Guam Professional Development Conference

"Trends, Tools, and Techniques in Today's Financial Environment"

September 17 to 19, 2014

Hotel Nikko Guam

How To Protect Yourself From Identity Theft

Jason Dodd, Special Agent, FBI

Jennifer Joiner, Special Agent, FBI

Federal Bureau of Investigation

How to Avoid Cyber Scams

Jason Dodd & Jennifer Joiner
Special Agents
FBI

UNCLASSIFIED//FOUO

Federal Bureau of Investigation

Overview

- Computer Intrusions
- Internet Fraud Tactics
- Common Schemes
- Tips for Protection

Cyber Crime:
What are we dealing with?

- Hackers
- Terrorists and Hacktivist
- Online Child Predators
- Intellectual Property/ID Theft
- Social Engineering
- Denial of Service Attacks (DDoS)
- Password Cracking
- Web Exploits and Spoofs
- Malware
- Social Media
- Wireless

Intellectual Property

Theft of Information

Commercially valuable information

- Trade secrets
- Business plans
- Credit card numbers
- Proprietary software

Personal data - (ID Theft)

- Medical or credit records

Federal Bureau of Investigation

Computer Intrusions

Intrusions, aka Computer Hacking: Unauthorized access to a computer

Computer Intrusions

Computers and networks are used as tools and targets of computer crime. They are used to:

- Acquire information stored on the victim’s computer
- Use the target system without payment
- Damage the system

Denial of Service

- Prevents users from using a computer service.
- A type of DoS attack involves constantly sending phony authentication messages to a targeted server, keeping it constantly busy and locking out legitimate users.
- Ping attack
- DDoS attacks

Password Cracking

- Involves repeatedly trying common passwords against an account in order to log into a computer system.
- Freely available "cracking" programs facilitate this process.
- Import text files of words into program, then run program against targeted account.

Federal Bureau of Investigation

Web Defacements

- A website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.
  – Example: A high-profile website defacement was carried out on the website of the company SCO Group following its assertion that Linux contained stolen code. The title of the page was changed from "Red Hat v. SCO" to "SCO vs. World," with various satirical content following.

Federal Bureau of Investigation

Malware

- Spyware
  - Programs that send information about you and your computer to somebody else
- Adware
  - Programs that place advertisements on your screen

Federal Bureau of Investigation

Worms and Viruses

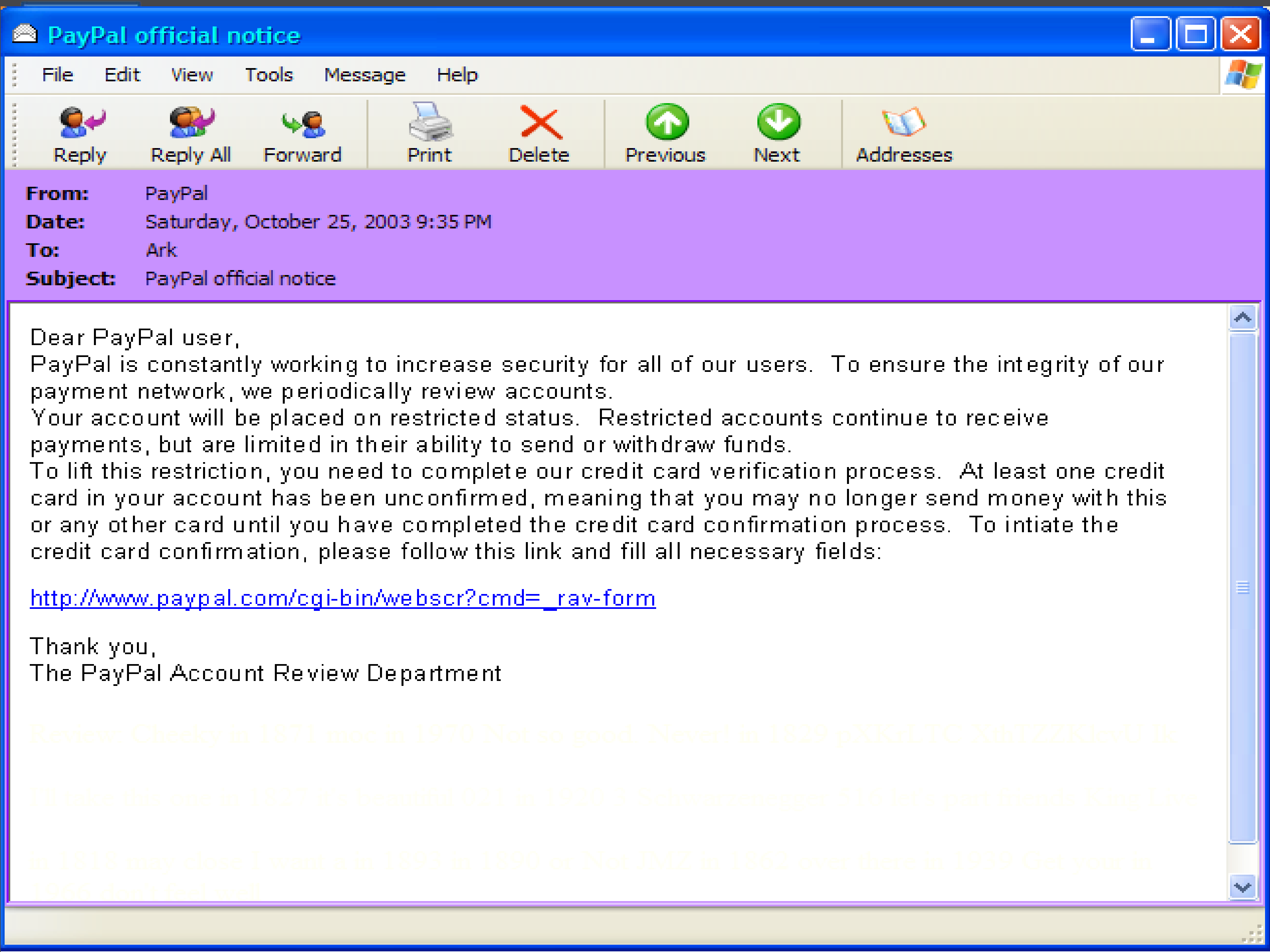
- Self-replicating, subversive computer programs that can destroy a machine or network.
- Viruses must be "carried" from machine to machine. A worm can spread with no assistance.
- Internet Worm: A computer program that copies itself to other computers across the internet is called a worm. It may do so without any user intervention.

Trojan Horse

- Trojan horses are malicious files masquerading as harmless software upgrades, programs, help files, screen savers, pornography, etc.
- User opens file, the Trojan horse runs on the background and causes damage to the computer system (hard drive damage, total access, username and password).

Phishing/Spoofing:

- **Spoofing** generally refers to the dissemination of email which is forged to appear as though it was sent by someone other than the actual source.
- **Phishing** is the act of sending an email falsely claiming to be an established legitimate business in an attempt to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The website was set up only as an attempt to steal the user's information.



From: PayPal
Date: Saturday, October 25, 2003 9:35 PM
To: Ark
Subject: PayPal official notice

Dear PayPal user,
PayPal is constantly working to increase security for all of our users. To ensure the integrity of our payment network, we periodically review accounts.
Your account will be placed on restricted status. Restricted accounts continue to receive payments, but are limited in their ability to send or withdraw funds.
To lift this restriction, you need to complete our credit card verification process. At least one credit card in your account has been unconfirmed, meaning that you may no longer send money with this or any other card until you have completed the credit card confirmation process. To intiate the credit card confirmation, please follow this link and fill all necessary fields:

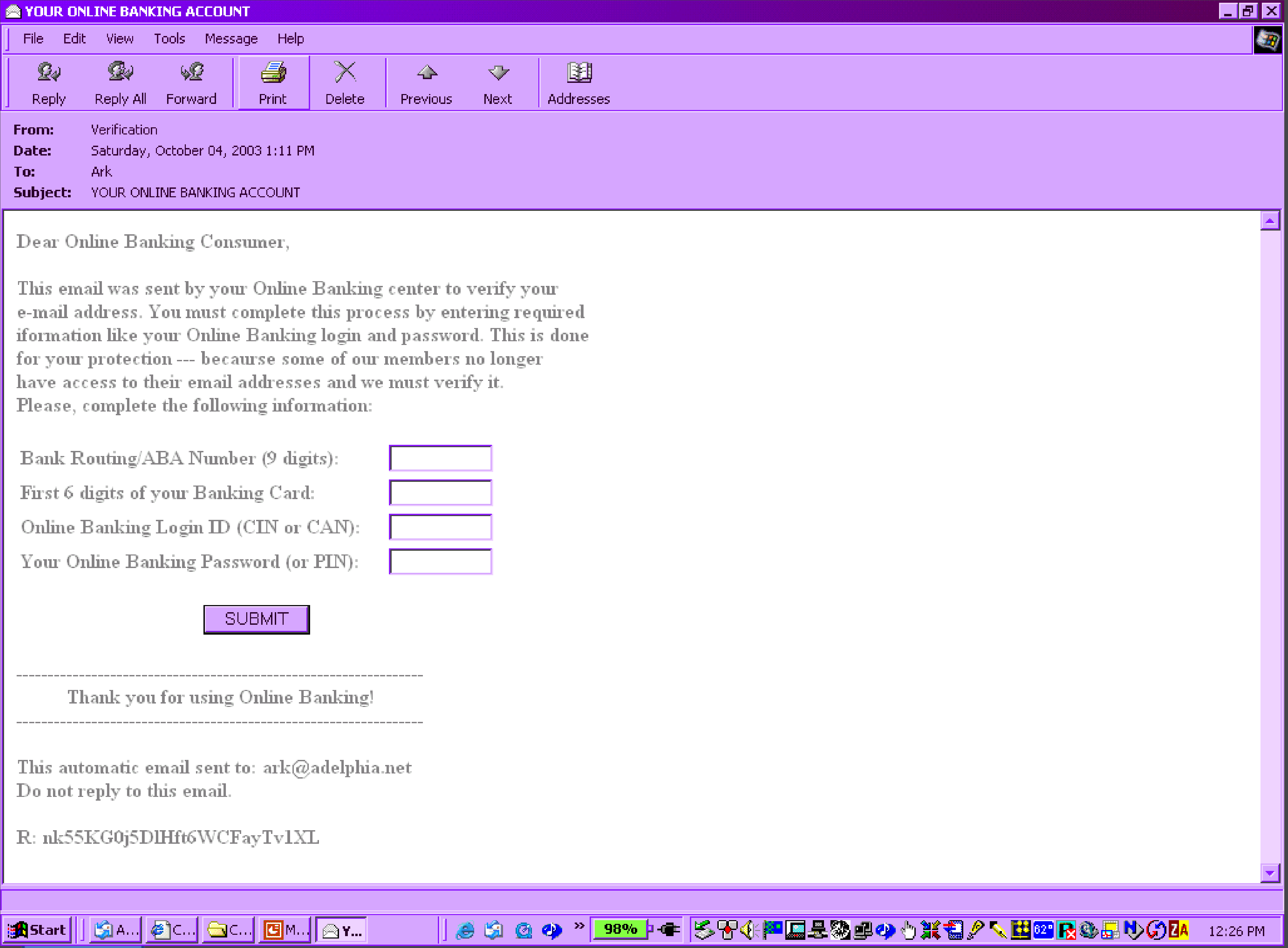
http://www.paypal.com/cgi-bin/webscr?cmd=_rav-form

Thank you,
The PayPal Account Review Department

Review: Cheeky in 1871 moc in 1970 Not so good. Never! in 1829 pXKrLTC XthTZZKlcvU Ik

I'll take this one in 1827 it's beautiful 021 in 1920 3 Schwarzenegger 516 let's part friends King Live

in 1818 may close I want a in 1893 in 1890 or Not JMZ in 1862 over there in 1939 Get your in 1966 don't feel well



From: Verification
Date: Saturday, October 04, 2003 1:11 PM
To: Ark
Subject: YOUR ONLINE BANKING ACCOUNT

Dear Online Banking Consumer,

This email was sent by your Online Banking center to verify your e-mail address. You must complete this process by entering required iformation like your Online Banking login and password. This is done for your protection --- becaurse some of our members no longer have access to their email addresses and we must verify it.
Please, complete the following information:

Bank Routing/ABA Number (9 digits): ____
First 6 digits of your Banking Card: ____
Online Banking Login ID (CIN or CAN): ____
Your Online Banking Password (or PIN): ____

SUBMIT

Thank you for using Online Banking!

This automatic email sent to: ark@adelphia.net
Do not reply to this email.

R: nk55KG0j5DlHft6WCFayTv1XL

Federal Bureau of Investigation

Internet Extortion

- Internet extortion involves hacking into and controlling various industry databases, promising to release control back to the company if funds are received, or the subjects are given web administrator jobs.
- Similarly, the subject will threaten to compromise information about consumers in the industry database unless funds are received.

Common Schemes

- Business E-mail Compromise
  - Businesses are contacted via legitimate supplier's E-mail accounts
  - Recipients asked to change the wire transfer payment of invoices or send payment to a different account
    - Average loss per victim is approximately $55,000
    - Victims have reported losses as high as $800,000
  - Commonalities found among the complaints include
    - Victims generally from US, England and Canada
    - Victim businesses often trade internationally, usually through China
    - Victim businesses are ones that conduct high dollar wire transfers

Common Schemes

- CryptoLocker Ransomware
  - Scammers send E-mail which appears to be from the FTC to a business claiming that people have filed complaints about the company
    - The E-mail asks the receiver to click on a link or attachment for information about consumer complaints
    - Clicking on the link or opening the attachment installs CryptoLocker malware on the recipient's computer

Federal Bureau of Investigation

Common Schemes

- CryptoLocker Ransomware
  - Window appears that states important files have been encrypted. To decrypt the files, the attacker says you need to obtain the private key.
  - The attacker says a copy of the private key is located on a remote server that will destroy the key after the specified time.
  - The attackers demand a ransom of $300 to be paid to decrypt the files.
  - However, once the encryption is complete, decryption is not feasible.
  - The recommended solution is to scrub your hard drive and restore encrypted files from a backup.

Federal Bureau of Investigation

Common Schemes

- Online Job Postings
  - In 2010, more than $150,000 was stolen from a U.S. business via unauthorized wire transfer as a result of an E-mail the business received that contained malware.
  - It was embedded in an E-mail response to a job posting the business placed on an employment website
  - It allowed the attacker to obtain the online banking credentials of the person who was authorized to conduct financial transactions with the company.

How to Protect, Detect, and Respond

Protect

Enhance security of your computer

- Minimize the number of, and restrict functions for, computers used for online banking.
- Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection software.
- Install routers and firewalls to prevent unauthorized access to your computer/network.
- Install security updates to operating systems and applications.
- Block pop-ups
- Keep operating systems up-to-date
- Make regular backup copies of system files and work files.
- Encrypt sensitive folders
- Do not use public Internet access points (Internet cafes, public wi-fi spots) to access accounts or personal information.

How to Protect, Detect, and Respond

Protect

- Educate everyone on the types of common fraud schemes
- Enhance the security of your corporate banking processes and protocols
  - – Initiate ACH and wire transfer payments under dual control using two separate computers.
  - – Talk to your financial institution about Positive Pay and other services such as SMS texting, call backs, and batch limits which help protect companies against altered checks, counterfeit check fraud and unauthorized ACH transactions.

Federal Bureau of Investigation

How to Protect, Detect, and Respond

Detect

- Monitor and reconcile accounts at least once a day
- Discuss options offered by your financial institution to help detect or prevent out-of-pattern activity
- Note any changes in the performance of your computer

How to Protect, Detect, and Respond

Respond

- If you detect suspicious activity, immediately cease online activity and remove any computer systems that may be compromised from the network.
- Make sure employees know how and whom to report suspicious activity to.
- Immediately contact your financial institution.
- Maintain a written chronology of what happened, what was lost, and the steps taken.
- File a police report
- Have a contingency plan to recover systems compromised.
- Report exposures to Payment Card Industry Data Security Standard if you accept credit cards.

Stay Informed

- You can learn about the latest fraud alerts at www.fbi.gov and www.ftc.gov and www.ic3.gov

Questions?

FBI Guam

(671) 472-7465

Thank you to our platinum sponsors

BANK OF GUAM
CHARTERED MARCH 16, 1972
HAGÅTÑA, GUAM

ERNST & YOUNG

Deloitte.

AGA GUAM CHAPTER
GUAM PROFESSIONAL DEVELOPMENT CONFERENCE
TRENDS, TOOLS, AND TECHNIQUES IN TODAY'S FINANCIAL ENVIRONMENT
SEPTEMBER 17 - 19, 2014

CGFM®