

ASIS Councils

NEWSLETTER

Banking and Financial Services Council

Banking and Financial Services Council

September 2007

August Council Meeting Notes

The August 2007 meeting for the ASIS Banking and Financial Services Council was held at 11:00 a.m. EST on August 1, 2007 via conference call. Attendees to this meeting were:

Mr. Kevin O'Brien
Mr. Terry Huskey
Mr. Larry Brown
Mr. Clark Cummings
Mr. Robert Ballagh
Mr. Kevin Smith
Mr. Steven Braden

Opening remarks for the meeting were initiated by Mr. Kevin O'Brien, Council Chair, who gave an update on the Council Pre-Seminar session and highlighted due date for the supporting tasks. Also highlighted was the CIWG update. Mr O'Brien was followed by Larry Brown, Council Vice Chair who discussed current Council membership issues.

During the meeting Open Discussion forum, Mr. Kevin Smith discussed the Early Warning System for potential hiring of new employees and Mr. Brown discussed clean desk policy as it relates to regulations.

Due to the preparations for the ASIS 2007 Annual Seminar, Kevin O'Brien, Council Chair, rescheduled the Council's September meeting to be held during the Council's pre-seminar activity.

Best Practices Corner

How ATM Alerts Helped Citizens Stop Fraud Ring **American Banker (07/30/07) Vol. 172, No. 145, P. 23 ; Wolfe, Daniel**

Citizens Financial Group credits software from ACI Worldwide for helping detect a data breach at a grocery chain, even when customers were not aware their card information was being stolen. In February, scammers were caught replacing card readers with skimmers at Stop and Shop Supermarket stores in Rhode Island, then began using the stolen card numbers in California. Although customers were not aware of the breach, Citizens' Proactive Risk Manager software raised alerts on dozens of ATMs. Citizens' assistant VP of card risk prevention Mark Macheska said that one weekend, the company received "ATM velocity alerts" that indicated fraudulent ATM withdrawals from strictly Rhode Island cards. Citizens notified corporate security, which then investigated the suspected areas for the breaches and located the skimmers at checkout counters. Derren Jones, director of product management for ACI's fraud and risk management unit, says its software is meant to help banks respond quicker to fraud, as investigators were able to track the transactions in real time and predict patterns in the scammers' tactics.

Mr. Kevin O'Brien – Chariman
The Bank of New York

Mr. Larry E. Brown – Vice Chair
First Citizens Bank & Trust

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 Dicampfi
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. Terry Huskey, CPP
Wachovia Corporation

Mr. Douglas W. Kohlsdorf, CPP

Mr. W. Joseph Majka
Visa USA

Mr. Richard L. Seba, CPP
JP Morgan Chase

Mr. Chris Smith
HBSC

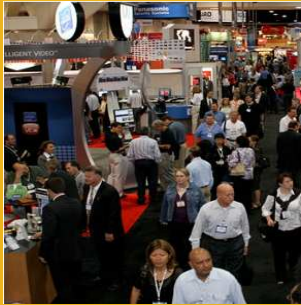
Mr. P. Kevin Smith, CPP
Chevy Chase Bank

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

The 2007 ASIS Seminar will be held at the Las Vegas Convention Center in Las Vegas, Nevada on September 24-27, 2007. This annual event is known for its high-quality educational program covering every aspect of security. The seminar consists of more than 150 dynamic sessions on the hottest issues and trends, as well as best practices and core security management topics that successful security professionals need to stay ahead. Each presentation is reviewed and selected by a committee of your peers to ensure that attendees learn from seasoned practitioners and subject matter experts with real-world experience and insights.



LOCATION

Las Vegas Convention Center
3150 Paradise Road
Las Vegas, NV 89101

Tel: (702) 892-0711
Fax: (702) 892-2824

EXHIBIT DATES/TIMES

September 24-26, 2007
9:00 am – 4:30 pm daily

NON-COMPETING EXHIBIT HOURS

9:00 am – 11:00 am daily
3:00 pm – 4:30 pm daily

Security Technology

Banks Test 'Text Messaging' Security

Investor's Business Daily (08/10/07) P. A4 ; Howell, Donna

Banks and brokerages have been on the hunt for just the right balance between convenience and cost to boost log-on and transaction security for customers. Tokens have been one solution to reinforcing banking security, as users type an up-to-the-minute passcode that is displayed on a token. Thieves' efforts are thus thwarted from logging on as a user, even if they know the user's name and password. Financial firms are also considering sending users a one-time pass code via text messages to their mobile phones, or by an automated phone call that would eliminate the use for tokens. Passcode generators can also be built into cell phone handsets. Since most consumers have cell phones, sending mobile notifications could be a viable authentication measure. A built-in credit card authentication option is also being considered by financial institutions. The card would display a one-time passcode once a pressure-sensitive area of the card is touched. VeriSign's Fran Rosch says this technology will undergo pilot tests and reach a sizeable distribution by next year.

Satellite Aids in Tracking Bank Robbers: Bad Guys Now Have to Worry About GPS Technology

New Haven Register (08/05/07) ; Kaempffer, William

Global Positioning System (GPS) technology is being utilized in New Haven, Conn., to follow bank thieves, most likely the first time it has been used for that reason. "The banks will tend to use it in higher-risk locations because it's not the cheapest," explains Connecticut Bankers Association senior vice president Lindsey R. Pinkham. "That, to some degree, has limited its deployment." Industry sources claim one product being worked on is a computerized fiscal recognition system in a current database. While GPS technology functions in a similar fashion to traditional dye packs, which are placed alongside money and go off after the thief exits the bank, the GPS tracker silently transmits signals that permit police to precisely uncover the suspect's whereabouts on a computer screen. Throughout the country, GPS technology has been more and more used by police to solve a broad variety of crimes. A female bank robber was recently apprehended in New Haven after exiting the branch with money and a concealed transmitter. Police were able to find and arrest her in minutes by using GPS to locate her.

New Bank Practices Make Hacking Easier

Dark Reading (08/08/07) ; Wilson, Tim

New techniques employed by banks to confirm users' identities are actually putting users at risk, according to research presented by security expert Brendan O'Connor at DefCon. In response to federal banking regulations, the majority of banks now require customers to answer a question or recognize a customized image before gaining access to their accounts. However, such questions force the user to reveal additional personal data, which criminals can then use to better their odds of hacking into an account. And while banks think that including a second image or question will stymie hackers, the "second" authentication factor actually clarifies the penetration path, thereby enhancing the hackers' ability to break in.

In The News

Bank Employee, Boyfriend Stage Armed Robbery, Police Say

Delaware News Journal (08/21/07)

A 23-year-old employee of a bank outside Lewes, Del., has been arrested for allegedly helping her boyfriend carry out a robbery of the bank. The employee, identified as Crystal Johnson, had told police that she was using the ATM at the Community Bank on Monday night when a masked man forced her at gunpoint to open the bank's vault. The robber, who turned out to be Johnson's boyfriend, fled on foot with an unspecified amount of money. Police did not buy Johnson's story and believe she is complicit in the robbery.

Thieves Turn Simple Strip Into Cutting-Edge Tool

USA Today (08/01/07) P. 8B ; Acohido, Byron; Swartz, Jon

Thieves have discovered a way to alter the magnetic stripe on the back of bank cards using a "magstripe reader-writer." A 26 year-old man was arrested in Canada in possession of thumb drives and computer printouts of credit card account data stolen from hundreds of U.S. and Canadian consumers. He also had prepaid gift cards from Visa and MasterCard. By altering the magstripes of authentic bank gift cards, the suspect was able to bypass a riskier task of fabricating fake credit cards. The ploy mimics a Miami ring that used counterfeited credit cards to buy stacks of Wal-Mart gift cards. Ring members then used the gift cards to amass \$1 million worth of big-ticket items from Sam's club, a Wal-Mart subsidiary. Like merchant gift cards, bank cards do not have embossed numerals or an individual's name on the card so no proof of identity is required to use them. Altering the magstripe on bank gift cards "is a way to convert small-value cards into big-value plastic," says information risk strategist John Pironti of Getronics. Visa, MasterCard, and American Express are rolling out contactless payment cards that use technology significantly more difficult to compromise.

Robberies at CUs Rose Much More Than Robberies at Banks Last Year, FBI Says

Credit Union Times (07/30/07) ; Morrison, David

The number of robberies at credit unions last year spiked sharply, easily outpacing a slight increase in bank robberies, according to statistics from the FBI. The stats show that the number of robberies at commercial banks increased just 2.24 percent from 2005 to 2006, compared with 23.4 percent for credit unions. During both 2005 and 2006, violent bank robberies accounted for 4.5 percent of all bank robberies, but that percentage has apparently increased during 2007, according to the FBI.

Modern Bank Robbers Are Low-Key

Associated Press (07/28/07) ; Mulvihill, Geoff

An examination of U.S. bank robberies from 2003 to 2006 finds that roughly three of every five bank robbers used notes passed to tellers to convey their threats. FBI statistics show that only one in 20 bank robberies are violent, and during the roughly 6,000 to 7,000 robberies that occur per year, about 20 people are killed, usually the robbers. Half of all bank robbers threaten to use a weapon when robbing a bank, but only 25 percent actually brandish a gun. Bank robberies tend to be more violent in Los Angeles, where organized bank robbery gangs that conduct "take-over" robberies account for 20 percent of the city's robberies. The vast majority of banks now have security measures in place, including security cameras, security alarms, exploding dye packs, and "bait bills." The FBI says that the modern bank robber is much more like New Jersey's "Mad Hatter" who robbed 18 banks and stole \$60,000 over a period of more than one year without a weapon.



Online Shoppers' Worries Over ID Theft Grow

DM News (07/26/07) ; Campanelli, Melissa

Data breaches at businesses, educational institutions, and medical facilities have resulted in changes in consumers' buying behavior, according to the results of two surveys released last week. The first study, the 2007 Consumer Survey on Data Security, found that 36 percent of consumers would not use their credit or debit cards to make a purchase on a Web site that they were not familiar with. The majority of the survey's respondents said that they were more cautious about entering their card information because of concerns about security. The second study, infoUSA's Opinion Research Corp.'s monthly "Ouch Point" series, found that the public's concern about personal financial matters should remain a primary consideration for financial institutions.

Lawsuits Target KFC Taco Bell Over Credit Card Data on Receipts

Courier-Journal (07/24/07) ; Davis, Alex

Two lawsuits filed against KFC and Taco Bell earlier this month claim the fast-food chains violated a law that limits the amount of credit card information companies can print on customers' receipts. The suit against KFC, which was filed July 11 in U.S. District Court in New Jersey, claims that a KFC restaurant in Shamong, N.J. illegally printed the expiration date of a customer's credit card on a receipt. The lawsuit claims that a skilled hacker could use the expiration date and the last four digits of a credit card number to engage in fraud or identity theft. The lawsuit against Taco Bell, which was filed July 5 in federal court in Illinois, also claims that the restaurant printed the expiration date from a customer's credit card on a receipt for a purchase made in June.

Wharton/ASIS Program for Security Executives

The security risks facing your organization are greater than ever, yet these rising challenges may not be reflected in your budget. How can you communicate a clear business case for investments in security? How can you present your strategy so the C-suite will listen and approve your recommendation? How can you manage your own resources to make the most impact for your organization? *Wharton/ASIS Program for Security Executives: Making the Business Case for Security* offers core business knowledge from one of the leading business schools. This 2-week certificate course is taught by many of the same faculty who have made Wharton's MBA program one of the top-ranked in the world. The *Wharton/ASIS* program covers the core concepts of business to broaden your managerial and strategic perspectives, enhance your business instincts and sharpen your ability to tackle management challenges. It will help you work more effectively with other leaders in your organization and communicate the bottom-line impact of security decisions. Registration is now open for the next offering of this highly successful, two-week program designed for CSOs and those aspiring to that position: November 25-30, 2007 and February 3-8, 2008.



Profiles in Excellence - Mr. P. Kevin Smith, Chevy Chase Bank



**Mr. P. Kevin Smith, CPP
Senior Vice President
Corporate Security Director
Chevy Chase Bank**

Mr. P. Kevin Smith is a Certified Protection Professional through the American Society for Industrial Security (ASIS), where he has been an active member of the Banking & Financial Services Council for more than 12 years. He is a Senior Vice President and Corporate Security Director for Chevy Chase Bank in Bethesda, Maryland, a \$16 Billion Federal Savings Bank with approximately 300 branches and 1,000 ATMs in the Baltimore/Washington Metropolitan area.

Mr. Smith's protective services career began in 1973, when he joined the Wilmington, Delaware Police Department, where his father served as Chief of Police until 1966. In fact, law enforcement is a Smith family tradition. Mr. Smith's brother, John J. (Chip) Smith, Jr., started with the WPD in 1970 and went on to a very successful career with the US Secret Service. Chip is now the Corporate Security Director for Bank of New York. During his WPD career, Mr. Smith served six years in the Crime Prevention area, an assignment he credits for much of his success in the bank security field. He opted for an early retirement in 1987, after achieving the rank of Lieutenant, when he was recruited by the Wilmington Trust Company to become Director of Security for Delaware's largest retail bank. Following a successful career at Wilmington Trust Company, Mr. Smith tossed his hat into the national ring and landed in Nashville, Tennessee as the Corporate Security Director for First American Bank, a 23 billion financial institution serving seven states in the southeast. In 2000, he was recruited by Chevy Chase Bank to direct their corporate security program, and he's been there ever since.

Mr. Smith holds a Master of Science degree in Administration, and a Bachelor of Science degree in Criminal Justice, both from West Chester University, in West Chester, Pennsylvania. He is a past chairman of the ASIS Council for Banking & Financial Services, and a member of the ABA Fraud Prevention Oversight Council. He also serves as the Security Committee Chairman for the Maryland Bankers Association and is a member of the Bank Administration Institute's Security Commission. Mr. Smith has lectured nationally on a variety of bank security topics for the Bank Administration Institute, the American Bankers Association, Bankers Online, and numerous trade associations. A recognized expert in the bank security field, he has also been published in several national security journals and periodicals.

Kevin and Judy, his wife of 34 years, reside in Elkridge, MD, and are the proud parents of two very successful young men. Todd, who lives in Chicago, is a Director of Event Technology for the Marriott Corporation, and Drew, of Scottsdale, AZ, is an assistant manager of the Coach store at the Kierland Commons Mall. In his spare time, Kevin may usually be found on the golf course, where he claims, "there is so much to concentrate on, you can forget about the job for a while".