

In this issueFrom the Chairman **P.1**4th Annual Roundtable forECC Declared a Success! **P.2**Pump & Dump Fraud **P.3**

The Center for Information Security

Awareness Offers Free Training **P.5**Searching Across Social Networks **P.5**Membership Directory **P.6****ECC OUTREACH****July 2009 –**

Association of Certified Fraud Examiners 20th Annual Fraud Conference (Las Vegas, NV): Pending presentations by R.A. [Andy] Wilson, Cynthia Hetherington and Jon McDowall.

**From the Chairman**

As I write this, reminders of a faltering global economy abound. Recession, repossession, reorganization, corporate down-sizing and related bailouts seem to have the full attention of the media.

History shows that economic downturn can translate to opportunity. For those with diminished scruples and defective moral compasses, fraud schemes of all sorts are pursued. For those of us who have built careers and reputations around economic crime fighting, the present economy will almost certainly provide different, though related, opportunities.

In January, the Economic Crime Council hosted its fifth annual Roundtable event at the Secret Service Headquarters in Washington, D.C. Invited guests from ASIS membership, councils and various nations participated as panelists, providing insight and commentary on emerging areas of economic crime, such as mortgage fraud, counterfeiting schemes and Second Life™.

As I enjoyed the tremendous networking and information sharing benefits of this roundtable, I was reminded yet again of the increasingly sophisticated and global nature of today's fraud schemes.

Thankfully, the ASIS International Economic Crime Council has risen in lock-step with today's fraud schemes with representation, cooperation, information-sharing and educational initiatives on several continents.

Though the current state of the economy is unnerving, there can be no doubt that opportunities will abound in the coming months for dedicated and experienced economic crime fighters and security professionals. Those who possess the insight to see and seize these opportunities will most certainly be rewarded with interesting casework, satisfaction of jobs well-done and, hopefully, related monetary reward.

In this increasingly globalized economy, the ASIS Economic Crime Council is of more relevance and value than at any time in its history. Our economic crime-related educational efforts have never been needed more than they are right now. I am honored to be associated with this amazingly-gifted group of professionals.

Jon McDowall**INTERVIEWS**

Feb. 19, 2009, R.A. (Andy) Wilson was interviewed by WMC-TV Channel 5, a NBC News affiliate regarding the allegations levied by the Securities & Exchange Commission against Sanford Financial executives surrounding a financial fraud scheme involving certificates of deposit.

4th Annual Roundtable for Economic Crime Council Declared a Success!

On Jan. 13, 2009, the United States Secret Service hosted the Economic Crime Council and members of the security community for the 4th Annual Economic Crime Roundtable. Held at the U.S. Secret Service headquarters in Washington D.C., the event drew a crowd and provided an exciting opportunity to network with security and law enforcement professionals.

In convivial and open discussions, attendees learned and shared information on emerging trends within the economic crime arena and received valuable information from subject matter experts.

Mike Osborne (outgoing ECC Chair) was recognized for his leadership, dedication and for making the ECC a leading ASIS International Council.

Several exceptional subjects were addressed. Sharon Ormsby, Section Chief, Financial Crimes Section Federal Bureau of Investigation provided some much needed clarity on the topic of *Mortgage Fraud: Analysis, Schemes, and Impact*.

Tripp Brinkley, Program Manager, Global Security & Investigations Division, U.S. Postal Inspection Service,



presented a frank and informative travelogue of his experiences conducting international investigations.

Kevin Sullivan, Investigator, New York State Police, previously assigned to HIFCA El Dorado Federal Task Force, provided an insightful examination of the potential for Fraud in the Virtual Worlds, focusing on Linden Labs' Second Life™.

Bud Miller, President-Efficient Research Solutions, Inc., in his presentation "*It is Not Just about Cents - The High \$\$ Cost of Coupon Fraud*" revealed the truly fascinating world of coupon fraud – a crime of surprising economic proportion that damages retailers and brands alike. Bud shared his expertise in describing the criminal enterprises and ways to remediate this crime.

Jon McDowall, incoming ECC Chair, wrapped up the 4th Annual Roundtable by voicing his commitment to the ECC and ASIS International.



Back row (L to R): Sharon Ormsby, Danny Platt, Dan Draz, John Hartness, and Stuart Tryon
Middle row: Mike Osborne, Andy Wilson, Tripp Brinkley, Mike Levin, Budd Miller
Seated: Kim Wood and John McDowall



Mike Osborne, (L) Outgoing Council Chair and **Jon McDowall, (R)** Incoming Council Chair

Pump & Dump (P&D) Fraud

By Mike Susong, iSIGHT Partners, Inc.

Overview

Pump and Dump (P&D) fraud is a new type of fraud largely realized in the 21st century. The roots of it come from a stock boom in the 1990s that led to many different sources of information and trust. It wasn't long before independent, unprofessional sources started predicting stock investments with greater returns than the experts and people started looking for "get rich opportunities" in very new ways on the Internet.

P&D fraud traditionally involves fraudsters purchasing penny stocks (pink sheets), sending out e-mails to promote the stock or posting data in forums and then dumping the shares for personal profit while devastating the penny stock investment fund. Traditional profits easily resulted in a 200 percent profit margin in multiple anecdotal cases.

Pump & Dump fraud involves many techniques and innovation related to anti-spam and financial fraud. Malicious code is traditionally known to be affiliated with P&D through codes that act as spambots, as well as computers that are compromised and then used to send out P&D spam.

Introduction to P&D Fraud

Traditional P&D fraud involves a fraudster investing in a penny stock fund and then promoting it to many users online, hoping to promote investment in the fund. This raises the value of their stock and enables them to dump their stock later for significant profit. Following are the common attributes of P&D fraud:

- E-mails are sent to many users attempting to lure some into investing in a stock.
- The stock promoted is inexpensive, typically a penny stock under a dollar.
- E-mails are constructed with confidence, using a professional appearance and HTML and/or image spam techniques along with reference to trusted names, such as ZDNet and IBM in this example.
- Promotions for penny stocks typically promise a huge gain in the stock in a short period of time (get-rich-quick social engineering).

P&D spam research reveals that the distribution of such content usually takes place during the weekday, not weekends. Message distribution shows slightly more messages earlier in the week, with Tuesday as the most frequent date of distribution and Friday as the least. This is, in part, reflected in the distribution schemes implemented by fraudsters and also in time zone differences, resulting in a low for Friday (whereas Sunday evening messages are counted as Monday for the start of the work day in Asia). The summary of spam distribution is that P&D fraud is not distributed on weekends, but during the day for maximum possibilities in both consumer and corporate e-mail account opportunities.

Video Vector

A new series of spam-mailing campaigns containing high-quality video was identified in late December 2007 and January 2008. These mailings promoted small-volume, low-priced stocks from a variety of companies in the oil and extractive industries. Such tactics correspond to "pump-and-dump"-style stock manipulation fraud scams. These stocks are usually supported by a variety of sophisticated advertising campaigns, including press releases and graphics-heavy websites.

The video used in these campaigns consists of 30- to 60-second clips that are activated based on embedded links within the e-mail. The video has a professional appearance, with good audio voiceovers by "financial analysts." Alternatively, some spam has been identified that aims to have the user query popular search engines for the videos based on a list of provided keywords.

Malcode Vector

In 2006, P&D fraudsters utilized a new, zero-day exploit for Windows Meta File (WMF) MS06-001 to spread malcode that acted as a spambot for P&D fraud. A hostile WMF file was hosted at beehappy.biz, which resulted in silent installation of malicious code on a computer. After installation, the code began a mass mailing routine, sending out P&D stock spam purportedly from Small-cap Investors, which promoted a Chinese pharmaceutical company called Habin Pingchuan Pharmaceutical (PGCN). Spam e-mails contained image spam to subvert anti-spam techniques at the time.

This P&D fraud infected many computers through an exploit vector sending out large volumes of spam for this and related P&D stocks. In this instance, the stock PGCN was changed to PGCN.OB. According to Yahoo Finance, at the time a spike in the stock price took place around the date of exploitation of WMF and Trojan attacks. The stock experienced a 100 percent increase in the value (going from \$.4 to \$.8 in a very short period of time. This inflated value quickly plummeted within a few days. Running a Yahoo finance chart on this stock, which has now changed to the symbol SZSN.OB, from the period 2004 through October 2008, showed its value as significantly declined since the days of P&D exploitation in 2006.

Pump & Dump (P&D) Fraud (continued)

Wrong Number P&D Fraud – Voice & Fax Vectors

The Securities and Exchange Commission (SEC) has identified a "wrong numbers" stock tips calling fraud technique used for P&D fraud. Fraudsters make voice calls to individuals, leaving a message promoting a stock. The fraudsters leave a call as if they know the individual. The victim quickly realizes that he or she doesn't know the person and that it's just a message left at the wrong number. Meanwhile, the message explains that they have a hot stock tip on a company that will make "a lot of money fast." They ask the person to call them on their cell phone but don't leave a number and then personalize the message at the end of the call. P&D victims then think they have some hot information accidentally leaked to their message machine, check it out online and purchase the stock. Fax submissions are also done this same way. Unsolicited fax messages are sent to fax machines with notices that are similar to HTML e-mail stock promotions utilized in P&D fraud.

Compromise Vector

Account credentials for online trading accounts (like E*Trade) make it possible for fraudsters to manipulate accounts for their financial gain. Large-scale fraud is then possible through traditional P&D promotion; fraudsters (both buying and selling through compromised accounts) make money in both directions as they exploit accounts and specific investments of interest. LPL Financial Corporation suffered a hacking compromise of 14 financial advisors and four assistants in branch offices. Fraudsters gained access to over 10,000 customer accounts to manipulate P&D stocks to their advantage.

Regulation S Vector (Chop Stock Fraud)

Stocks sold to offshore foreign investors do not need to register stock according to Regulation S. This form of P&D fraud involves a microcap company selling unregistered stock at a deep discount to purported foreign investors who are actually fraudsters. They then turn around and sell the stocks to U.S. investors for a huge profit. This eventually leads to a depletion of value for the stock, with U.S. investors suffering significant losses.

A 2007 news article in Business Week identified this aspect of criminal activity involving many so-called "chop stocks" among the microcap stocks, discussing how billions of dollars are taken from small investors in the process. The article noted that "chop stocks constitute a vast underworld of the securities markets--a \$10 billion-a-year business that regulators and law enforcement have barely dented in their recent prosecutions."

"Poop & Scoop" Fraud

This is slang for a related form of P&D fraud, where actors attempt to spread false rumors to discredit a company and drive the price of stock down. The actor buys when the stock is low, waiting for it to rebound after rumors are dispelled.

Mitigation

Penny stocks are not normally traded frequently. It is common for such stocks to have no trading activity for any given day. By monitoring trading volumes on penny stocks, it is possible for financial organizations to quickly identify potential penny stock fraud and take appropriate counteractions.

The SEC suggests the following tips:

- Research investments at the SEC Edgar database at <http://www.sec.gov/edgar.shtml>.
- Use licensed and registered brokers and research them before conducting business.
- Research the owners of companies to see if they have a history of trust or fraud.
- Register complaints at:
 - <http://www.sec.gov/complaint.shtml>
 - enforcement@sec.gov
 - 202-772-9295 Fax
 - 1-800-SEC-0330 VOICE

The Center for Information Security Awareness Offers Free Training

Recently, ECC members Jon McDowall and Michael Levin announced that The Center for Information Security Awareness, which they co-founded with long-time friend and security expert Neal O'Farrell, had formed a partnership with the InfraGard National Members Alliance, a collaborative effort between private sector security professionals and the Federal Bureau of Investigation.

The resulting FREE information security awareness training may be found at www.InfraGardAwareness.com. This web-based course, created by The Center for Information Security Awareness, is professionally narrated throughout and consists of 14 separate lessons covering key information security issues that can impact the workplace. These include the following:

- Cyber threats to the workplace and the nation
- Understanding how employee behavior is exploited
- The importance of regulatory compliance
- Better workplace security
- Effective password practices
- Understanding social engineering
- Improved e-mail practices
- Safer web-surfing practices
- Protection of sensitive data, as well as laptop, PDA and mobile security

Participants can also elect to obtain their personalized InfraGard Certificate in Information Security Awareness in the Workplace. More information may be found at www.GetSecurityAware.com and www.InfraGardAwareness.com.

Searching Across Social Networks

By Cynthia Hetherington, President of The Hetherington Group

Spokeo.com

Spokeo.com is the search engine designed specifically to locate online profiles within Social Networks and track them. This very direct site allows you to search by a person's name, their e-mail address, or phone number. You can also paste in the actual URL for a Myspace.com (or similar) profile and set it up for tracking. A list of their supported services, can be found at the following site: http://www.spokeo.com/blog/?page_id=127.

For investigators and researchers, this is an incredible tool that helps us track down subject information in a way Google.com never did. You may know about the subject's profile in Facebook.com and Myspace.com, but were you aware that they were also listed in Hi5.com? Are they in Xanga? Did you even know what Xanga was? One of the great features for Spokeo, is that as they are adding partner sites to search queries, and tracking those members. Spokeo also makes us aware of new sites. For example, Wretch.com is a Chinese social network and Hi5.com is rather popular in India. All of these services become apparent as you start using Spokeo.com. You can search and track the first handful of e-mail addresses or names for free. But after a limit of searches, you will be required you to pay about \$24.00 per year, or \$2.00 per month. It's worth it!

yoName.com

Yoname.com is very similar to Spokeo.com and searches 18 of the same services that Spokeo.com does.

The exception to Yoname.com is that it is a free service. However, the results are a bit random. Often, I will run a search by e-mail or the name of someone I know that has a profile, yet it does not appear. Spokeo.com has a better return rate on its searches. It's important to note with Yoname.com: If you search by a users e-mail address, they will get an e-mail sent to them stating someone was looking up "yo name" in Yoname.com. The e-mail does not contain your information, but it could be enough to alert a suspicious fraudster.

Cynthia Hetherington is a Licensed Private Investigator and the president of Hetherington Group, an investigative consultancy specializing in due diligence.

Membership Directory

Council Chair

Jon McDowall, CFE, PCI, CIFI, CII
Chief Executive Officer
Fraud Resource Group
jon@fraudresourcegroup.com

1st Vice Chair

John Hartness
Security Officer
State Farm Bank
john.hartness.gbea@statefarm.com

2nd Vice Chair

Kimberly C. Wood, CMA, CFE
Manager of Investigation
Dow Chemical Company
kwood@dow.com

Senior Advisor

Michael W. Osborne, CPP
Director Global Security
Kinross Gold Corporation
Mike.Osborne@kinross.com

Members

Joel Bartow, CFE, CPP
Director, Program Integrity
Express Scripts
jbartow@express-scripts.com

Fred Cantz, CPA, CFE
Sr. Manager, Internal Audit
University of Medicine and Dentistry
of New Jersey
Fred.cantz@umdnj.edu

George Curtis
Associate Professor
Economic Crime and Justice Studies
– Utica College
gcurtis@utica.edu

Bruce Dean, JD, CPP, CFE
Investigative Management
Consultant
bruceadamsdean@aol.com

Daniel W. Draz, MS, CFE
Corporate Investigations Manager,
TransUnion
ddraz@transunion.com

Peter Grant
Managing Director
C Risk International (Pty) Ltd
Petergrant@criskinternational.com

Cynthia Hetherington, MLS, MSM
President, Hetherington Group
ch@hetheringtongroup.com

Ponno Kalastree, CII, IWWA
Managing Director
Mainguard International Pte Ltd
p.kalastree@Mainguard-intl.com.sg

Michael Levin
CEO
MyPCITraining.com
mdlevin@myPCITraining.com

George H Millard, JD, MBA
Police Chief and Professor
Sao Paulo Police Academy
millard@terra.com.br

Edmund "Bud" Miller, CPP
President
Efficient Research Solutions, Inc.
ersalexandria@msn.com

Karl Perman
Manager, Corporate Security
Programs – Exelon
karl.perman@exeloncorp.com

Daniel Platt
Manager, Global Security
Avon Products, Inc.
Daniel.platt@avon.com

Mike Susong, CPP
Vice President/Chief Risk Officer
iSIGHT Partners, Inc.
msusong@isightpartners.com

Bill Wagner, CPP
Manager of Security and Safety
American Hotel Register Company
bwagner@americanhotel.com

R.A. (Andy) Wilson, CFE, CPP
Managing Director Wilson & Turner Inc.
raw@wilson-turner.com

Government Members

Tripp Brinkley
United States Postal Inspection Service
tbrinkley@uspis.gov

Sharn Ormsby
Federal Bureau of Investigation
Sharon.ormsby@ic.fbi.gov

Stuart Tryon
United States Secret Service
stuart.tryon@uss.s.dhs.gov

ASIS Council Vice President

Richard Chase
Special Agent in Charge
U.S. Department of Justice (ATF)
1961 Stout Street, Suite 674
Denver, Colorado 80294
Richard.E.Chase@usdoj.gov