Cybercrime, Cyberforensics and Electronically Stored Information

Joint Presentation of

Northern California East Bay Chapter

Institute of Internal Auditors

And

San Francisco Chapter

ISACA

January 9, 2014

Chevron – Bishop Ranch 1 – San Ramon, CA

Presenters

John Steensen | CISA, CRISC
IT Audit Manager
Safeway Inc.

Tim Bryan | CPA/CFF/CITP, CISA, EnCE
Forensic Technology Services
Crowe Horwath LLP

Presentation Overview

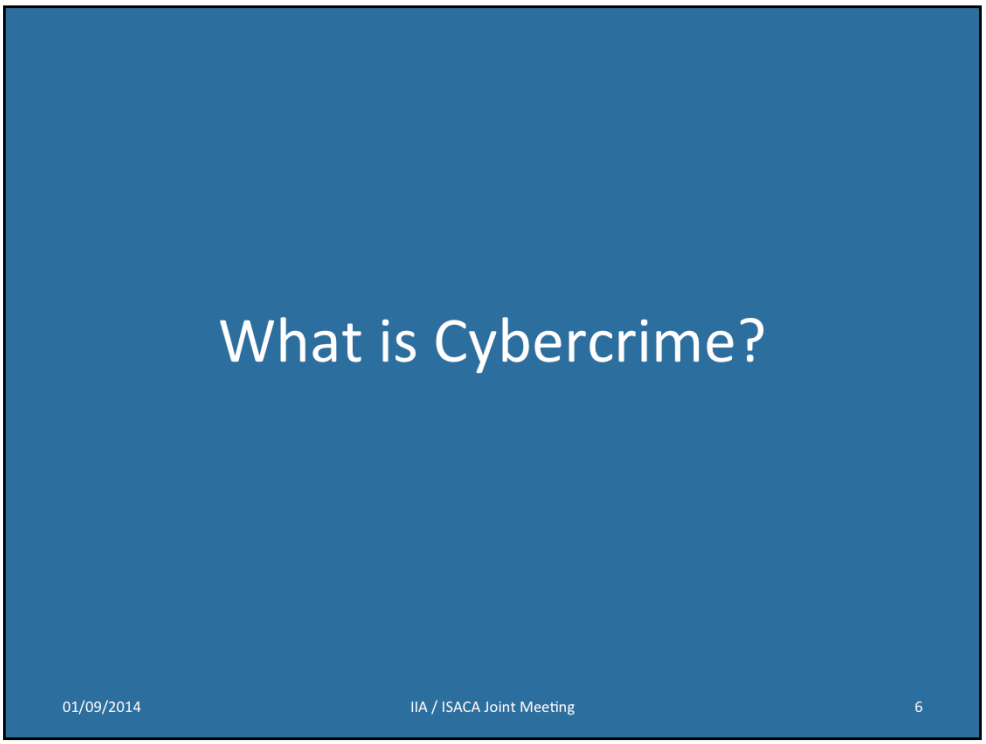
- Cybercrime – An Evolving Landscape
- Cyberforensics – The Heavy Lifting
- Questions and Answers

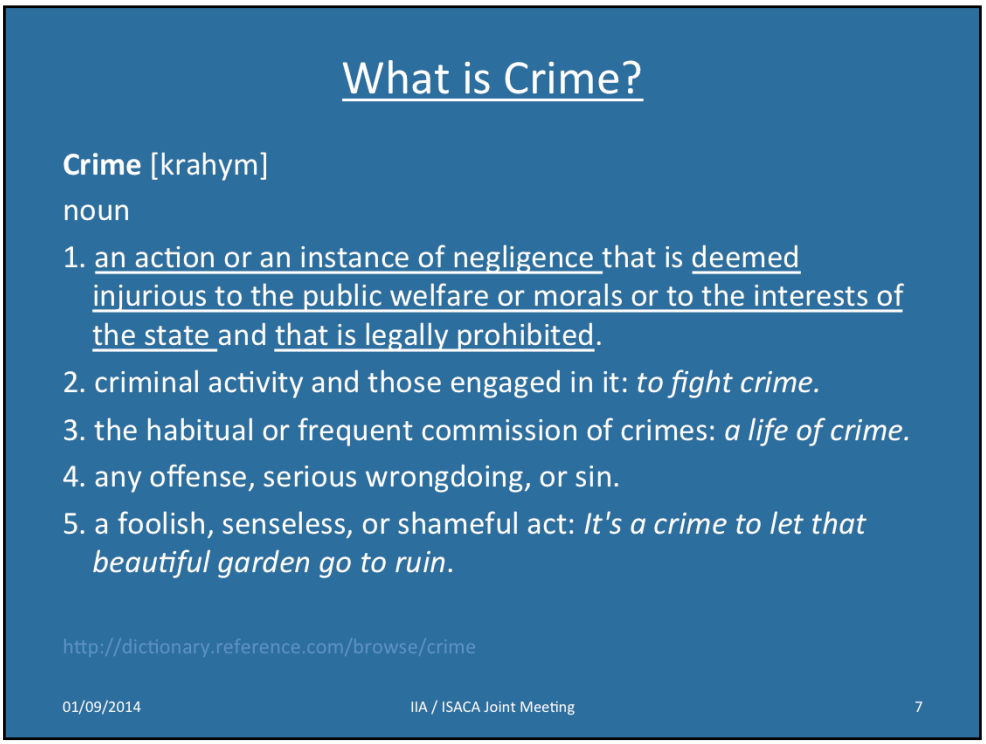
Disclaimers

- I am not a lawyer and nothing in this presentation should be construed as legal advice. If you have questions please consult your personal or corporate legal counsel.
- Furthermore, nothing in this presentation reflects information regarding Safeway, its employees, its business partners or its position with regard to any of the material presented.

Cybercrime – An Evolving Landscape

- What is cybercrime?
- Is cybercrime a serious threat?
- What types of cybercrime are most prevalent?
- How can you protect yourself from cybercrime?
- What are your options if you think you or your company is a victim of a cybercrime?


What is Cybercrime?
01/09/2014
IIA / ISACA Joint Meeting
6

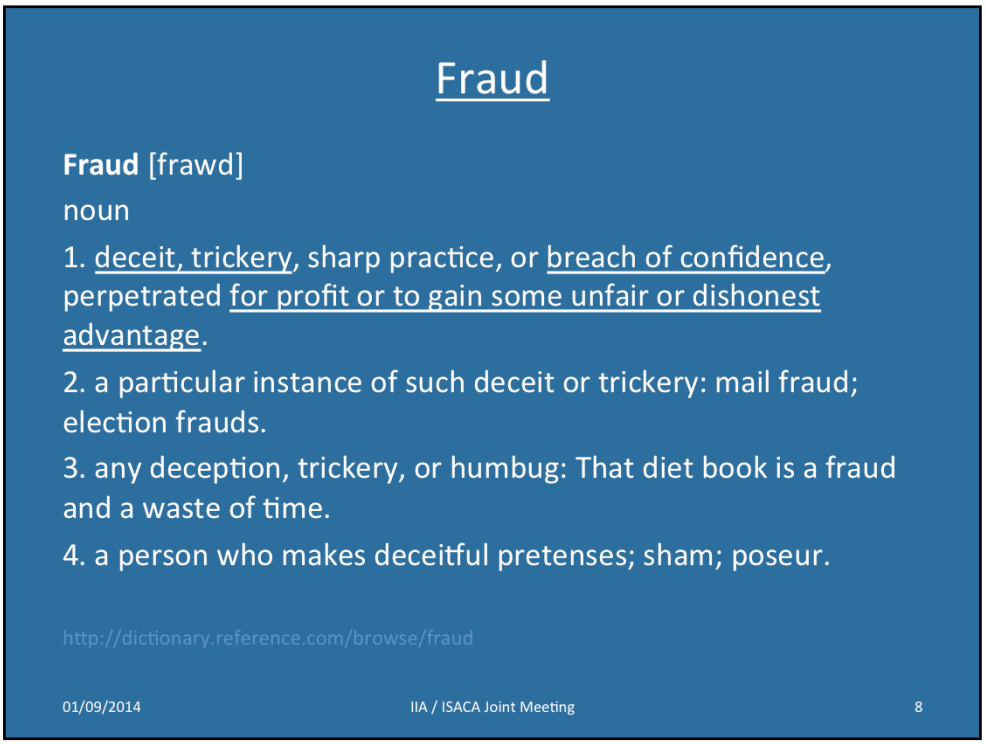


Current slide:

Something you did, or something you failed to do, that is "deemed injurious" (i.e., causes harm) to "the public welfare or morals" (prevailing attitudes of society) or to "the interests of the state" (i.e., the government that codifies the crime) AND "that is legally prohibited". This is an essential element – if it is not legally prohibited then it is not a crime.

Lead-in to next slide:

The primary type of crime associated with computers is fraud.



Current slide:

In particular we will be discussing crimes involving fraudulent behavior often perpetrated using false personas or falsely using real personas.

So, could the government have defined crimes involving electronic communication 100 years ago? Yes – with telegraphs and telephones.

Lead-in to next slide:

What are the chances that you inadvertently committed a crime today?

40,000 New Laws

"Across the US, 40,000 new federal, state and local laws are set to go into effect [on 1/1/2012], ranging from states requiring ID's to vote, minimum wage hikes and rules for light bulbs."

Many of these new laws relate to the use of computers, mobile phones and the Internet as facilitating illegal behaviors.

http://www.nbcnews.com/id/45819570/ns/us_news-life/t/new-laws-toughen-rules-abortions-immigrants-voters/

What is Cybercrime?

Simply put "a cybercrime is a crime committed within **cyberspace**."

So what is cyberspace?

cy·ber·space [sahy-ber-speys] noun

1. the realm of electronic communication.

2. virtual reality.

Coined in 1982, often as two words at first, by science fiction writer William Gibson (best known for "Neuromancer") and used by him in a short story published in 1982, from cyber- (see cybernetics) + space.

http://dictionary.reference.com/browse/cyberspace

Why use Computers or Electronic Devices to Commit Crimes?

- The perpetrators or criminals can remain hidden
- The perpetrators or criminals can choose the jurisdictional venue to operate from
- The means to commit the crime can remain hidden or obscured
- Evidence regarding the crime may be more difficult to identify, collect and attribute
- Criminally acquired assets may be hidden or placed into jurisdictional limbo

Why use Computers or Electronic Devices to Commit Crimes?

- The perpetrators or criminals can remain hidden
  - They can work through third party services such as BotNets
  - They can use relay services or systems to reduce the chances of detection and identification
  - They can use false personas
  - They can falsely use real personas
  - They can change personas frequently
  - They can operate as part of a larger organization

Why use Computers or Electronic Devices to Commit Crimes?

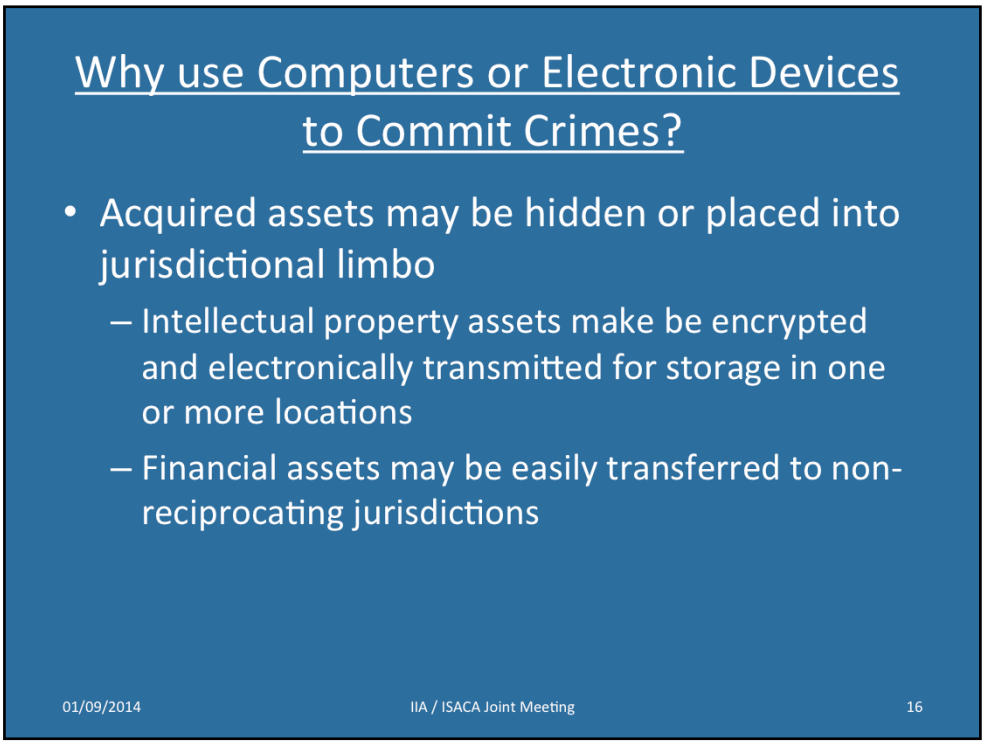
- The perpetrators or criminals can choose the jurisdictional venue to operate from
  - They can operate from countries such as Romania and Latvia that have very different laws regarding cybercrime
  - They can more easily coordinate with partners in other jurisdictions
  - They can "virtually" re-locate from one jurisdiction to another

Why use Computers or Electronic Devices to Commit Crimes?

- The means to commit the crime can remain hidden or obscured
  - The tools to commit the crime can be hidden malware, rogue websites, or even armies of volunteers dispersed in cyberspace
  - The criminal activity can be buried under a blanket of legitimate activity
  - The electronic "footprint" of the activity can be erased as the last step in the crime

Why use Computers or Electronic Devices to Commit Crimes?

- Evidence regarding the crime may be more difficult to identify, collect and attribute
  - The evidence may be dispersed across multiple computer systems in multiple locations (possibly numbering in the millions)
  - The cataloguing of the information with proper chains of custody may be very labor intensive
  - Attributing a specific piece of electronic evidence to a specific perpetrator may be very difficult



Cloud storage providers are available world-wide at dirt cheap prices – many with the first few gigabytes free.

1.Amazon Cloud Drive – 5GB
2.DropBox – 2GB
3.SugarSync – 5GB
4.MegaCloud – 8GB
5.Google Drive – 5GB
6.Microsoft SkyDrive – 7GB
7.JustCloud – Unlimited
8.Box – 5GB

Note: More and more jurisdictions are agreeing to report out financial asset transactions and holdings to other countries. "Caymans Sign Up To British FATCA" (http://www.iexpats.com/caymans-sign-british-fatca/). FATCA refers to the US Foreign Account Tax Compliance Act, which comes into force in 2014.

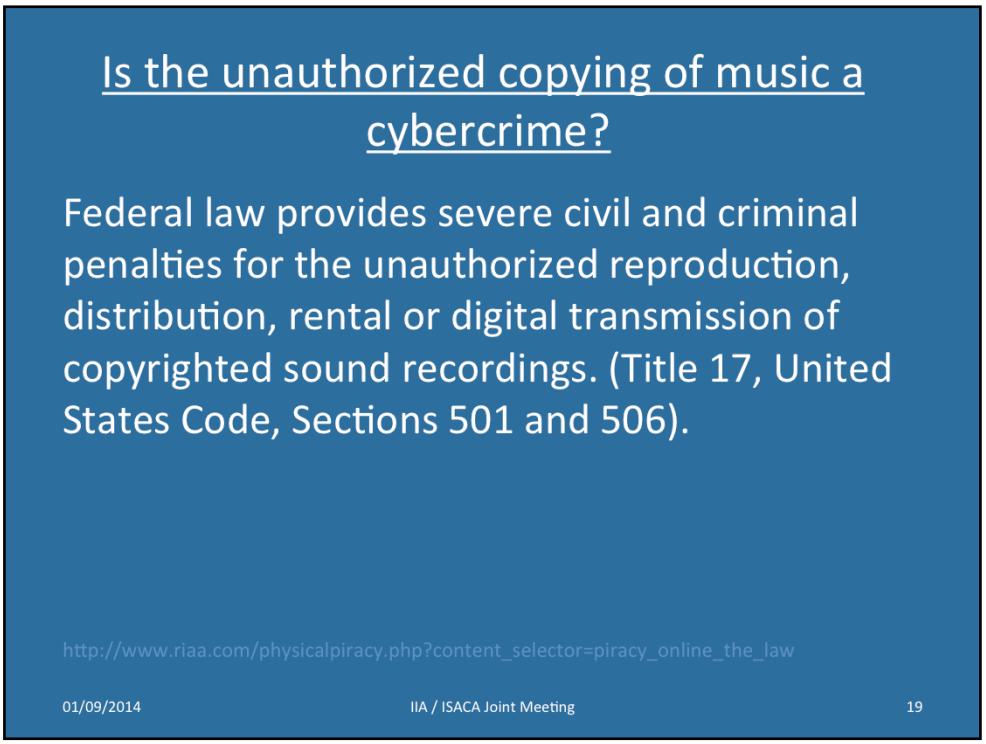
Means, Motive and Opportunity

- **Means**—the tools are there, nicely catalogued and ready to go.
- **Motives**—with so much on the Internet, motives are there.
- **Opportunity**—there are many, many access points to the Internet. Most are inexpensive, some are free (your local library).

Cybersleuthing: Means, Motive, and Opportunity
http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitysum00.cfm

The Blurry Line of Cybercrime

- Is the unauthorized copying of music a cybercrime?
- Is a crank call a cybercrime? What if it uses a service to hide the caller's identity?
- When does an unflattering text message become cyber-bullying?
- Is forging a fake invoice using a computer a cybercrime or just fraud?



17 USC § 501 - Infringement of copyright

(a) Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 122 or of the author as provided in section 106A (a), or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright or right of the author, as the case may be. For purposes of this chapter (other than section 506), any reference to copyright shall be deemed to include the rights conferred by section 106A (a). As used in this subsection, the term "anyone" includes any State, any instrumentality of a State, and any officer or employee of a State or instrumentality of a State acting in his or her official capacity. Any State, and any such instrumentality, officer, or employee, shall be subject to the provisions of this title in the same manner and to the same extent as any nongovernmental entity. (http://www.law.cornell.edu/uscode/text/17/501)

Is a crank call a cybercrime? What if it uses a service to hide the caller's identity?

Spoofing Calls and Texts

http://covertcalling.com/demo.php

01/09/2014 IIA / ISACA Joint Meeting 20

http://www.fcc.gov/guides/caller-id-and-spoofing

Truth in Caller ID Act of 2009

The Truth in Caller ID Act of 2009, which was signed into law Dec. 22, 2010, **prohibits caller ID spoofing for the purposes of defrauding or otherwise causing harm.** In June 2010, the Federal Communications Commission adopted rules implementing the Truth in Caller ID Act.

FCC Rules

- Prohibit any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value.
- Subject violators to a penalty of up to $10,000 for each violation of the rules.
- Exempt authorized activities by law enforcement agencies and situations where courts have authorized caller ID manipulation to occur.

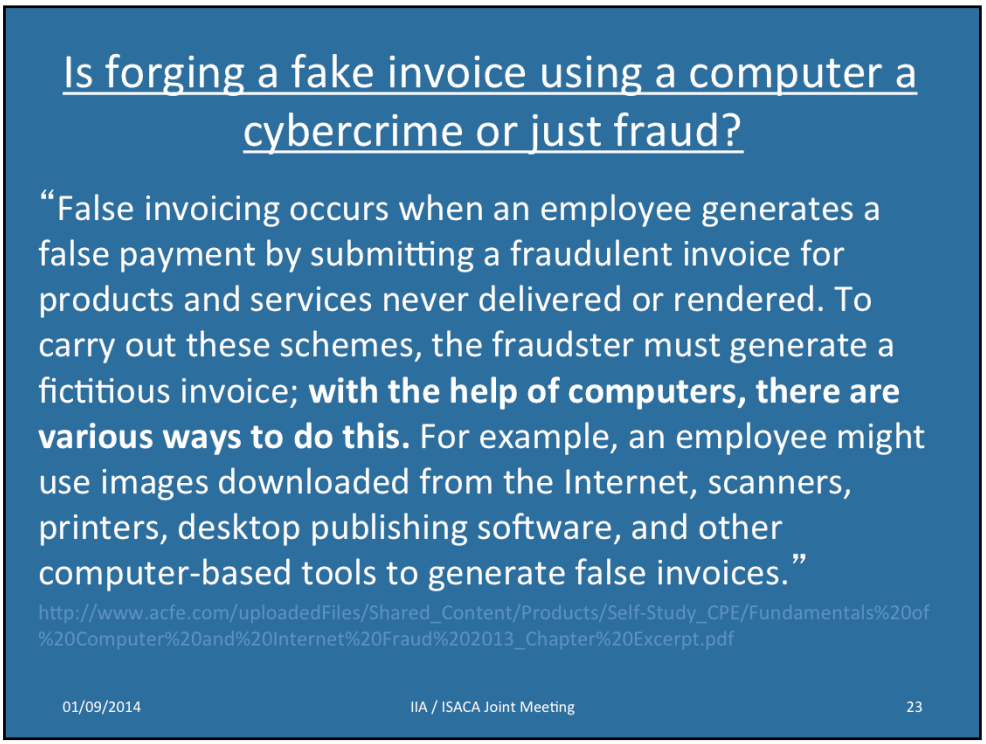
When does an unflattering text message become cyber-bullying?

The National Crime Prevention Council defines cyber-bullying as "the process of using the internet, cell phones or other devices to send or post text or images intended to hurt or **embarrass another person**."

When does an unflattering text message become cyber-bullying?

In 2011, approximately 9 percent of students ages 12–18 reported being cyber-bullied anywhere during the school year. Of those students, about 4 percent each reported that another student had posted hurtful information on the Internet and reported being the subject of harassing text messages.

Bureau of Justice Statistics report: Indicators of School Crime and Safety - 2012 (June 2013) - http://www.bjs.gov/content/pub/pdf/iscs12.pdf



Association of Certified Fraud Examiners (ACFE)

Issues the Certified Fraud Examiner (CFE) certification

The Top 5 Frauds of 2013 - http://www.acfeinsights.com/acfe-insights/2013/12/23/the-top-5-frauds-of-2013.html

ACFE Case Studies - http://www.acfe.com/case-studies.aspx

Encyclopedia of Cybercrime

Proliferation of computing and networked devices throughout the world, including computers, PDAs, and cellular phones is among the most profound technological changes in human history. Increasing capacity of information technologies (IT) to transform ways we work and function as a society is unprecedented. However, any technological advancement provides potential avenues for abuse and harm. Behaving in ways that are uncommon or unacceptable within a particular cultural setting may be considered deviant. When deviant acts rise to a level of causing harm, they are considered to be against the law (i.e., criminalized). ''Cybercrime'' is a broad term covering all the ways in which computers and other types of portable electronic devices such as cell phones and PDAs capable of connecting to the Internet are used to break laws and cause harm. A slightly more technical definition would be ''use of computers or other electronic devices via information systems such as organizational networks or the Internet to facilitate illegal behaviors'' (McQuade, 2006, p. 16).

ENCYCLOPEDIA OF CYBERCRIME, Greenwood Press, 2009, Edited by Samuel C. McQuade, III

Cyber Extortion – Extortion by computer and internet

The cliché, "the more things change the more they stay the same" applies to the new era of extortion. The traditional crime of extortion is defined as an attempt to threaten a person or entity into giving up something in exchange for not being harmed in some way. Cyber extortion merely modernizes this crime by using the Internet and computers to carry out a wide variety of threats.

http://www.acfe.com/article.aspx?id=4294967630

Cyberstalking and Cyberharassment

Cyberstalking is the use of the Internet, email or other electronic communications to stalk, and generally refers to a pattern of threatening or malicious behaviors.

Cyberharassment differs from cyberstalking in that it may generally be defined as not involving a credible threat. Cyberharassment usually pertains to threatening or harassing email messages, instant messages, or to blog entries or websites dedicated solely to tormenting an individual.

http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx

Cyber + (Name your Crime)

The National Computer Security Survey (NCSS) documents the nature, prevalence, and impact of cyber intrusions against businesses in the United States. It examines three general types of cybercrime:

1) Cyber attacks are crimes in which the computer system is the target. Cyber attacks consist of computer viruses (including worms and Trojan horses), denial of service attacks, and electronic vandalism or sabotage.

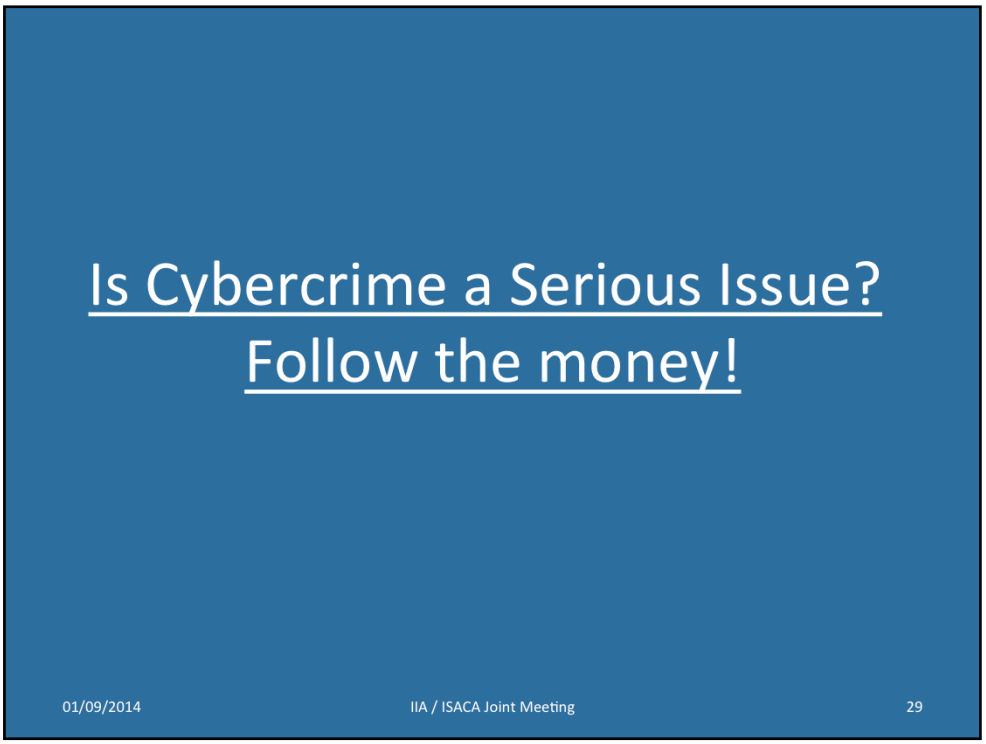
http://www.bjs.gov/index.cfm?ty=tp&tid=41

Cyber + (Name your Crime) (cont.)

2) Cyber theft comprises crimes in which a computer is used to steal money or other things of value. Cyber theft includes embezzlement, fraud, theft of intellectual property, and theft of personal or financial data.

3) Other computer security incidents encompass spyware, adware, hacking, phishing, spoofing, pinging, port scanning, and theft of other information, regardless of whether the breach was successful.

http://www.bjs.gov/index.cfm?ty=tp&tid=41


Is Cybercrime a Serious Issue?
Follow the money!
01/09/2014
IIA / ISACA Joint Meeting
29

Big Bucks are Being Spent on Law Enforcement to Address Cybercrime

Many agencies are involved with combatting cybercrime:

- Federal Bureau of Investigation (FBI)
- US Secret Service (USSS)
- Internet Crime Complaint Center (IC3)
- National White Collar Crime Center (NW3C)
- And more…

FBI Budget Request for Fiscal Year 2014

The FBI's fiscal year (FY) 2014 budget request totals $8.4 billion in direct budget authority, including 34,787 permanent positions (13,082 special agents, 3,026 intelligence analysts, and 18,679 professional staff). This funding level provides critical funding to address threats posed by terrorists, cyber attackers, and criminals.

http://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2014

FBI Budget Request for Fiscal Year 2014

As this committee knows, the cyber arena has significantly changed over the last decade. **Cyber attacks and crimes are becoming more commonplace, more sophisticated, and more dangerous.** The scope and targets of these attacks and crimes encompass the full range and scope of the FBI's criminal investigative and national security missions. **Traditional crime, from mortgage and health care fraud to child exploitation, has migrated online**.

FBI Budget Request for Fiscal Year 2014

There is always more work to be done, but we have had some success, including the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme. **The Rove Digital scheme infected more than four million computers located in more than 100 countries with malware.** The malware secretly altered the settings on infected computers, enabling the hackers to digitally hijack Internet searches using rogue servers for Domain Name System (DNS) routers and **re-routing computers to certain websites and ads.**

FBI Budget Request for Fiscal Year 2014

We have also worked against infrastructure we believe has been used in distributed denial of service (DDoS) attacks, preventing it from being used for future attacks. **Since October, the FBI and DHS have released nearly 168,000 Internet Protocol (IP) addresses determined to be infected with DDoS malware.** We have released this information through joint indicator bulletins (JIBs) to 129 countries. Both the DHS' Computer Emergency Readiness Team and FBI's legal attachés released JIBs to our foreign partners. These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDoS attacks.

FBI Budget Request for Fiscal Year 2014

U.S. law enforcement and intelligence communities, along with our international and private sector partners, are making progress. Technological advancements and the Internet's expansion continue to provide malicious cyber actors the opportunity to harm U.S. national security and the economy. Given the consequences of such attacks, the FBI must be able to keep pace with this rapidly developing and diverse threat. Because of this, **the FY 2014 budget request includes an additional 152 positions (60 special agents, one intelligence analyst, and 91 professional staff) and $86.6 million to help address this threat.**

FBI's Cyber's Most Wanted

http://www.fbi.gov/wanted/cyber

United States Secret Sevice

In their 5 year strategic plan the US Secret Service stated: As a result of technological advancements, electronic and financial crimes transcend national borders more fluidly than ever before. A June 2005 round table discussion by the Payments System Development Committee of the Federal Reserve System stated that:

"…the difficulties in investigating and prosecuting Internet fraud cases are often exacerbated in international cases because, at times, the necessary cooperation with…

United States Secret Sevice

…foreign law enforcement agencies adds additional complexity to an investigation. **This is a growing concern because of the international scale of the Internet and increasing amounts of fraud that originate outside of the United States**."

"Strategic Objective 1.2: Reduce the amount of financial losses resulting from electronic crimes, financial crimes, computer crimes, compromised payment systems, identity theft and other types of financial crimes."

http://www.secretservice.gov/usss_strategic_plan_2008_2013.pdf

Internet Crime Complaint Center (IC3)

The IC3 was established as a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to serve as a means to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate. The IC3 was intended, and continues to emphasize, serving the broader law enforcement community to include federal, as well as state, local, and international agencies, which are combating Internet crime and, in many cases, participating in Cyber Crime Task Forces.

http://www.ic3.gov/default.aspx

Internet Crime Complaint Center (IC3)

Now in its 12th year, IC3 continues to serve as the largest single repository for Internet-related complaints. IC3 also conducts research and compiles criminal activity information for referrals to law enforcement agencies. In 2012, consumers filed 289,875 complaints detailing a variety of scams and frauds for a total adjusted dollar loss of $522 million[1]. On average, consumers who reported a financial loss were defrauded $4,543.

[1]FBI IC3 Unit staff reviewed for validity all complaints that reported a loss of more than $100,000. FBI Analysts also converted losses reported in foreign currencies to dollars. The final amounts of all reported losses above $100,000 for which the complaint information did not support the loss amount were excluded from the statistics.

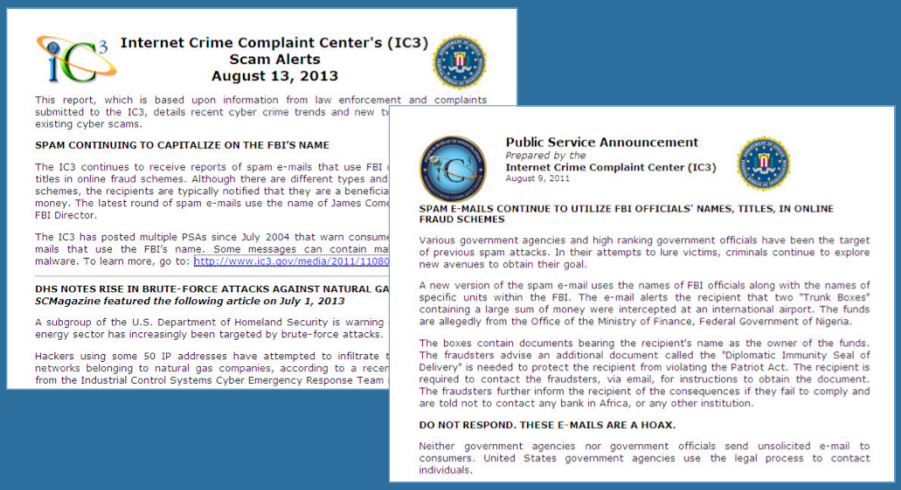
IC3 2012 Statistics
Top Five[1] Reported Crime Types

Rank/Crime Type

1. FBI Impersonation Scams – 28,130
2. Identity Theft – 26,131
3. Advance Fee Fraud – 21,133
4. Non-Auction – Non-Delivery of Merchandise – 20,090
5. SPAM (Misc.) – 19,454

[1]Complaint category statistics based on the perceptions of complainants are not typically accurate for statistical purposes. The statistics pulled from the complaints themselves are more accurate as they are categorized and grouped through the IC3 automated system. IC3 does not verify complaint data.

Internet Crime Complaint Center



Internet Crime Complaint Center's (IC3) Scam Alerts
August 13, 2013

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new t existing cyber scams.

SPAM CONTINUING TO CAPITALIZE ON THE FBI'S NAME

The IC3 continues to receive reports of spam e-mails that use FBI titles in online fraud schemes. Although there are different types and schemes, the recipients are typically notified that they are a beneficia money. The latest round of spam e-mails use the name of James Com FBI Director.

The IC3 has posted multiple PSAs since July 2004 that warn consume mails that use the FBI's name. Some messages can contain ma malware. To learn more, go to: http://www.ic3.gov/media/2011/11080

DHS NOTES RISE IN BRUTE-FORCE ATTACKS AGAINST NATURAL GA
SCMagazine featured the following article on July 1, 2013

A subgroup of the U.S. Department of Homeland Security is warning energy sector has increasingly been targeted by brute-force attacks.

Hackers using some 50 IP addresses have attempted to infiltrate t networks belonging to natural gas companies, according to a recer from the Industrial Control Systems Cyber Emergency Response Team

Public Service Announcement
Prepared by the
Internet Crime Complaint Center (IC3)
August 9, 2011

SPAM E-MAILS CONTINUE TO UTILIZE FBI OFFICIALS' NAMES, TITLES, IN ONLINE FRAUD SCHEMES

Various government agencies and high ranking government officials have been the target of previous spam attacks. In their attempts to lure victims, criminals continue to explore new avenues to obtain their goal.

A new version of the spam e-mail uses the names of FBI officials along with the names of specific units within the FBI. The e-mail alerts the recipient that two "Trunk Boxes" containing a large sum of money were intercepted at an international airport. The funds are allegedly from the Office of the Ministry of Finance, Federal Government of Nigeria.

The boxes contain documents bearing the recipient's name as the owner of the funds. The fraudsters advise an additional document called the "Diplomatic Immunity Seal of Delivery" is needed to protect the recipient from violating the Patriot Act. The recipient is required to contact the fraudsters, via email, for instructions to obtain the document. The fraudsters further inform the recipient of the consequences if they fail to comply and are told not to contact any bank in Africa, or any other institution.

DO NOT RESPOND. THESE E-MAILS ARE A HOAX.

Neither government agencies nor government officials send unsolicited e-mail to consumers. United States government agencies use the legal process to contact individuals.

http://www.ic3.gov/media/2013/130813.aspx

National White Collar Crime Center (NW3C)

In July 2012, NW3C announced a strategic partnership with X1 Discovery, Inc. to provide support and training for Internet and social media investigations. X1 produces and sells X1 Social Discovery, an industry-leading software product that serves as an investigative tool for forensically gathering evidence from social media sites. The X1 product is designed to help combat child exploitation, financial fraud, drug trafficking and other **illegal activities involving the direct or indirect use of social media and the Internet.**

Scotland Yard

Scotland Yard cyber crime unit to dramatically expand

The Metropolitan Police is planning a major expansion of its E-crime unit as the threat of a cyber attack continues to grow

Scotland Yard cyber crime unit to expand. Photo: Alamy

By Martin Evans, Crime Correspondent
7:00AM GMT 09 Nov 2013

Follow 2,480 followers

Scotland Yard is to dramatically expand its specialist E-Crime unit which could see 500 dedicated officers drafted in to tackle the ever growing problem of cyber attacks and internet fraud, the Daily Telegraph can disclose.

With MPs warning that cybercrime is now a Tier One threat to the country – on a par with international terrorism – resources are to be directed away from more traditional crime fighting areas to the specialist unit.

113 Facebook 21 Twitter 92 Email LinkedIn 0 8+1 0

Crime

"With MPs warning that cybercrime is now a Tier One threat to the country – on a par with international terrorism…"

01/09/2014 IIA / ISACA Joint Meeting 44

Not just the US but foreign governments are shifting their focus and resources to cybercrime.

What types of cybercrime are most prevalent?

Target breach:

40 million credit and debit cards were stolen – even though stolen PIN codes were encrypted note that you can crack more than 10 percent of random PINs by dialing in 1234. Expanding a bit, 1234, 0000, and 1111, make up about 20 percent.

See http://www.popsci.com/technology/article/2012-09/infographic-day-fastest-way-crack-4-digit-pin-number

Affordable Care Act (Obamacare) fraud:

Some Obamacare navigators—taxpayer-funded workers who were meant to help Americans wade through the insurance exchanges and buy health insurance—have been giving Americans misinformation and in some instances encouraging Americans to commit fraud, according to a House Oversight and Government Reform Committee that was released today.

See http://blog.heritage.org/2013/12/16/obamacare-navigators-encourage-fraud-safe-private-information-report-warns/

Internet Crime Schemes

10. Internet Extortion
11. Investment Fraud
12. Lotteries
13. Nigerian Letter or "419"
14. Phishing/Spoofing
15. Ponzi/Pyramid
16. Reshipping
17. Spam
18. Third Party Receiver of Funds

http://www.ic3.gov/crimeschemes.aspx

Auction Fraud

Auction fraud involves fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Consumers are strongly cautioned against entering into Internet transactions with subjects exhibiting the following behavior:

- The seller posts the auction as if he resides in the United States, then responds to victims with a congratulatory email stating he is outside the United States for business reasons, family emergency, etc.
- Similarly, beware of sellers who post the auction under one name, and ask for the funds to be transferred to another individual.

Auction Fraud (cont.)

- The subject requests funds to be wired directly to him/her via Western Union, MoneyGram, or bank-to-bank wire transfer. By using these services, the money is virtually unrecoverable with no recourse for the victim.
- Sellers acting as authorized dealers or factory representatives in countries where there would be no such dealers should be avoided.
- Buyers who ask for the purchase to be shipped using a certain method to avoid customs or taxes inside another country should be avoided.
- Be suspect of any credit card purchases where the address of the card holder does not match the shipping address. Always receive the card holder's authorization before shipping any products.

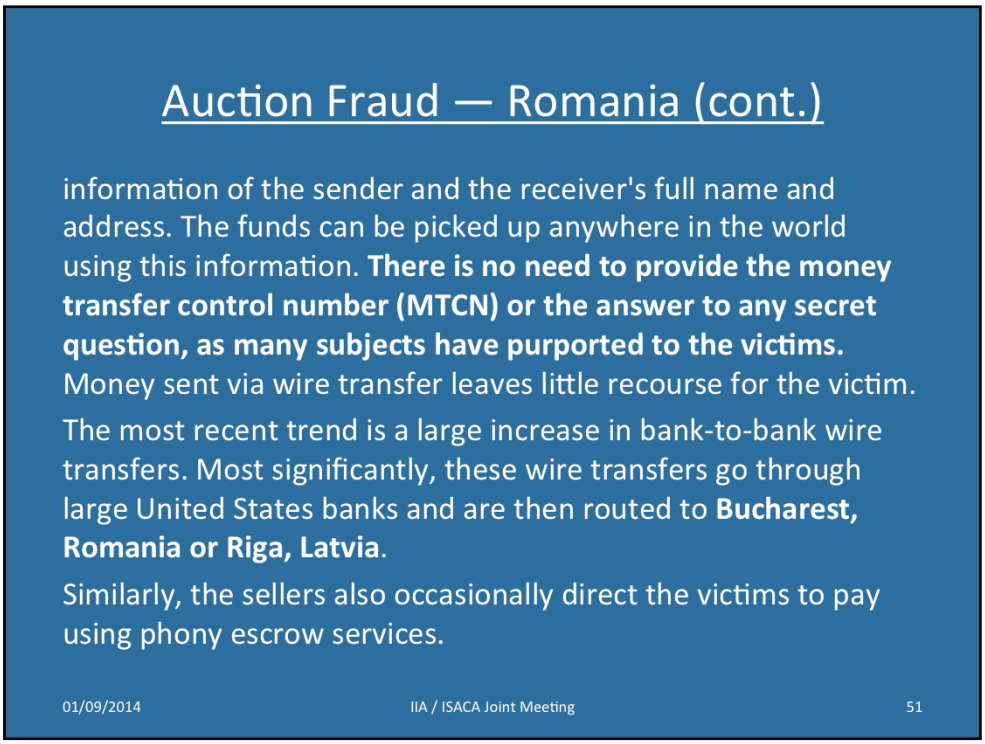
Tips for avoiding Auction fraud:

1. Before you bid, contact the seller with any questions you have.
2. Review the seller's feedback.
3. Be cautious when dealing with individuals outside of your own country.
4. Ensure you understand refund, return, and warranty policies.
5. Determine the shipping charges before you buy.
6. Be wary if the seller only accepts wire transfers or cash.
7. If an escrow service is used, ensure it is legitimate.
8. Consider insuring your item.
9. Be cautious of unsolicited offers.

Auction Fraud — Romania

Auction fraud is the most prevalent of Internet crimes associated with Romania. The subjects have saturated the Internet auctions and offer almost every in-demand product. The subjects have also become more flexible, allowing victims to send half the funds now, and the other half when the item arrives.

The auctions are often posted as if the seller is a United States citizen, then the subject advises the victim to send the money to a business partner, associate, sick relative, a family member, etc., usually in a European country. The money is usually transferred via MoneyGram or Western Union wire transfer. The Internet Crime Complaint Center has verified in order to receive funds via Western Union, the receiver must provide the complete



Wire transfer never-evers!

http://www.westernunion.com/sites/us/consumer-protection/KnowledgeCenter.page

Lower your chances of falling victim to fraud by checking out these eight things you should never do when using a money transfer service.

1.Never send money to people you haven't met in-person.

2.Never send money to pay for taxes or fees on lottery or prize winnings.

3.Never use a test question as an additional security measure to protect your transaction.

4.Never provide your banking information to people or businesses you don't know.

5.Never send money in advance to obtain a loan or credit card.

6.Never send money for an emergency situation without verifying that it's a real emergency.

7.Never send funds from a check in your account until it officially clears—which can take weeks.

8.Never send a money transfer for online purchases.

Counterfeit Cashier's Check

The counterfeit cashier's check scheme targets individuals that use Internet classified advertisements to sell merchandise. Typically, an interested party located outside the United States contacts a seller. The seller is told that the buyer has an associate in the United States that owes him money. As such, he will have the associate send the seller a cashier's check for the amount owed to the buyer.

The amount of the cashier's check will be thousands of dollars more than the price of the merchandise and the seller is told the excess amount will be used to pay the shipping costs associated with getting the merchandise to his location. The seller is instructed to deposit the check, and as soon as it clears, to wire the excess funds back to the buyer or to another associate

Counterfeit Cashier's Check (cont.)

identified as a shipping agent. In most instances, the money is sent to locations in West Africa (Nigeria).

Because a cashier's check is used, a bank will typically release the funds immediately, or after a one or two day hold. Falsely believing the check has cleared, the seller wires the money as instructed.

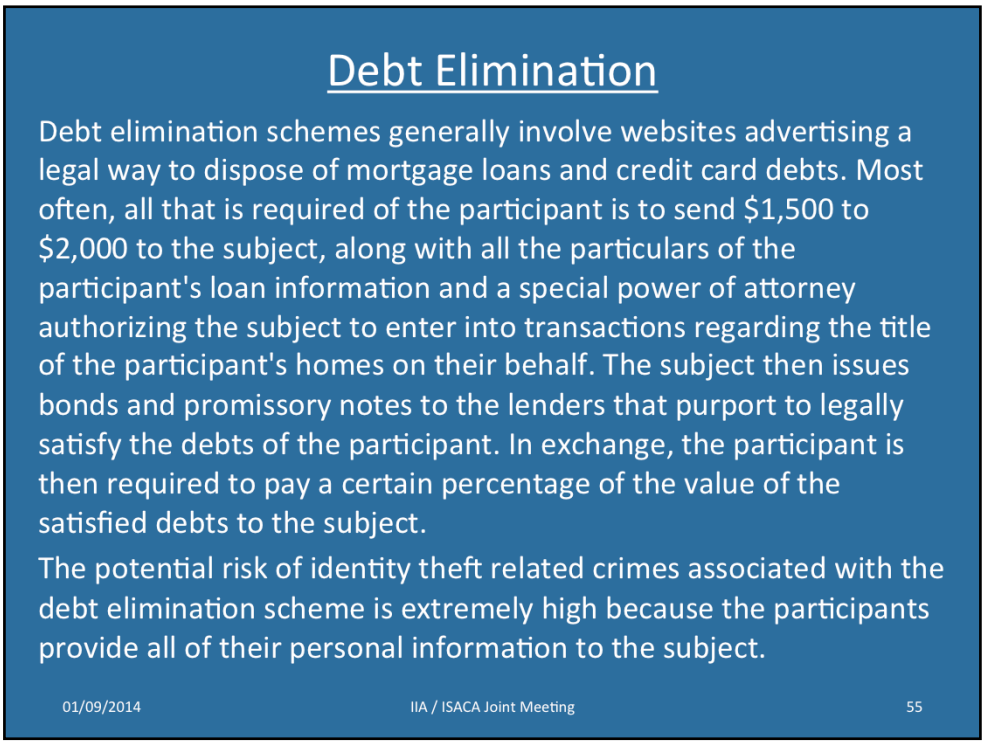
In some cases, the buyer is able to convince the seller that some circumstance has arisen that necessitates the cancellation of the sale, and is successful in conning the victim into sending the remainder of the money. Shortly thereafter, the victim's bank notifies him that the check was fraudulent, and the bank is holding the victim responsible for the full amount of the check.

Tips for avoiding Counterfeit Cashier's Check fraud:

1. Inspect the cashier's check.
2. Ensure the amount of the check matches in figures and words.
3. Check to see that the account number is not shiny in appearance.
4. Be watchful that the drawer's signature is not traced.
5. Official checks are generally perforated on at least one side.
6. Inspect the check for additions, deletions, or other alterations.
7. Contact the financial institution on which the check was drawn to ensure legitimacy.
8. Obtain the bank's telephone number from a reliable source, not from the check itself.
9. Be cautious when dealing with individuals outside of your own country.

Tips for avoiding Credit Card fraud:

1. Ensure a site is secure and reputable before providing your credit card number online.
2. Don't trust a site just because it claims to be secure.
3. If purchasing merchandise, ensure it is from a reputable source.
4. Promptly reconcile credit card statements to avoid unauthorized charges.
5. Do your research to ensure legitimacy of the individual or company.
6. Beware of providing credit card information when requested through unsolicited emails.



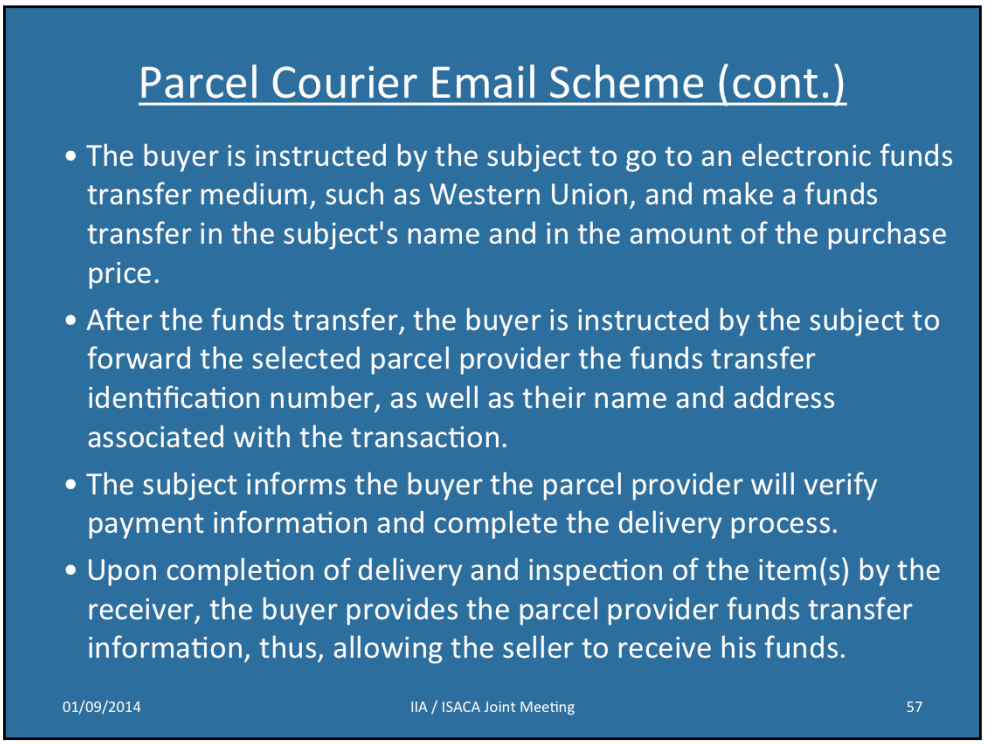
Tips for avoiding Debt Elimination fraud:

1.Know who you are doing business with — do your research.
2.Obtain the name, address, and telephone number of the individual or company.
3.Research the individual or company to ensure they are authentic.
4.Contact the Better Business Bureau to determine the legitimacy of the company.
5.Be cautious when dealing with individuals outside of your own country.
6.Ensure you understand all terms and conditions of any agreement.
7.Be wary of businesses that operate from P.O. boxes or mail drops.
8.Ask for names of other customers of the individual or company and contact them.
9.If it sounds too good to be true, it probably is.

Parcel Courier Email Scheme

The Parcel Courier Email Scheme involves the supposed use of various National and International level parcel providers such as DHL, UPS, FedEx and the USPS. Often, the victim is directly emailed by the subject(s) following online bidding on auction sites. Most of the scams follow a general pattern which includes the following elements:

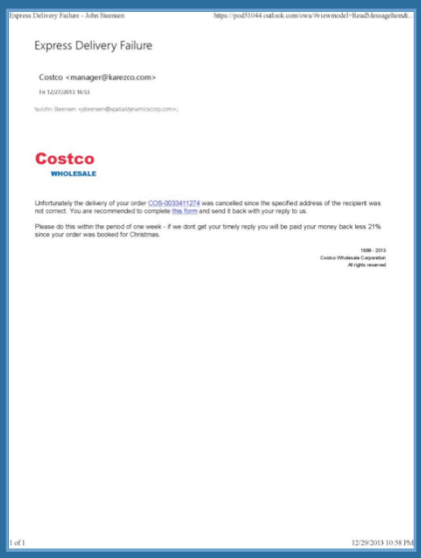
- The subject instructs the buyer to provide shipping information such as name and address.
- The subject informs the buyer that the item will be available at the selected parcel provider in the buyer's name and address, thereby, identifying the intended receiver.
- The selected parcel provider checks the item and purchase documents to guarantee everything is in order.
- The selected parcel provider sends the buyer delivery notification verifying their receipt of the item.



Tips for avoiding Parcel Courier fraud:

1. Beware of individuals using the DHL or UPS logo in any email communication.
2. Be suspicious when payment is requested by money transfer before the goods will be delivered.
3. Remember that DHL and UPS do not generally get involved in directly collecting payment from customers.
4. Fees associated with DHL or UPS transactions are only for shipping costs and never for other costs associated with online transactions.
5. Contact DHL or UPS to confirm the authenticity of email communications received.

Delivery Phishing



Employment/Business Opportunities

Employment/business opportunity schemes have surfaced wherein bogus foreign-based companies are recruiting citizens in the United States on several employment-search websites for work-at-home employment opportunities. These positions often involve reselling or reshipping merchandise to destinations outside the United States.

Prospective employees are required to provide personal information, as well as copies of their identification, such as a driver's license, birth certificate, or social security card. Those employees that are "hired" by these companies are then told that their salary will be paid by check from a United States company reported to be a creditor of the employer. This is done under the pretense that the employer does not have any banking set up in the United States.

Employment/Business Opportunities (cont.)

The amount of the check is significantly more than the employee is owed for salary and expenses, and the employee is instructed to deposit the check into their own account, and then wire the overpayment back to the employer's bank, usually located in Eastern Europe. The checks are later found to be fraudulent, often after the wire transfer has taken place.

In a similar scam, some web-based international companies are advertising for affiliate opportunities, offering individuals the chance to sell high-end electronic items, such as plasma television sets and home theater systems, at significantly reduced prices.

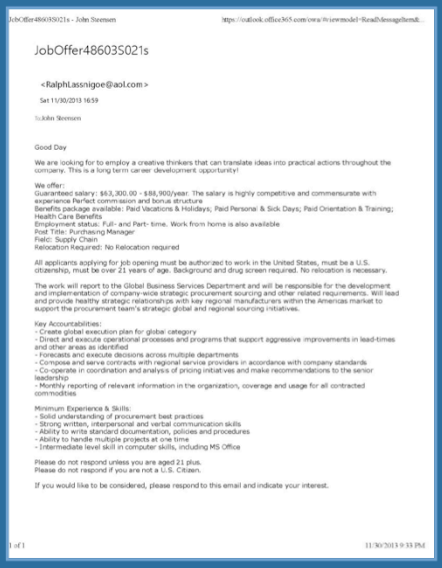
Employment/Business Opportunities (cont.)

The affiliates are instructed to offer the merchandise on well-known Internet auction sites. The affiliates will accept the payments, and pay the company, typically by means of wire transfer. The company is then supposed to drop-ship the merchandise directly to the buyer, thus eliminating the need for the affiliate to stock or warehouse merchandise. The merchandise never ships, which often prompts the buyers to take legal action against the affiliates, who in essence are victims themselves.

Tips for avoiding Employment/Business Opportunities fraud:

1. Be wary of inflated claims of product effectiveness.
2. Be cautious of exaggerated claims of possible earnings or profits.
3. Beware when money is required up front for instructions or products.
4. Be leery when the job posting claims "no experience necessary".
5. Do not give your social security number when first interacting with your prospective employer.
6. Be cautious when dealing with individuals outside of your own country.
7. Be wary when replying to unsolicited emails for work-at-home employment.
8. Research the company to ensure they are authentic.
9. Contact the Better Business Bureau to determine the legitimacy of the company.

Fake Job email



JobOffer48603S021s - John Steensen https://outlook.office365.com/owa/#viewmodel=ReadMessageItemM...

JobOffer48603S021s

<RalphLassnigoe@aol.com>

Sat 11/30/2013 16:59

To John Steensen

Good Day

We are looking for to employ a creative thinkers that can translate ideas into practical actions throughout the company. This is a long term career development opportunity!

We offer:
Guaranteed salary: $63,300.00 - $88,900/year. The salary is highly competitive and commensurate with experience Perfect commission and bonus structure
Benefits package available: Paid Vacations & Holidays; Paid Personal & Sick Days; Paid Orientation & Training; Health Care Benefits
Employment status: Full- and Part- time. Work from home is also available
Post Title: Purchasing Manager
Field: Supply Chain
Relocation Required: No Relocation required

All applicants applying for job opening must be authorized to work in the United States, must be a U.S. citizenship, must be over 21 years of age. Background and drug screen required. No relocation is necessary.

The work will report to the Global Business Services Department and will be responsible for the development and implementation of company-wide strategic procurement sourcing and other related requirements. Will lead and provide healthy strategic relationships with key regional manufacturers within the Americas market to support the procurement team's strategic global and regional sourcing initiatives.

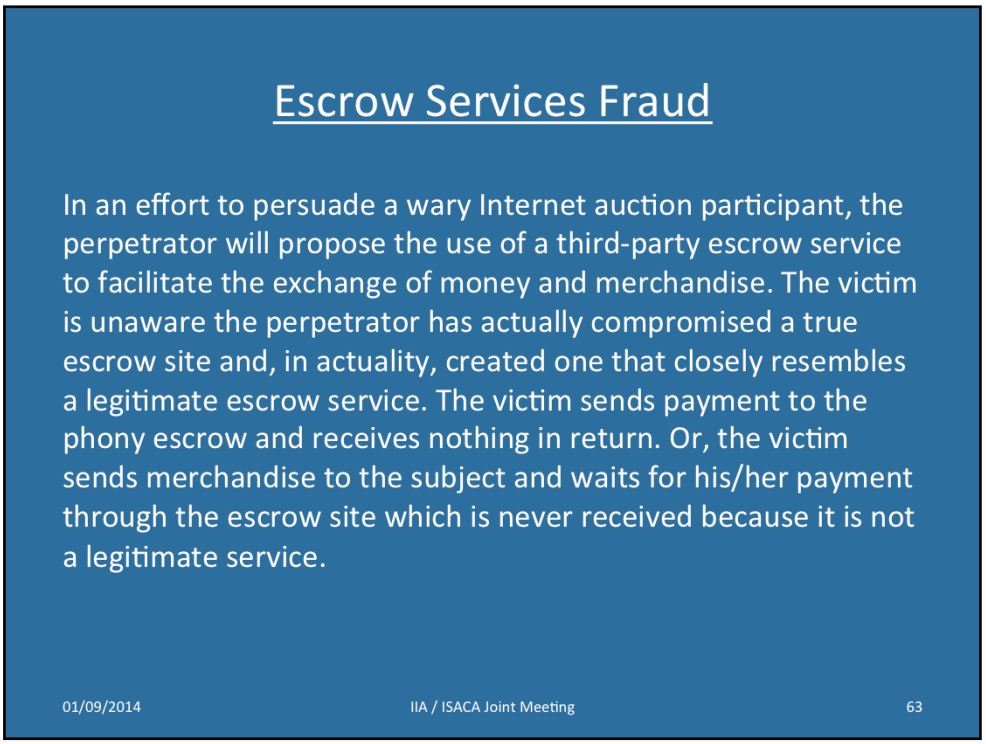
Key Accountabilities:
- Create global execution plan for global category
- Direct and execute operational processes and programs that support aggressive improvements in lead-times and other areas as identified
- Forecasts and execute decisions across multiple departments
- Compose and serve contracts with regional service providers in accordance with company standards
- Co-operate in coordination and analysis of pricing initiatives and make recommendations to the senior leadership
- Monthly reporting of relevant information in the organization, coverage and usage for all contracted commodities

Minimum Experience & Skills:
- Solid understanding of procurement best practices
- Strong written, interpersonal and verbal communication skills
- Ability to write standard documentation, policies and procedures
- Ability to handle multiple projects at one time
- Intermediate level skill in computer skills, including MS Office

Please do not respond unless you are aged 21 plus.
Please do not respond if you are not a U.S. Citizen.

If you would like to be considered, please respond to this email and indicate your interest.

1 of 1 11/30/2013 9:33 PM



Tips for avoiding Escrow Services fraud:

1. Always type in the website address yourself rather than clicking on a link provided.
2. A legitimate website will be unique and will not duplicate the work of other companies.
3. Be cautious when a site requests payment to an "agent", instead of a corporate entity.
4. Be leery of escrow sites that only accept wire transfers or e-currency.
5. Be watchful of spelling errors, grammar problems, or inconsistent information.
6. Beware of sites that have escrow fees that are unreasonably low.

Identity Theft

Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business, sometimes as a response to an email solicitation to update billing or membership information, or as an application to a fraudulent Internet job posting.

In yesterday's (01/08/2014) Wall Street Journal an article quoted the IRS as saying "Identify Theft Grew Sharply Last Year."

Tips for avoiding Identity Theft:

1.Ensure websites are secure prior to submitting your credit card number.

2.Do your homework to ensure the business or website is legitimate.

3.Attempt to obtain a physical address, rather than a P.O. box or mail drop.

4.Never throw away credit card or bank statements in usable form.

5.Be aware of missed bills which could indicate your account has been taken over.

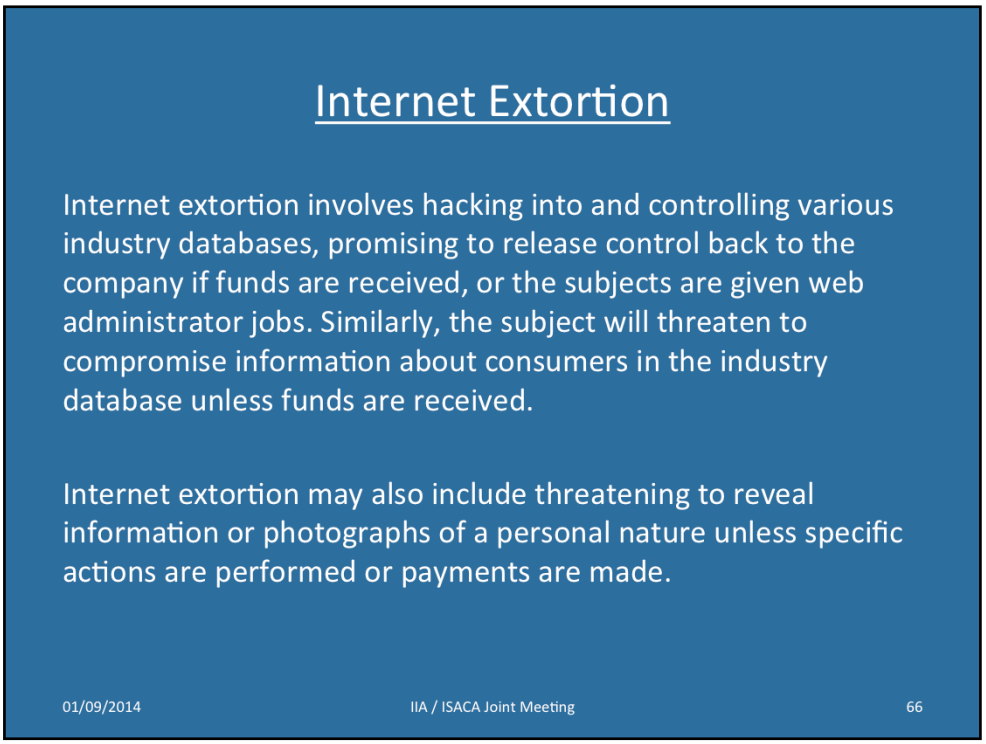
6.Be cautious of scams requiring you to provide your personal information.

7.Never give your credit card number over the phone unless you make the call.

8.Monitor your credit statements monthly for any fraudulent activity.

9.Report unauthorized transactions to your bank or credit card company as soon as possible.

10.Review a copy of your credit report at least once a year.



Tips for avoiding Internet Extortion:

1. Security needs to be multi-layered so that numerous obstacles will be in the way of the intruder.
2. Ensure security is installed at every possible entry point.
3. Identify all machines connected to the Internet and assess the defense that's engaged.
4. Identify whether your servers are utilizing any ports that have been known to represent insecurities.
5. Ensure you are utilizing the most up-to-date patches for your software.

Internet Extortion

Man in beauty pageant extortion case posts bail

Updated: Sep 26, 2013 8:31 PM PDT

SANTA ANA, Calif. (AP) - A 19-year-old man was charged Thursday with hacking webcams at the home of Miss Teen USA Cassidy Wolf and other women to extort nude photos and videos from them, with authorities contending he forced several women to strip.

Jared James Abrahams of Temecula surrendered to agents at the FBI office in Orange County to face a charge of extortion that could send him to federal prison for up to two years, FBI spokeswoman Laura Eimiller said.

He was later freed on $50,000 bail but a judge confined him to his family home, ordered him to wear a GPS monitor, and said he could only use the home computer for schoolwork, with software to be installed that will monitor its use.

Authorities said Abrahams knew Wolf, a 19-year-old graduate of Great Oak High School in Temecula who won the Miss Teen USA crown Aug. 9. She is identified only by her initials in the criminal complaint.

Last month, Wolf told the website of NBC's "Today" show that earlier this year she received an anonymous email in which the sender claimed to have stolen images from the camera on her home computer.

The sender of the email threatened to go public with images captured from Wolf's webcam unless she would provide nude pictures of herself, Eimiller said - a crime commonly known as "sextortion."

Instead, Wolf went to authorities, and an investigation was launched in March.

A federal complaint filed on Sept. 17 and unsealed Thursday charges him with extortion but Eimiller said other charges are possible.

In this file photo, Cassidy Wolf is crowned Miss Teen USA, 2013 (AP Photo/Miss Universe L.P., LLLP, File)

More Local News more»

Thibodaux man arrested for firing gun at vehicle
Incident occurred Sunday around 9:00 p.m.
more>>

Pair wanted for Gentilly armed robbery
Incident occurred Saturday around 5:20 p.m.
more>>

http://www.fox8live.com/story/23543986/man-in-beauty-pageant-extortion-case-posts-bail

Tips for avoiding Internet Extortion:

1. Security needs to be multi-layered so that numerous obstacles will be in the way of the intruder.
2. Ensure security is installed at every possible entry point.
3. Identify all machines connected to the Internet and assess the defense that's engaged.
4. Identify whether your servers are utilizing any ports that have been known to represent insecurities.
5. Ensure you are utilizing the most up-to-date patches for your software.

Tips for avoiding Investment fraud:

1. If the "opportunity" appears too good to be true, it probably is.
2. Beware of promises to make fast profits.
3. Do not invest in anything unless you understand the deal.
4. Don't assume a company is legitimate based on "appearance" of the website.
5. Be leery when responding to investment offers received through unsolicited email.
6. Be wary of investments that offer high returns at little or no risk.
7. Independently verify the terms of any investment that you intend to make.
8. Research the parties involved and the nature of the investment.
9. Be cautious when dealing with individuals outside of your own country.
10. Contact the Better Business Bureau to determine the legitimacy of the company.

Lotteries

The lottery scheme deals with persons randomly contacting email addresses advising them they have been selected as the winner of an International lottery. The Internet Crime Complaint Center has identified numerous lottery names being used in this scheme.

The email message usually reads similar to the following:

"This is to inform you of the release of money winnings to you. Your email was randomly selected as the winner and therefore you have been approved for a lump sum payout of $500,000.00. To begin your lottery claim, please contact the processing company selected to process your winnings."

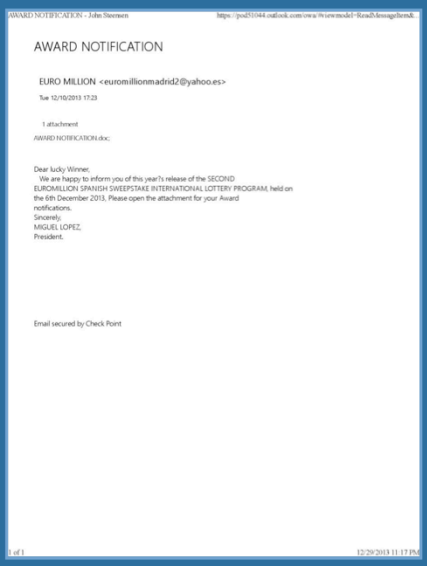
Lotteries (cont.)

An agency name follows this body of text with a point of contact, phone number, fax number, and an email address. An initial fee ranging from $1,000 to $5,000 is often requested to initiate the process and additional fee requests follow after the process has begun. These emails may also list a United States point of contact and address while also indicating the point of contact at a foreign address.

Tips for avoiding Lottery fraud:

1. If the lottery winnings appear too good to be true, they probably are.
2. Be cautious when dealing with individuals outside of your own country.
3. Be leery if you do not remember entering a lottery or contest.
4. Be cautious if you receive a telephone call stating you are the winner in a lottery.
5. Beware of lotteries that charge a fee prior to delivery of your prize.
6. Be wary of demands to send additional money to be eligible for future winnings.
7. It is a violation of federal law to play a foreign lottery via mail or phone.

Lottery



AWARD NOTIFICATION - John Steensen https://pod51044.outlook.com/owa/#viewmodel=ReadMessageItem&

AWARD NOTIFICATION

EURO MILLION <euromillionmadrid2@yahoo.es>

Tue 12/10/2013 17:23

1 attachment

AWARD NOTIFICATION.doc;

Dear lucky Winner,
We are happy to inform you of this year?s release of the SECOND EUROMILLION SPANISH SWEEPSTAKE INTERNATIONAL LOTTERY PROGRAM, held on the 6th December 2013. Please open the attachment for your Award notifications.
Sincerely,
MIGUEL LOPEZ.
President.

Email secured by Check Point

1 of 1 12/29/2013 11:17 PM

Nigerian Letter or "419"

Named for the violation of Section 419 of the Nigerian Criminal Code, the 419 scam combines the threat of impersonation fraud with a variation of an advance fee scheme in which a letter, email, or fax is received by the potential victim. The communication from individuals representing themselves as Nigerian or foreign government officials offers the recipient the "opportunity" to share in a percentage of millions of dollars, soliciting for help in placing large sums of money in overseas bank accounts. Payment of taxes, bribes to government officials, and legal fees are often described in great detail with the promise that all expenses will be reimbursed as soon as the funds are out of the country.

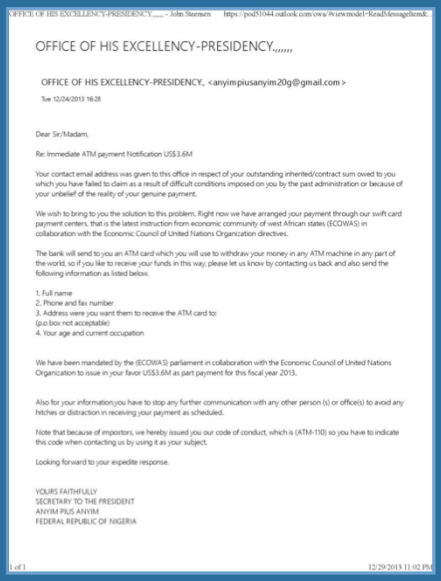
Nigerian Letter or "419" (cont.)

The recipient is encouraged to send information to the author, such as blank letterhead stationary, bank name and account numbers, and other identifying information using a facsimile number provided in the letter. The scheme relies on convincing a willing victim to send money to the author of the letter in several installments of increasing amounts for a variety of reasons.

Tips for avoiding Nigerian Letter or "419" fraud:

1. If the "opportunity" appears too good to be true, it probably is.
2. Do not reply to emails asking for personal banking information.
3. Be wary of individuals representing themselves as foreign government officials.
4. Be cautious when dealing with individuals outside of your own country.
5. Beware when asked to assist in placing large sums of money in overseas bank accounts.
6. Do not believe the promise of large sums of money for your cooperation.
7. Guard your account information carefully.
8. Be cautious when additional fees are requested to further the transaction.

419



OFFICE OF HIS EXCELLENCY-PRESIDENCY.,,,,,,

OFFICE OF HIS EXCELLENCY-PRESIDENCY, <anyimpiusanyim20g@gmail.com>

Tue 12/24/2013 16:28

Dear Sir/Madam,

Re: Immediate ATM payment Notification US$3.6M

Your contact email address was given to this office in respect of your outstanding inherited/contract sum owed to you which you have failed to claim as a result of difficult conditions imposed on you by the past administration or because of your unbelief of the reality of your genuine payment.

We wish to bring to you the solution to this problem. Right now we have arranged your payment through our swift card payment centers, that is the latest instruction from economic community of west African states (ECOWAS) in collaboration with the Economic Council of United Nations Organization directives.

The bank will send to you an ATM card which you will use to withdraw your money in any ATM machine in any part of the world, so if you like to receive your funds in this way, please let us know by contacting us back and also send the following information as listed below.

1. Full name
2. Phone and fax number
3. Address were you want them to receive the ATM card to:
(p.o box not acceptable)
4. Your age and current occupation

We have been mandated by the (ECOWAS) parliament in collaboration with the Economic Council of United Nations Organization to issue in your favor US$3.6M as part payment for this fiscal year 2013.

Also for your information,you have to stop any further communication with any other person (s) or office(s) to avoid any hitches or distraction in receiving your payment as scheduled.

Note that because of impostors, we hereby issued you our code of conduct, which is (ATM-110) so you have to indicate this code when contacting us by using it as your subject.

Looking forward to your expedite response.

YOURS FAITHFULLY
SECRETARY TO THE PRESIDENT
ANYIM PIUS ANYIM
FEDERAL REPUBLIC OF NIGERIA

1 of 1 12/29/2013 11:02 PM

419

YOUR IMMEDIATE CONTRACT PAYMENT.(CASE FILE 54AC003)

Fund Release Department <jimmyhui@pinesystems.com>

YOUR IMMEDIATE CONTRACT PAYMENT(CASE FILE 54AC003)

YOUR IMMEDIATE CONTRACT PAYMENT.
CONTRACTN: MAN/PAP/GOV/MRV/013.

Attention:

The Federal Government of Nigeria has been seriously warned by the United States Government, International Monetary Fund (IMF), World Bank, United Nations (UN) and other international bodies to make sure we settle most of our outstanding foreign debts we owed to Next of Kin's, Fund Beneficiaries and foreign contractors that executed contract with us immediately, this program is organized by the Board of Trustees and Directors for the end of the Year "POVERTY REDUCTION AND ERADICATION". We are using our reputable and well known organization to let you know that you are one of our chosen beneficiaries for this program of "POVERTY REDUCTION AND ERADICATION" in your country e-mail directory.

We hereby inform you that you have successfully being chosen and compensated for an International ATM card written out in your name in the amount of $750, 000, 00 in our West Africa regional Annex. Now, for the compensated price, you will have to contact the Finance House and the Compensation Department for your perusals and claims of your compensated price and my dear beneficiary, below is the contact of the Finance House and Compensation Department (FHCD) for the collection and claims of your international certificated ATM card:

But, a very surprising record was discovered in your payment file that is why you have not been contacted about this since then. Records showed that your inheritance payment has been approved four times and duly completed two times. Also we found out that these funds totaling $750,000.00 was transferred directly from the central bank of Nigeria to the below stated bank account on your authorization and an international ATM CARD was also sent to your house address. This has now resulted in bringing the USA and British Government into the case and we really want you to explain to us what you know about this transfer/payment and delivery.

BANK NAME: STANDARD CHATTERED BANK
BANK ADDRESS, 15B-161 1ST FLOOR, EDINBURGH TOWER,
THE LANDMARK, 15 QUEENS ROAD, CENTRAL HONG KONG.
ACCOUNT NAME: INDO-CHINA GROUP LTD.
A/C #: USD114-102-5567-B.
SWIFT CODE: SCBL 196111

The most baffling part is this payment keeps coming up in every period of debt reconciliation and verification always receives approval like now. NOW OUR QUESTION IS, HAVE YOU RECEIVED YOUR FULL PAYMENT OR ANY PART OF YOUR FUND ENTITLEMENT OWED TO YOU BY THE NIGERIAN GOVERNMENT? WE NEED AN ANSWER FROM YOU WITHIN 24HOURS FROM NOW, AND IF WE DO NOT HEAR FROM YOU IMMEDIATELY YOU RECEIVE THIS MESSAGE TODAY, WE WILL ASSUME YOU ARE INVOLVED AND HAVE RECEIVED OVER PAYMENT, WHICH ONE SHOULD BE RETURNED TO NIGERIA.

Help us to help you, If not call him immediately you receive this message today on is direct number(+2348161992581) or send me a details email disclaiming the information so that you will be issued with claim identification code (CIC) which will help you to secure your claim and payment from fraudulent officials. And also you will be advised and guided accordingly on how you will receive your legitimate fund entitlement from the Nigerian Government, which will be credited into your nominated bank account within 72hours from now or delivered to you as well to your door step.

Therefore, I would advise you to contact FBI Agent Rev Kelvin Williams (JP) for assistance and inform him that your CASE FILE is 54AC003. Contact him directly via the information below if you are yet to receive your funds.

UNITED NATIONS COMPENSATION AWARD PROGRAM
CONTACT Officer:Rev Kelvin Williams (JP)
EMAIL (rev_kelvinwilliams@outlook.com)
CELL PHONE: +2348161992581

Once again it is important to note that your Fund/Payment was released with the following particulars attached to it.

(1) File Number: F1267-2009
(2) Ref Code: KP23-BS7/MCLS /CO
(3) Grant Number: MCC/97846634/09/2D6
(4) Personal Identification Number (PIN): 08647501

Once again stop contacting those people. I adviser that you contact Rev Kelvin Williams (JP) so that he can help you in the collection of your ATM CARD payment instead of dealing with those liars that will be turning you around asking for different kind of money to complete your transaction and the FBI agent can also direct you to the paying bank.

Finally remember that I have forwarded instruction to the finance house on your behalf to send the International ATM card to you as soon as you contact them without delay. Please be informed that you should treat this as confidential as ever and in good faith from the Board and Management of the Organization. Also be informed that the International ATM CARD must get to you through a courier company which you will be responsible for the fees as soon as you contact the agent and also if you want the fund to be transferred as well through the paying bank.

What you have to do now is to contact the Rev Kelvin Williams (JP) as soon as possible to know when they will deliver your package to you because of the expiring date. The only money you will send to the agent to deliver your International ATM card to your postal Address in your country is ($265USD) Dollars only being documentation and Security Keeping Fee of the Courier Company so far. Again, don't be deceived by anybody to pay any other money, except $265USDollars, beside if you fail to comply with the needed $265 US Dollars required there's no way we can

deliver the International ATM card to your country. Disregard any email you get from any impostors or offices claiming to be in possession of your ATM card, you are hereby advise only to be in contact with Rev.Kelvin Williams (JP) who is the rightful person to deal with in regards to your payment and forward any emails you get from impostors to him so he could act upon it immediately. Help stop cyber crime.

You are to provide the following information.

Your Full Name:.....
Your Address:.....
Personal Telephone Number:.....
Age:.....
Sex:.....
Occupation:.....
Nationality:.....
Country:.....

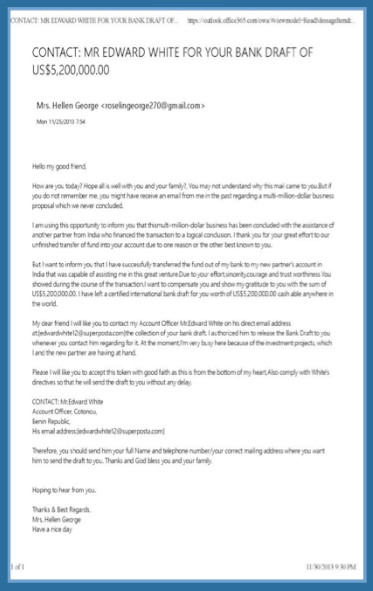
Thanks. God Loves and Bless you and your family.

Hope to contact the F.H.C.D soon.

Your's Faithfully,
Kofi Annan
FORMER UN SECRETARY GENERAL
(CHAIRMAN OF FUND RELEASE)

NOTE : If You Receive This Message In Your Junk Or Spam Its Due To Your Internet Provider.

419



CONTACT: MR EDWARD WHITE FOR YOUR BANK DRAFT OF... https://outlook.office365.com/owa/#viewmodel=ReadMessageItem&...

CONTACT: MR EDWARD WHITE FOR YOUR BANK DRAFT OF US$5,200,000.00

Mrs. Hellen George <roselingeorge270@gmail.com>

Mon 11/25/2013 7:54

Hello my good friend,

How are you today? Hope all is well with you and your family?. You may not understand why this mail came to you.But if you do not remember me, you might have receive an email from me in the past regarding a multi-million-dollar business proposal which ve never concluded.

I am using this opportunity to inform you that thismulti-million-dollar business has been concluded with the assistance of another partner from India who financed the transaction to a logical conclusion. I thank you for your great effort to our unfinished transfer of fund into your account due to one reason or the other best known to you.

But I want to inform you, that I have successfully transferred the fund out of my bank to my new partner's account in India that was capable of assisting me in this great venture.Due to your effort,sincerity,courage and trust worthiness You showed during the course of the transaction.I want to compensate you and show my gratitude to you with the sum of US$5,200,000.00. I have left a certified international bank draft for you worth of US$5,200,000.00 cash able anywhere in the world.

My dear friend I will like you to contact my Account Officer Mr.Edward White on his direct email address at(edwardwhite12@superposta.com)the collection of your bank draft. I as thorized him to release the Bank Draft to you whenever you contact him regarding for it. At the moment,I'm very busy here because of the investment projects, which I and the new partner are having at hand.

Please I will like you to accept this token with good faith as this is from the bottom of my heart,Also comply with White's directives so that he will send the draft to you without any delay.

CONTACT: Mr.Edward White
Account Officer, Cotonou,
Benin Republic.
His email address:(edwardwhite12@superposta.com)

Therefore, you should send him your full Name and telephone number/your correct mailing address where you want him to send the draft to you. Thanks and God bless you and your family.

Hoping to hear from you.

Thanks & Best Regards.
Mrs. Hellen George
Have a nice day

1 of 1 11/30/2013 9:30 PM

419

Greetings in the name of God 9/12/2013 - John Steensen https://pod51044.outlook.com/owa/?viewmodel=ReadMessageItemM...

Greetings in the name of God 9/12/2013

MRS. JULIANA WILLIAMS <marylouis60@outlook.com>

Mon 12/09/2013 8:39

Dear Friend.

I warmly greet you.

Please forgive me if my plea sounds a little strange or unbelievable to you. My family attorney who could have handled the process of executing my WILL & TESTAMENT on my behalf died early this year after a protracted illness. I therefore prayed fervently and by the special grace of GOD, I got your email ID from your country's guest book. I am Mrs. Juliana Williams, a native of United Kingdom, I am 58 years old. I am suffering from protracted cancer of the lungs which has also affected part of my brain cells due to complications. From all indication, my condition has deteriorated and it is quite obvious according to my doctors that i may not live for the next couple of months, because my condition has gotten to a critical and life threatening stage.

I was orphaned at the age of four and was raised in an orphanage. I was married to my late husband Engineer. Steve Williams for twenty years without a child. STEVE had cardiovascular condition and died of cardiac arrest few years ago.I am a fervent Believer and a God fearing woman just like my late husband. Steve and i lived in Nigeria for over 18 years, where my husband a petrochemical engineer by profession worked and rose through the ranks to become an executive director with a multinational construction and oil servicing conglomerate, before his demise. He also established huge private investments that i assisted in managing.

Sequel to the unfortunate and shocking demise of my priceless husband, i decided as a rule not to re-marry, when my cancer ailment became terminal & more so because i do not have a next of kin to bequeath all that STEVE & i labored for. I sold off all our choice properties and other inherited belongings comprising of a shopping mall, an hotel, shares, bonds, jewelries and other valuable family treasures and deposited the proceeds amounting to USD$10,000,000.00 (TEN MILLION DOLLARS ONLY) with First Inland Bank of Nigeria plc. As i write this fund is still deposited with the bank. The management of the bank just wrote me as the sole owner because of the unservicesble status of the fund and suggested to me in a 2 paragraph statement to issue a letter of authorization to someone who can manage the fund on my behalf because of my ill health and also threatened that the fund could be confiscated upon my failure to adhere to their Banking rules and regulations within a stipulated time frame.

I am presently at the intensive care unit of a London hospital, located at Fulham road in west London. It is the leading cancer treatment hospital in the world and i have been undergoing treatment there for late-stage terminal cancer of the lungs. I am computer literate and was fortunate enough to have my personal laptop with me. hence I am writing from my sick bed. I rarely talk; my doctors told me that I have only few months to live, unless there is a divine intervention. It is my last WISH therefore to see that 90% of this fund is invested in any charitable organization of your choice and administered as you may deem fit, especially to the orphanage homes and homes for destitute and the mentally retarded, you can also extend some part of the funds to churches and mosques and to those struck by natural disaster, if you wish.10% of the fund could also be expended on cost of administration of WILL & TESTAMENT and also on logistic support and other sundry arrangements that you may require as soon as the fund

I crave your indulgence as a God fearing individual and as someone who cares for the less-privileged as much as i do, to take it upon yourself and use this fund for the above mentioned purposes. I took this painstaking decision in other to

1 of 2 12/29/2013 11:22 PM

Greetings in the name of God 9/12/2013 - John Steensen https://pod51044.outlook.com/owa/?viewmodel=ReadMessageItemM...

help humanity in my little capacity before i rest in peace in the bosom of GOD almighty. According to my physicians my time will soon be up.

As soon as I receive your reply and personal information as listed below, I shall give you the official contact of the First Inland Bank plc officials, to enable you contact the Bank without delays. I will also issue you with a letter of authorization, so that my bankers will recognize your status as the new beneficiary of the fund.

The letter of authorization will further prove that you are the new beneficiary of my ESTATE, WILL & TESTAMENT, the funds have an open beneficiary mandate and as such, it is whom i authorize or appoint to act on my behalf that the bank will recognize and release the funds to.Please assure me that you will not treat this offer with levity but will rather give my bequest continued existence.

Send the information in this order:

(1) Your full names: ==========
=====
(2) Personal or official contact address:========== =========
(3) Home or Office phone:==========Cell phone:==========Fax:========
(4) Your Age: ==========
(5) Occupation:========== ========
(6) Sex/Marital status:========== =
(7) Private E-mail Address: ==========

Awaiting your kind response while craving your appreciation of my predicament.

Your Friend In Christ.

Mrs. Juliana Williams
(London Uk)
Private Email: mrsjuliana.ws76@globomail.com

2 of 2 12/29/2013 11:22 PM

419

Re: Can I Trust You???

Heath Quincy <bilgi@beyaztv.com.tr>

Mon 12/02/2013 0:24

I am Capt. Heath Quincy of the US Army base in Afghanistan for peace keeping I found your contact detail in a address journal am seeking your assistance to evacuate the sum of $18,000,000.00 to you as long as I am assured that it will be safe in your care until I complete my service here in Afghanistan. This is not stolen money and there are no dangers involved, I count on your understanding,please get back to my personal email: heathmquincy@yahoo.com.hk
Heath Quincy

1 of 1 12/29/2013 11:29 PM

419

Attention Read And Comply ASAP From BANK OF AMERICA - In... https://pod51044.outlook.com/owa/#viewmodel=ReadMessageItemE...

Attention Read And Comply ASAP From BANK OF AMERICA

BANK OF AMERICA <mr.denis.k.montag01@outlook.com>

Wed 12/04/2013 0:20

FROM THE DESK OF MR.DENIS K. MONTAG,
ATM DEPARTMENT DIRECTOR BANK OF AMERICA,
OFFICE TEL NUMBER: 9174609343
EMAIL: mr.denis.k.montag2013@r7.com

BANK OF AMERICA: ATM CARD PAYMENT NOTIFICATION

ATTN: PLEASE,

I AM MR.DENIS K. MONTAG, THE ATM DEPARTMENT DIRECTOR BANK OF AMERICA, PLEASE READ THIS MAIL CAREFULLY AND PROCEED TO COLLECT YOUR ATM CARD WORTH OF $23,300,000.00 PAYMENT. FOLLOWING THIS YEAR'S (2013) REVIEW OF THE GLOBAL FINANCIAL MATTERS AND JUST CONCLUDED INVESTIGATIONS BY THE FEDERAL BUREAU OF INVESTIGATION IN CONJUNCTION WITH THE ECONOMIC AND FINANCIAL CRIME COMMISSION, IT IS REVEALED THAT YOUR EMAIL IS AMONG THE LIST OF PEOPLE WHO HAVE NEVER RECEIVED ANY OF THEIR PAYMENTS AMONG LOTTERY, INHERITANCE, COMPENSATION AND AWARDED CONTRACT FUNDS AND VICTIMS WHO HAVE LOST A LOT OF MONEY TO SCAMMERS WHILE TRYING TO CLAIM THEIR FUNDS, IN VIEW OF THE FOREGOING, A NEW PAYMENT OF US$23,300,000.00 HAS BEEN APPROVED IN YOUR FAVOR AND CREDITED INTO AN ATM CARD WHICH SHALL BE DELIVERED TO YOU.

THIS IS TO INFORM YOU THAT WE RECEIVED A PAYMENT NOTIFICATION FROM THE PRESIDENCY AND EXECUTIVE COUNCIL FEDERAL REPBLIC OF NIGERIA, AND ALSO FROM THE FEDERAL BUREAU OF INVESTIGATION FBI IN CONJUNCTION WITH THE ECONOMIC AND FINANCIAL CRIME COMMISSION EFCC THAT WE THE BANK OF AMERICA REACHED OUT AN AGREEMENT WITH THE FEDERAL EXECUTIVE COUNCIL AND THE SENATE TO USE THE FEDERAL RESERVE ACCOUNT TO SETTLE ALL OUT ALL OUR STANDING PAYMENT TO ALL OUR FOREIGN DEBTORS,RIGHT NOW WE HAVE ARRANGED YOUR PAYMENT OF 2.3,3MILLION DOLLARS THROUGH OUR SWIFT CARD PAYMENT CENTER ASIA PACIFIC, THAT IS THE LATEST INSTRUCTION FROM THE PAYMENT PANEL COMMITTEE FEDERAL REPUBLIC OF NIGERIA.THIS CARD CENTER WILL SEND YOU AN ATM CARD WHICH YOU WILL USE TO WITHDRAW YOUR MONEY IN ANY ATM MACHINE IN ANY PART OF THE WORLD, SO IF YOU LIKE TO RECEIVE YOUR FUND IN THIS WAY, PLEASE GET BACK TO US WITH THE REQUIRED INFORMATION BELOW.

1) FULL NAME:
2) ADDRESS WERE YOU WANT US TO SEND THE ATM CARD:
3) PHONES:
4) FAX NUMBER:
5) YOUR AGE:
6) CURRENT OCCUPATION:
7) ATTACH COPY OF YOUR IDENTIFICATION:

PLEASE DO PROVIDE THE ABOVE INFORMATION ACCURATELY, BECAUSE THIS OFFICE CANNOT AFFORD TO BE HELD LIABLE FOR ANY WRONG TRANSFER OF FUNDS. THANKS FOR BANKING WITH BANK OF AMERICA WHILE WE LOOKING FORWARD TO SERVING YOU WITH THE BEST OF OUR SERVICE.NOTE: THOUSANDS OF FRAUDSTERS HAVE

1 of 2 12/29/2013 11:32 PM

Attention Read And Comply ASAP From BANK OF AMERICA - In... https://pod51044.outlook.com/owa/#viewmodel=ReadMessageItemE...

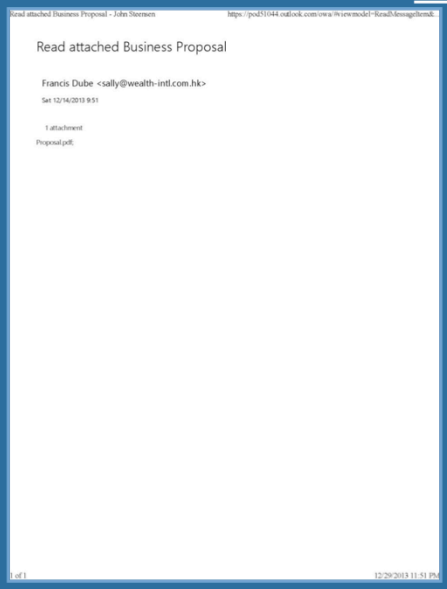
BEEN USING THIS METHOD IN SCAMMING MOST FOREIGN CREDITORS, WHICH WE HAVE IN THE PAYMENT LIST HERE IN OUR OFFICE. WE USE THIS MEDIUM TO INFORM YOU THAT ANY MAIL THAT DO NOT COME WITH THE NEW COMMUNICATION CODE: (BOA/FBI/EFCC/NG) IS FALSE. IN THIS CASE, YOU'RE ADVICE NOT TO RESPOND TO ANY MAIL THAT DOES NOT COME WITH THE ABOVE COMMUNICATION CODE FOR SAFETY PURPOSE.OUR FINAL CONCLUSION WAS THAT, THE FUND SHOULD BE PAID TO YOU VIA AN AUTOMATED TELLER MACHINE CARD (ATM) AS IT SEEMS, THIS WILL BE EASIER AND FASTER FOR YOU TO RECEIVE. YOUR NEW COMMUNICATION CODE:(BOA/FBI/EFCC/NG)

LOOKING FORWARD TO SERVING YOU BETTER.

THANKS AND GOD BLESS.
YOURS TRULY
MR.DENIS K. MONTAG,
ATM DEPARTMENT DIRECTOR BANK OF AMERICA,
OFFICE TEL NUMBER: 9174609343
EMAIL: mr.denis.k.montag2013@r7.com

2 of 2 12/29/2013 11:32 PM

419


Read attached Business Proposal - John Steensen https://pod51044.outlook.com/owa/#viewmodel=ReadMessageItem&I...

Read attached Business Proposal

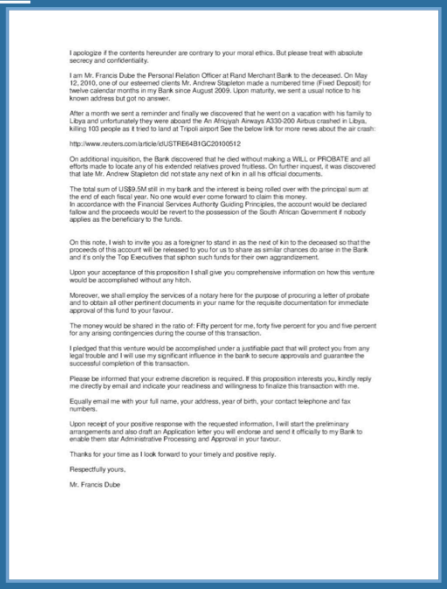
Francis Dube <sally@wealth-intl.com.hk>

Sat 12/14/2013 9:51

1 attachment

Proposal.pdf;

1 of 1 12/29/2013 11:51 PM


I apologize if the contents hereunder are contrary to your moral ethics. But please treat with absolute secrecy and confidentiality.

I am Mr. Francis Dube the Personal Relation Officer at Rand Merchant Bank to the deceased. On May 12, 2010, one of our esteemed clients Mr. Andrew Stapleton made a numbered time (Fixed Deposit) for twelve calendar months in my Bank since August 2009. Upon maturity, we sent a usual notice to his known address but got no answer.

After a month we sent a reminder and finally we discovered that he went on a vacation with his family to Libya and unfortunately they were aboard the An Afriqiyah Airways A330-200 Airbus crashed in Libya, killing 103 people as it tried to land at Tripoli airport See the below link for more news about the air crash:

http://www.reuters.com/article/idUSTRE64B1QC20100512

On additional inquisition, the Bank discovered that he died without making a WILL or PROBATE and all efforts made to locate any of his extended relatives proved fruitless. On further inquest, it was discovered that late Mr. Andrew Stapleton did not state any next of kin in all his official documents.

The total sum of US$9.5M still in my bank and the interest is being rolled over with the principal sum at the end of each fiscal year. No one would ever come forward to claim this money.
In accordance with the Financial Services Authority Guiding Principles, the account would be declared fallow and the proceeds would be revert to the possession of the South African Government if nobody applies as the beneficiary to the funds.

On this note, I wish to invite you as a foreigner to stand in as the next of kin to the deceased so that the proceeds of this account will be released to you for us to share as similar chances do arise in the Bank and it's only the Top Executives that siphon such funds for their own aggrandizement.

Upon your acceptance of this proposition I shall give you comprehensive information on how this venture would be accomplished without any hitch.

Moreover, we shall employ the services of a notary here for the purpose of procuring a letter of probate and to obtain all other pertinent documents in your name for the requisite documentation for immediate approval of this fund to your favour.

The money would be shared in the ratio of: Fifty percent for me, forty five percent for you and five percent for any arising contingencies during the course of this transaction.

I pledged that this venture would be accomplished under a justifiable pact that will protect you from any legal trouble and I will use my significant influence in the bank to secure approvals and guarantee the successful completion of this transaction.

Please be informed that your extreme discretion is required. If this proposition interests you, kindly reply me directly by email and indicate your readiness and willingness to finalize this transaction with me.

Equally email me with your full name, your address, year of birth, your contact telephone and fax numbers.

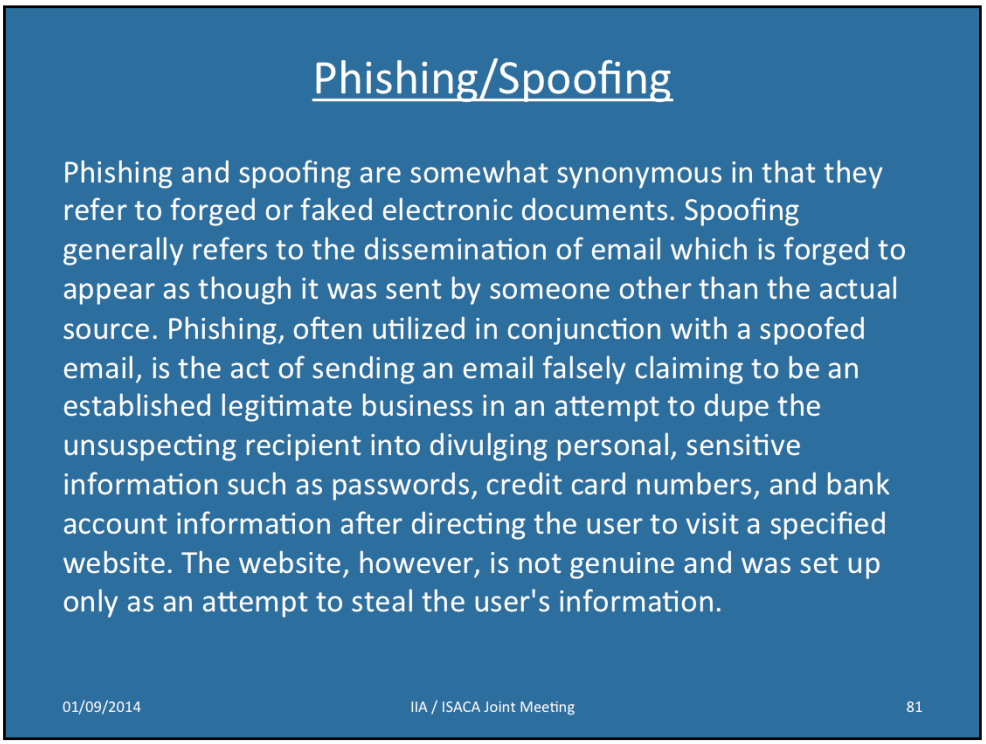
Upon receipt of your positive response with the requested information, I will start the preliminary arrangements and also draft an Application letter you will endorse and send it officially to my Bank to enable them star Administrative Processing and Approval in your favour.

Thanks for your time as I look forward to your timely and positive reply.

Respectfully yours,

Mr. Francis Dube

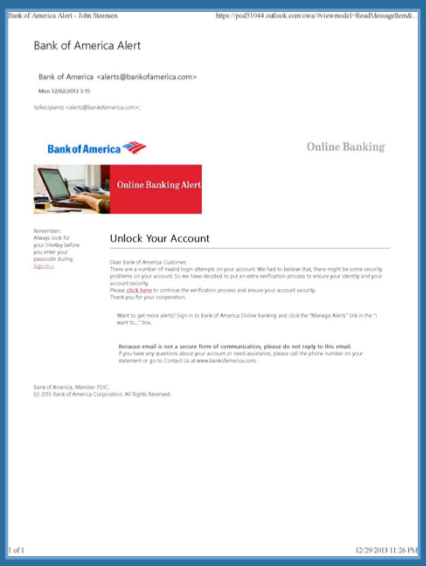
01/09/2014 IIA / ISACA Joint Meeting 80



Tips for avoiding Phishing/Spoofing fraud:

1. Be suspicious of any unsolicited email requesting personal information.
2. Avoid filling out forms in email messages that ask for personal information.
3. Always compare the link in the email to the link that you are actually directed to.
4. Log on to the official website, instead of "linking" to it from an unsolicited email.
5. Contact the actual business that supposedly sent the email to verify if the email is genuine.

Phishing email



Bank of America Alert - John Steenen https://pod51044.outlook.com/owa/#viewmodel=ReadMessageItemM...

Bank of America Alert

Bank of America <alerts@bankofamerica.com>

Mon 12/02/2013 1:15

ToRecipients <alerts@bankofamerica.com>;

Bank of America

Online Banking

Online Banking Alert

Remember:
Always look for your SiteKey before you enter your passcode during Sign In.

Unlock Your Account

Dear Bank of America Customer,
There are a number of invalid login attempts on your account. We had to believe that, there might be some security problems on your account. So we have decided to put an extra verification process to ensure your identity and your account security.
Please click here to continue the verification process and ensure your account security.
Thank you for your cooperation.

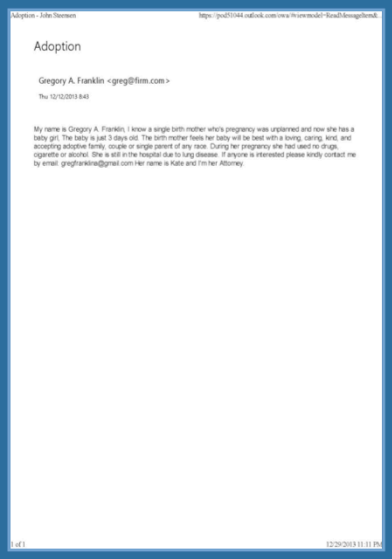
Want to get more alerts? Sign in to Bank of America Online Banking and click the "Manage Alerts" link in the "I want to..." box.

Because email is not a secure form of communication, please do not reply to this email.
If you have any questions about your account or need assistance, please call the phone number on your statement or go to Contact Us at www.bankofamerica.com.

Bank of America, Member FDIC.
(c) 2013 Bank of America Corporation. All rights reserved.

1 of 1 12/29/2013 11:26 PM

Phishing email



Adoption

Gregory A. Franklin <greg@firm.com>

Thu 12/12/2013 8:43

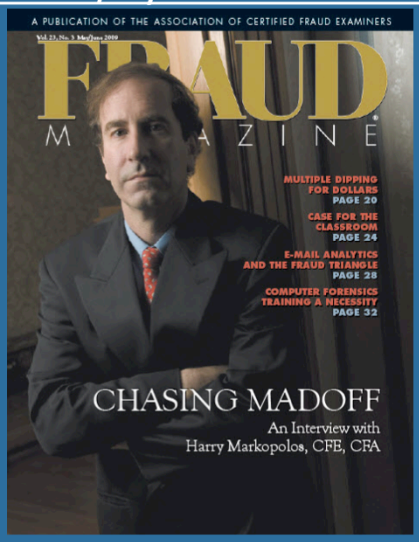
My name is Gregory A. Franklin, I know a single birth mother who's pregnancy was unplanned and now she has a baby girl. The baby is just 3 days old. The birth mother feels her baby will be best with a loving, caring, kind, and accepting adoptive family, couple or single parent of any race. During her pregnancy she had used no drugs, cigarette or alcohol. She is still in the hospital due to lung disease. If anyone is interested please kindly contact me by email: gregfranklinx@gmail.com Her name is Katie and I'm her Attorney.

1 of 1

Ponzi/Pyramid Scheme

Ponzi or pyramid schemes are investment scams in which investors are promised abnormally high profits on their investments. No investment is actually made. Early investors are paid returns with the investment money received from the later investors. The system usually collapses. The later investors do not receive dividends and lose their initial investment.

Ponzi/Pyramid Scheme



http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/Chasing-Madoff.pdf

01/09/2014 IIA / ISACA Joint Meeting 85

Tips for avoiding Ponzi/Pyramid Scheme fraud:

1. If the "opportunity" appears too good to be true, it probably is.
2. Beware of promises to make fast profits.
3. Exercise diligence in selecting investments.
4. Be vigilant in researching with whom you choose to invest.
5. Make sure you fully understand the investment prior to investing.
6. Be wary when you are required to bring in subsequent investors.
7. Independently verify the legitimacy of any investment.
8. Beware of references given by the promoter.

Reshipping

The "reshipping" scheme requires individuals in the United States, who sometimes are co-conspirators and other times are unwitting accomplices, to receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.

"Reshippers" are being recruited in various ways but the most prevalent are through employment offers and conversing, and later befriending, unsuspecting victims through Internet Relay Chat Rooms.

Unknown subjects post help-wanted advertisements at popular Internet job search sites and respondents quickly reply to the online advertisement. As part of the application process, the prospective employee is required to complete an employment

Reshipping (cont.)

application, wherein he/she divulges sensitive personal information, such as their date of birth and social security number which, unbeknownst to the victim employee, will be used to obtain credit in his/her name.

The applicant is informed he/she has been hired and will be responsible for forwarding, or "reshipping," merchandise purchased in the United States to the company's overseas home office. The packages quickly begin to arrive and, as instructed, the employee dutifully forwards the packages to their overseas destination. Unbeknownst to the "reshipper," the recently received merchandise was purchased with fraudulent credit cards.

Reshipping (cont.)

The second means of recruitment involves the victim conversing with the unknown individual in various Internet Relay Chat Rooms. After establishing this new online "friendship" or "love" relationship, the unknown subject explains for various legal reasons his/her country will not allow direct business shipments into his/her country from the United States. He/she then asks for permission to send recently purchased items to the victim's United States address for subsequent shipment abroad for which the unknown subject explains he/she will cover all shipping expenses.

Tips for avoiding Reshipping fraud:

1. Be cautious if you are asked to ship packages to an "overseas home office."
2. Be cautious when dealing with individuals outside of your own country.
3. Be leery if the individual states that his country will not allow direct business shipments from the United States.
4. Be wary if the "ship to" address is yours but the name on the package is not.
5. Never provide your personal information to strangers in a chat room.
6. Don't accept packages that you didn't order.
7. If you receive packages that you didn't order, either refuse them upon delivery or contact the company where the package is from.

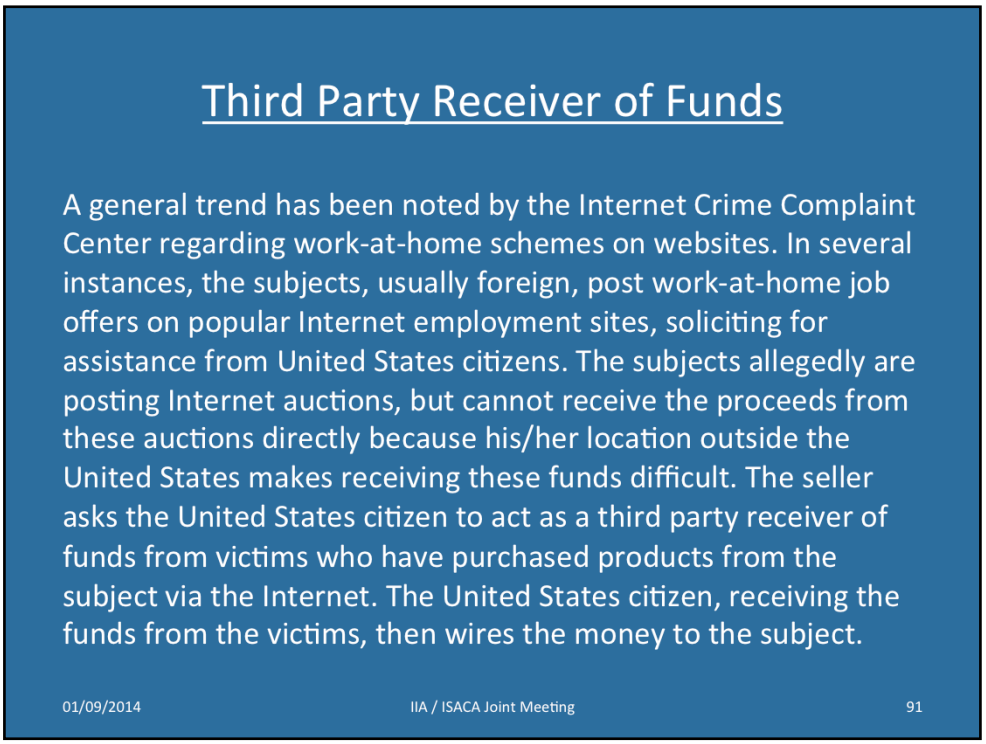
Spam

With improved technology and world-wide Internet access, spam, or unsolicited bulk email, is now a widely used medium for committing traditional white collar crimes including financial institution fraud, credit card fraud, and identity theft, among others. It is usually considered unsolicited because the recipients have not opted to receive the email. Generally, this bulk email refers to multiple identical messages sent simultaneously. Those sending this spam are violating the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, Title 18, U.S. Code, Section 1037.

Spam can also act as the vehicle for accessing computers and servers without authorization and transmitting viruses and botnets. The subjects masterminding this Spam often provide hosting services and sell open proxy information, credit card information, and email lists illegally.

Tips for avoiding Spam and Spam-related fraud:

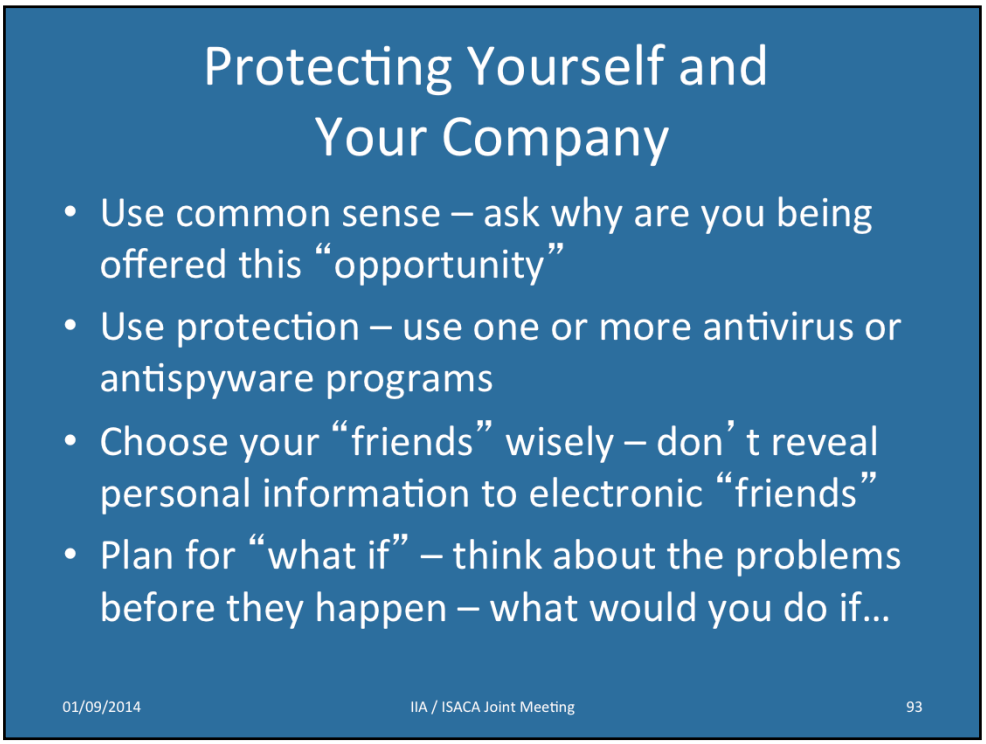
1. Don't open spam. Delete it unread.
2. Never respond to spam as this will confirm to the sender that it is a "live" email address.
3. Have a primary and secondary email address - one for people you know and one for all other purposes.
4. Avoid giving out your email address unless you know how it will be used.
5. Never purchase anything advertised through an unsolicited email.



Tips for avoiding Third Party Receiver of Funds fraud:

1. Do not agree to accept and wire payments for auctions that you did not post.
2. Be leery if the individual states that his country makes receiving these type of funds difficult.
3. Be cautious when the job posting claims "no experience necessary".
4. Be cautious when dealing with individuals outside of your own country.

How can you protect yourself from cybercrime?



How to Protect Yourself from Cyber Crime

Wealth Daily's Weekend Edition

http://www.wealthdaily.com/articles/how-to-protect-yourself-from-cyber-crime/3280

1. Keep your firewall turned on. First, lock your doors. A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information.

2. Install or update your antivirus software. Second, roll up your windows. Antivirus software is designed to prevent malicious software programs from embedding themselves on your computer. Most types of antivirus software can be set up to update automatically.

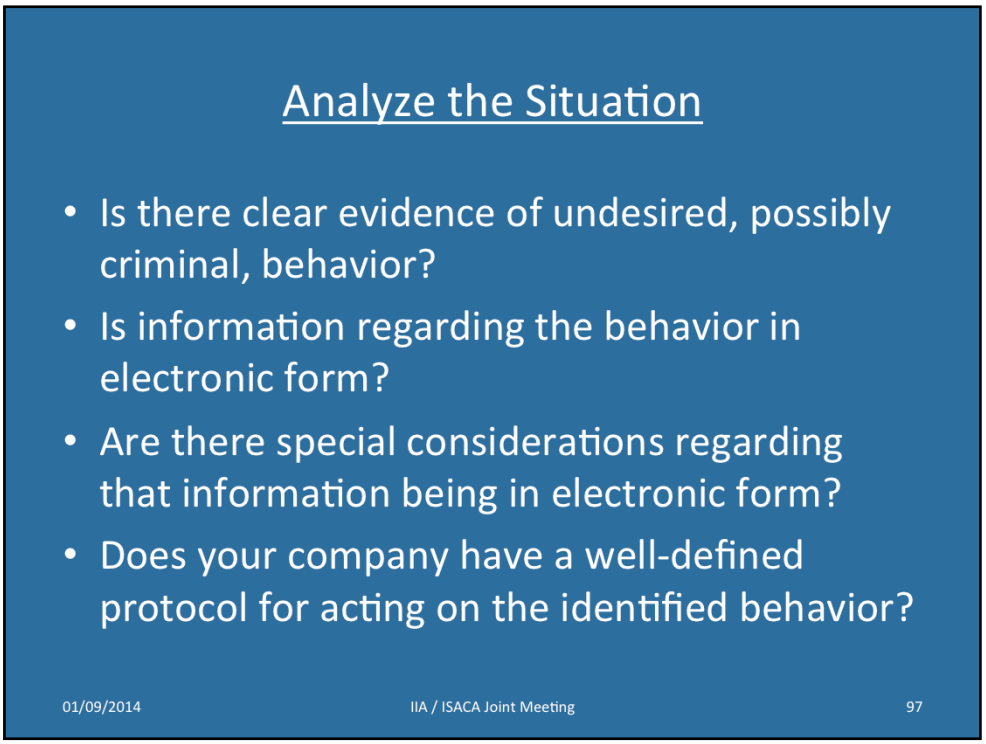
3. Install or update your antispyware technology. Spyware is just what it sounds like: Software that lets other people spy on you. Some spyware collects information about you without your consent; others produce unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store.

Looks Too Good To Be True

- http://www.lookstoogoodtobetrue.com/
- Funded by USPS, FBI, NW3C, Target, Monster.com and others

Legitimate vendors almost always have security warnings and advice on how to use their site safely and securely. Take a few minutes to review their advice.

What are your options if you think you or your company is a victim of a cybercrime?



Remember: Only law enforcement personnel can authoritatively state a crime has been committed.

"Who Ya Gonna Call?"

- Not the Ghostbusters! 
- Law Enforcement
  - **Local Police**
  - **IC3** (http://www.ic3.gov/complaint/default.aspx)
- Legal Counsel
- Forensic Examiner