

ASIS Councils NEWSLETTER

Banking and Financial Services Council

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

Banking and Financial Services Council November – December 2007

Seasons Greetings

The Holiday Season is with us again!!! It time to reflect on the challenges and accomplishments of this year as well as the challenges and goals for 2008. Let us also reflect on the many blessings we have and strive to make a difference the lives of others this season. What better season and reason to give of ourselves to others. On behalf of our Council President Kevin O'Brien, our President-elect Larry Brown, and all the members of the ASIS Banking and Financial Services Council, we want to wish you a very Happy Holiday Season and our hopes for a prosperous New Year!

In The News

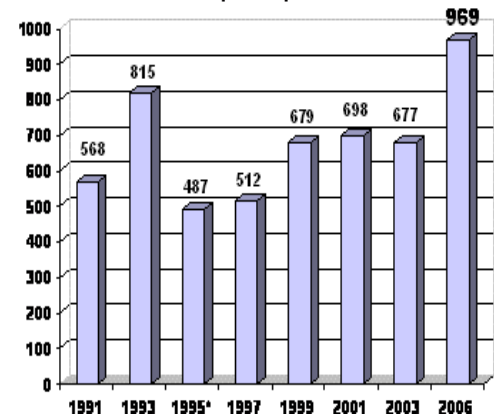
Attempted Check Fraud Doubles to \$12.2 Billion According to ABA Survey. ABA News

Attempted check fraud at the nation's banks has more than doubled in the past three years reaching an estimated \$12.2 billion in 2006, according to the latest American Bankers Association Deposit Account Fraud Survey Report.

While *attempted* check fraud continued to rise, the increase in *actual* dollars lost was less dramatic -- \$969 million compared to \$677 million in 2003, the last year of ABA's survey. Banks' check fraud prevention systems were credited with keeping actual losses significantly lower than the attempted fraud numbers. Attempted fraud totaled \$5.5 billion in 2003.

Counterfeit checks, stemming from crimes such as check and wire and lottery scams, has now become the fastest growing cause of actual dollars lost, increasing from 15 percent of the total actual dollar loss in 2003 (or an estimated \$104 million) to 28 percent in 2006 (or an estimated \$271 million). While the number of check fraud cases actually decreased from 616,469 cases in 2003 to 561,306 cases in 2006, the average loss per case increased from \$1,098 in 2003 to \$1,727 in 2006.

CHECK FRAUD LOSSES AT U.S. BANKS
(trillions)



All types of fraud combined, the median loss per bank varied from \$9,994 for community banks, to \$43,350 for mid-sized banks, to \$698,955 for regional banks, and to \$6.7 million for the largest institutions. (See explanation of bank sizes in "About the Survey" at the end of the release.) The amount of check fraud loss from individual accounts declined slightly from 77 percent in 2003 to 75 percent in 2006. However, check loss from small business accounts rose slightly from 14 percent in 2003 to 16 percent in 2006. On average, 44 percent of community banks' 2006 check fraud losses could be attributed to organized customer scams such as fake lottery scams. Counterfeit checks had the highest median loss per case at \$2,758 followed by kiting and alterations, both at \$2,000.





FTC Releases Survey of Identity Theft in the U.S. Study Shows 8.3 Million Victims in 2005. ABA News

The Federal Trade Commission today released a survey showing that 8.3 million American adults, or 3.7 percent of all American adults, were victims of identity theft in 2005. Of the victims, 3.2 million, or 1.4 percent of all adults, experienced misuse of their existing credit card accounts; 3.3 million, or 1.5 percent, experienced misuse of non-credit card accounts; and 1.8 million victims, or 0.8 percent, found that new accounts were opened or other frauds were committed using their personal identifying information.

"Whether you're from Malibu or Manhattan, Tacoma or Tallahassee, no one is immune to identity theft," said Lydia B. Parnes, Director of the FTC's Bureau of Consumer Protection. "The important thing is that people learn how to deter identity thieves, detect suspicious activity on their financial records, and defend against the crime, should it happen."

The survey found that the costs associated with identity theft varied widely. The survey first looked at the value of the goods or services that the thieves obtained using the victims' personal information. In at least half of all incidents, thieves obtained goods or services worth \$500 or less. In 10 percent of cases, however, thieves got at least \$6,000 worth of goods or services.

The survey also gathered information about victims' out-of-pocket expenses resulting from the theft of their identities. In more than half of the incidents, victims incurred no out-of-pocket expenses. Some victims, however, incurred substantial out-of-pocket expenses – 10 percent of all victims reported out-of-pocket expenses of \$1,200 or more.

In addition, the survey asked victims to estimate the amount of time they spent resolving problems caused by the theft. The median time spent resolving problems by all victims was four hours. Ten percent of victims, however, spent at least 55 hours resolving their problems, and half of those spent at least 130 hours.

The survey found that thieves obtained more goods and services – and victims spent more time and money recovering – in cases where the thief opened new accounts rather than only hijacking existing accounts. Where the theft was limited to the misuse of existing accounts, the median value of goods and services obtained by the thieves was less than \$500. Where the thieves opened new accounts or committed other frauds, the median value of goods and services they obtained was \$1,350.

Banks Make 1,088 Terror Tip-offs BBC News

Financial institutions in the UK submitted 1,088 Suspicious Activity Reports (SARs) related to possible terrorist activity in the last year. All told, there were over 220,000 SARs filed between October 2006 and October 2007, mostly by banks suspicious of money laundering or terrorist financing. Security officials say that SARs are vital to identify and stop money laundering by terrorists and organized crime. The Serious Organized Crime Agency (SOCA) spends 7 million pounds a year overseeing SARs, and have petitioned the government for an extra 10 million pounds a year to overhaul their IT infrastructure. "SARs produces at least that amount of return," said SOCA representative Paul Evans. "By following the movements of illegal finance, we build knowledge of criminal organizations and hit them where it hurts."



CYBER SECURITY NEWS

FBI Director Targets the Internet's Top Dangers Network World

FBI director Robert Mueller spoke on Nov. 6 about the dark side of the Internet and the army of experts working to battle the numerous online dangers. Mueller used the example of al Qaeda Web master Younis Tsouli to illustrate how infiltrated servers and scams can finance or aid terrorists. Tsouli broke into servers to steal bandwidth, mounted phishing schemes to access credit card accounts, and founded a Web site for terrorists. Mueller pointed out that the Internet is a target for attacks as well as a means for launching attacks. The "cyber blockade" of Estonia's federal and infrastructure-related Web sites in April 2007 was the example used by Mueller to illustrate this threat. Botnets and hackers continue to wreak havoc as well, from disabling power grids to stealing sensitive intelligence. However, cyber criminals are increasingly being found and prosecuted by specialists in Regional Computer Forensic Labs. But because a growing number of cyber threats are coming from abroad, more international collaboration on such investigations is essential, Mueller said. The FBI's Cyber Fusion Center is another valuable resource that lets cyber experts, federal agents, merchants such as Target and Bank of America, and others discuss security breaches and cyber threats. Finally, the FBI's InfraGard program works on the community level to let members share data about risks to their own businesses through a secure computer service. Almost 21,000 members--from small companies to Fortune 500 businesses--currently participate in this localized private sector partnership, according to Mueller.

Top 5 Security-Menace Predictions for 2008 Network World

Oliver Friedrichs of Symantec has outlined the top five anticipated Web threats for 2008. He forecasts that bots such as the malicious Storm worm will frequent attacks through peer-to-peer networks. Due to bots' lack of a centralized center, they are difficult to isolate and immobilize. Web sites remain a target for hackers plugging malicious codes into seemingly safe sites, while social networking sites will hold the most potential for future targeted attacks. The increasing usage of Web access via mobile phones will lead cybercriminals to potentially interfere with consumers attempting to conduct mobile banking operations or perform in auctions. Virtual world-games such as Second Life and World of Warcraft will also receive their share of hackers, who will attempt to hijack other players' accounts for profits. Finally, the presidential elections will likely endure cyberattacks, as former candidates have experienced phishing and denial-of-service attacks. As candidates take online contributions, hackers could either interfere with the transmission of funds from one party to another or pilfer the profits themselves.

Best Practices Corner

The Changing Face of Security Security Products Magazine

To enhance security at access points, managers should consider three-dimensional (3-D) face-reading biometrics, which offer greater security and authenticity than 2-D devices or card readers. While video cameras and 2-D readers are inhibited by factors like light and shadow, 3-D readers employ near-infrared light sources that reflect the contours of a person's face. Many 3-D readers such as Bioscrypt's VisionAccess software work in conjunction with card readers and fingerprint scans, and can be set to different thresholds of security.



Banking and Financial Services Council Survey Results

Recently our fellow council member Bob Ballagh conducted a survey of how financial institutions conduct their pre-employment screening processes. The survey specifically questioned what management function owned the pre-employment screening process; who conducted the process; as well as the size of the pre-screening staff. Depicted below is the summary of the survey which highlights some very interesting trends.

1. Who "owns" the pre-employment screening process, HR or Security?

In all cases, HR owned the policy for pre-employment screening, but partnered with the security team for the background investigation. Security managed the process and the investigation, especially in the case of adverse information.

2. Is screening done by an in-house staff, or is it outsourced, or is it a combination of both?

All banks use a combination of outsourced information (FBI database or vendor such as ChoicePoint or Verifications) and internal resources to complete investigations and fill in the gaps.

3. If HR is the owner, what role does the security team play in reviewing the results of pre-employment and post employment screens?

Security ensures compliance with the established standards and reports results of further investigation of exceptions to HR.

4. Who has the final say on whether an offer should be made if the results are less than sterling: HR, Security, or hiring manager?

Security recommends hire/no-hire to HR based on results of investigation and compliance with established standard. If there is a disagreement with HR and/or the hiring manager, higher management gets involved to resolve. In one case, Security recommends directly to the hiring manager (but informs HR).

5. What is the average size of investigative staff that handles the screening?

Range is one to eight people. In one case, an individual coordinates the investigation among 75 local individuals (distributed work load) who perform local checks as part of their normal security function.

6. Does the investigative staff (wherever it is located) contact references and prior employers about the candidates?

In most cases, the Security team contacts previous employers and references, especially if vendors are unable to do so or if there appear to be issues. One respondent considers it the responsibility of the hiring manager.



Profiles in Excellence - Mr. Kevin O'Brien Bank of New York - Mellon



Mr. Kevin O'Brien, CPP
Vice President
Corporate Security Director
Bank of New York - Mellon

Mr. Kevin O'Brien is an active member of ASIS and the outgoing ASIS Banking and Financial Services Council Chair, a position he has served in for 3 years. Mr. O'Brien holds the position in the Corporate Security Department of Vice President, Global Physical Security Manager and Chief Administrative Officer (CAO) for The Bank of New York Mellon in New York City. He is also responsible for the physical protection of this \$180 billion financial institution, covering 37 countries on 6 continents with over 40,000 employees. As CAO, Mr. O'Brien has been the lead manager for the Company's Corporate Security Department through two acquisitions and mergers over the past two years, and manages the administration of the Department.

Mr. O'Brien has been with The Bank of New York Mellon since 2000 and was promoted to his current role in 2002, shortly after the Company was able to re-occupy its office space in downtown, NYC. Reflecting on his career at The Bank of New York Mellon he mentioned the events of 9/11; "Working through the events of 9/11/01, the large scale relocation and restoration process, among many things, was the most profound single learning experience of my lifetime. Working with great people within the Corporate Security Department as well as the Company and the citizens of the city and country that came to help is (hopefully) a once in a lifetime experience that taught me more about myself and this industry than I ever could have imagined." Part of the team Mr. O'Brien mentions is Chip Smith, Managing Director, Director of Global Corporate Security at The Bank of New York Mellon, Kevin's supervisor and mentor for his entire tenure at the Company.

Prior to joining The Bank of New York Mellon, Mr. O'Brien spent time with HSBC and Republic National Bank both in New York City, holding progressively higher positions within the Corporate Security Departments. He also spent several years with a small security firm that offered numerous services holding several positions in sales and operations. The security industry has been the mainstay of Mr. O'Brien's career, however, it should be mentioned that he holds a Bachelor of Science degree in Education and was a teacher in Brooklyn, NY for 4 years – something he eventually wants to do again.

Kevin resides in Middletown, NJ with his wife Jennifer of 12 years and 3 children; he speaks often of his family of which he obviously could not be prouder of.

