. Joseph Majka  
Visa USA

Mr. Richard L. Seba, CPP  
JP Morgan Chase

Mr. Chris Smith  
HBSC

Mr. P. Kevin Smith, CPP  
Chevy Chase Bank

Mr. Francis X. Tesorero Jr, CPP  
GE Consumer Finance

Dr. Hector R. Torres, PhD, CPP  
Banco Popular de Puerto Rico

Mr. James W. Zardecki  
Sovereign Bank

## Banking and Financial Services Council

July – September 2009

### ASIS International Quick Notes



#### **New PCI Review Released**

The new PCI review is now available [online](#) and on [CD](#). Prepare for your PCI exam at your own pace.

#### **Certification Spotlight**

ASIS proudly congratulates the thousands of professionals who have sought and attained board certification.

#### **Web Sites Launched for Military and Law Enforcement Practitioners**

Learn about the special benefits of ASIS certification, education, and membership for active duty, transitional, and reserve [military](#) and [law enforcement](#) security practitioners

### **ASIS Upcoming Events**



### SEMINARS

**October 26-27:** [Enhanced Violence Assessment and Management](#)

**October 26-29:** [CCTV](#)

**October 28-29:** [Active Shooter: Prevention, Intervention, and Response](#)

**November 16-19:** [Assets Protection Course I - Concepts and Methods](#)





**November 20:** [Return on Investment \(ROI\): How to Successfully Sell Security to Management](#)

**November 30-December 4:** [Wharton/ASIS Program for Security Executives](#)

**December 7-December 8:** [Executive Protection](#)

**December 7-December 9:** [TRANSPORTATION SECURITY: Is Your Cargo REALLY Secure?](#)

**December 7-December 9:** [Security Force Management](#)

## **WEBINARS**

**October 21:** [Social Network Sites: Can You Always Trust What You See?](#)

**November 4:** [Achieving Operational Interoperability through Emerging Standards](#)

**November 18:** [Web 2.0 Investigations That Move Beyond Google](#)

## **IN THE NEWS**

### **North Miami Beach resident arrested in foreign currency investment scheme, 08/12/09, US Department of Justice**

The acting United States attorney for the southern district of Florida and the acting special agent in charge, Federal Bureau of Investigation (FBI), Miami Field Office, announced on August 12 that a North Miami Beach resident was arrested earlier on August 12 on mail and wire fraud charges arising from an investment fraud scheme in which more than 100 investors lost approximately \$4,000,000. As alleged in the Indictment, from January 2002 through November 2004, the suspect defrauded investors by soliciting investments for the purported purpose of trading foreign currencies in the international foreign exchange market. The suspect caused investors to believe that, based on his alleged extensive experience trading foreign currencies; he would trade foreign currencies on the investors' behalf in return for a share of the profits generated by his trading activities.

### **Attorneys general form mortgage fraud task force, 08/24/09, Associated Press**

Ten state attorney generals and four federal agencies have announced the formation of a task force to combat mortgage fraud. According to a statement issued by the Washington state attorney general, targets of the enforcement effort include equity skimming, bogus foreclosure rescue, straw purchases and unethical lending practices. The group is headed by the Washington state attorney general and the Iowa attorney general. Other members include the attorneys general of Arizona, Colorado, Illinois, Nevada, North Carolina, Massachusetts, Missouri and Ohio, as well as representatives from the Department of Justice, federal treasury, Department of Housing and Urban Development and Federal Trade Commission.





## **NY businessman charged with \$74 million bank fraud against Citigroup, 08/25/09, Dow Jones Newswires**

A New York man was charged with allegedly defrauding Citigroup Inc. out of \$74 million in loans. The U.S. attorney in Manhattan and the Federal Bureau of Investigations say the defendant, with residences in Manhattan and Katonah, New York, fraudulently applied for the loans for Nemazee Capital Corp., of which he is chairman and chief executive. Federal prosecutors contend Nemazee obtained the money by giving the banking giant "numerous documents that purported to establish the existence of accounts in Nemazee's name at various financial institutions containing many hundreds of millions of dollars," the Justice Department said in a statement.

## **ABA Warns of Fraudulent Letters, Fake Checks, 08/27/09, ABA**

The ABA has been alerted that individuals sending cash-prize letters purporting to be from the association are part of a fake check scam. The con artists are sending letters asking people to call a phone number to find out how to collect a prize -- a popular technique to get personal financial information from letter recipients. Many of the letters contain one or more fraudulent checks, and a number of individuals have attempted to cash or deposit these fraudulent checks. The fraudulent checks are listed as from ABA and ABD Federal Credit Union, but the association believes other financial institutions may be targeted. The check amount is typically between \$1,000 and \$5,000. ABA is working with law enforcement to identify and disrupt the source of the letters.

## **Cleveland: Largest mortgage scam in U.S. history uncovered here, 08/27/09, WKYC 3 Cleveland, Ohio**

Just as Cleveland became the foreclosure capital of the country, prosecutors say a savvy man with an eye for real estate found a way to scam and profit. Uri Gofman, of Beachwood, was charged Tuesday for masterminding the largest mortgage scam in U.S. history. "Uri Gofman, the leader of this enterprise, orchestrated the nation's largest mortgage fraud case by enlisting family, friends and others to invest in his real estate company," said Cuyahoga County Prosecutor Bill Mason.

For over thirty minutes on Tuesday, representatives from the F.B.I., the Ohio Attorney General's Office and Cuyahoga County prosecutors explained in detail how Gofman capitalized on the crisis. Prosecutors allege he would enlist "straw buyers" to purchase foreclosed homes. A second set of buyers would then use false documents to acquire bank loans that allowed them to buy the home at twice the original purchase price. Gofman and his team would then pocket the difference, leaving the lenders holding the bag. In all, 453 homes were purchased with \$44 million in fraudulent loans.

## **Man accused of running Ponzi scheme in Brooklyn, 09/09/09, New York Times**

A Brooklyn money manager was arrested on Tuesday and charged with swindling hundreds of investors, including many retirees, out of \$40 million in what prosecutors called a "classic Ponzi scheme" dating to the 1970s. The money manager ran a group of small companies, known collectively as the Leverage Group, out of a small storefront office in Bay Ridge, where he grew up and where he still lives, and earned the trust of investors through his local ties and unassuming nature, his clients told investigators. He eventually collected the \$40 million from 800 investors by promising consistent returns of 12 percent or higher from stock options, according to the criminal complaint.





## **Investigations of mortgage fraud soar 63%, FBI reports, 09/17/09, New York Daily News**

Mortgage fraud cases under investigation by the FBI have jumped by about 63 percent in the past year, according to the bureau director. "The schemes have evolved with the changing economy, targeting vulnerable individuals, victimizing them even as they are about to lose their homes," he told the Senate Judiciary Committee on September 16. The FBI has more than 2,600 cases open, with most of them involving losses of more than \$1 million, the director said. The bureau has declined to identify any companies under criminal probes.

## **CYBER SECURITY NEWS**

### **Forget e-mail — 'phishers' now using cell text messages, 08/11/09, KOMO 4, Seattle**

Texting is quickly becoming the method of choice for scammers looking to scare victims into giving out their passwords, account numbers and other personal information. The old scam has already conned millions of consumers out of their personal information. Consumer fraud trackers rank phishing as the 4th most common form of fraud on the Internet, after lottery scams, Internet auctions, and Nigerian money scams. Diverting the focus to cell phones increases the chance of finding new victims who will take the bait.

### **Text messaging scam hits cell phones during weekend, 08/10/09, WEAU 13 Eau Claire**

Police are warning people about a text messaging scam that hit cell phones recently. La Crosse Police say cell phone customers got a message that shows their credit card was deactivated. Officers say it also directs them to call a phone number to reactivate their credit card. Police say it appears to be a phishing scam, aimed at getting personal and banking information.

### **Citi, Bank of America say Massachusetts customers hit by potential data-security breaches, 08/10/09, Boston Business Journal**

Two of the largest U.S. banks, Bank of America Corp. and Citigroup Inc., recently issued new credit and debit cards to customers after running into data safety concerns. Bank of America and Citigroup each recently issued replacement cards to consumers, telling them in letters that their account numbers may have been compromised.

### **Cybercrooks increasingly target small business accounts, 08/25/09, Computerworld**

An organization representing more than 15,000 financial institutions has issued a warning about a growing wave of attacks against small banks and businesses by cyber criminals using stolen banking credentials to plunder corporate accounts. In an alert to its members earlier this month, NACHA — the Electronic Payments Association — said that attackers are increasingly stealing online banking credentials, such as user names and passwords, from small businesses by using keystroke logging tools and other malware. The cybercriminals are using the stolen credentials to "raid" and "take over" corporate accounts and initiate the unauthorized transfer of funds over electronic payment networks.





## **European cyber-gangs target small U.S. firms, group says, 08/25/09, Washington Post**

Organized cyber-gangs in Eastern Europe are increasingly preying on small and mid-size companies in the United States, setting off a multimillion-dollar online crime wave that has begun to worry the nation's largest financial institutions. A task force representing the financial industry sent out an alert on August 21 outlining the problem and urging its members to implement many of the precautions now used to detect consumer bank and credit card fraud. The alert was sent to members of the Financial Services Information Sharing and Analysis Center, an industry group created to share data about critical threats to the financial sector. The group is operated and funded by such financial heavyweights as American Express, Bank of America, Citigroup, Fannie Mae and Morgan Stanley.

## **FDIC Issues Alert on EFT Transactions, 08/27/09, FDIC**

The Federal Deposit Insurance Corporation (FDIC) alerted financial institutions providing Web-based payment origination services for business customers to increase reports of fraudulent EFT transactions resulting from compromised login credentials. Over the past year, the FDIC has detected an increase in the number of reports and the amount of losses resulting from unauthorized EFTs.

## **International hacker pleads guilty for massive hacks of U.S. retail networks, 09/11/09, Department of Justice**

An international computer hacker pleaded guilty today to multiple charges relating to hacking activity and credit card fraud, announced the Assistant Attorney General of the Criminal Division, the Acting U.S. Attorney for the District of Massachusetts, the U.S. Attorney for the Eastern District of New York and the Director of the U.S. Secret Service. More than 40 million credit and debit card numbers were stolen from major U.S. retailers as a result of the hacking activity. The 28-year-old suspect of Miami, pleaded guilty today to 19 counts of conspiracy, computer fraud, wire fraud, access device fraud and aggravated identity theft relating to hacks into numerous major U.S. retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble and Sports Authority. According to the indictments, the suspect and his co-conspirators concealed and laundered their fraud proceeds by using anonymous Internet-based currencies both within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

## **Spam, Malware Dominate Online User Comments, Websense Reports, 09/16/09, Network World**

An incredible 95 percent of all user-generated comments for blogs, chat rooms, and other online forums are spam or predatory, finds the latest Websense study on security attack trends. The Websense Security Labs "State of Internet Security Q1 -Q2 Study," which covers the first six months of 2009, also observes that the number of virus-laden Web sites for the period increased by more than 300 percent. Additionally, more than three in four compromised Web sites--77 percent--are said to be authentic sites that have been hacked. "The bad guys are finding new ways for disseminating malware," says Websense's Patrick Runald. "It's getting worse." Close to 50 percent of the 100 most popular sites, especially social-networking sites such as Facebook or YouTube enable user-generated input, which the report claims is an increasingly preferred way to spread malware and launch attacks. "On Facebook and other social-networking sites, there's an explicit sense of trust," Runald says. "That's why the bad guys are attempting to exploit it, with malware like Koobface, which could hijack your machine and send messages."



## New scam adds live chat to phishing attack, 09/16/09, CNET News

Online scammers have created a phishing site masquerading as a U.S.-based bank that launches a live chat window where victims are tricked into revealing more information, researchers at the RSA Fraud Action Research Team said on September 16. After a user accesses the phishing site, the chat window messages come through the browser and not via a typical instant messenger application, RSA said in a blog post. The chat window is displayed if the log-in credentials are typed in or if any other link on the page is clicked, said an online fraud expert at RSA. The scammer claims to be from the bank's fraud department and says that the bank is requiring members to validate their accounts, asking for additional information such as name, phone number, and e-mail address, according to screenshots.

