

Commercial Client Risk and Internet Fraud Update

Carl L. Hairston

Regional Manager, Capital Region

Business & Professional Banking Group

Tuesday, March 22, 2011

Agenda

- Understanding new Internet risks and fraud trends
- Understanding crimeware like Zeus and how it works
- How to help your clients protect their businesses
- Review business fraud protection and risk reduction checklist
- Discuss some fraud risks and solutions
- Questions & Answers

Disclaimer

- This presentation is intended for information purposes
- Clients should contact their Information Technology provider to determine the best way to safeguard the security of their computers and networks
- Clients should familiarize themselves with their institution's account agreement and understand their liability for fraud as ACH and Wire transactions are regulated under the Uniform Commercial Code.

Drawing Some Relevant Correlations



"You know, you can do this just as easily online."

Drawing Some Relevant Correlations



Trends: Internet Fraud Waves

1st Attack Wave: Internet Merchant Databases

Began: Mid 1990s.

Target: Attack Internet merchant payment databases.

Security: Inadequate merchant security with no security standards.

2nd Attack Wave: Magnetic-stripe Data

Began: Early 2000s – continuing.

Target: Attack stores of magnetic-stripe data.

Security: PCI initiated; stores of magnetic-stripe data eliminated.

Counter-offensive: Attackers place own sniffers to collect magnetic-stripe data.

3rd Attack Wave: Consumer-entered Data

Began: Mid 2000s – evolving.

Target: PCs key-logged as consumers enter financial data.

Security: Countering Trojans targeting consumer PCs increasing difficult.

Problems: Expands beyond payment cards to engulf other financial industries.

Fraudsters Continue to Target Consumers

- Symantec indentified more than 90,000 unique versions of the Zeus/Zbot trojan crimeware in 2009 alone
- **There were more than *25 million new strains of malware (crimeware) created in 2009***
- In Q2 2010, the total number of PCs infected with some form of crimeware was 9,215,692
- Payments services continues to be most targeted sector by fraudsters in 2009 and Q1 and Q2 of 2010

Sources : : http://www.pcworld.com/article/186037/25_million_strains_of_malware_identified_in_2009.html
<http://www.apwg.org/>
<http://www.symantec.com> – April 2010 Internet Threat Report

Fraudsters

The fraud is carried out when the “fraudster” creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through ACH or Wire that are directed to the bank accounts of willing or unwitting individuals often within a couple days or even hours.

¹Keystroke logging (often called keylogging) is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

Who's watching your online activity?



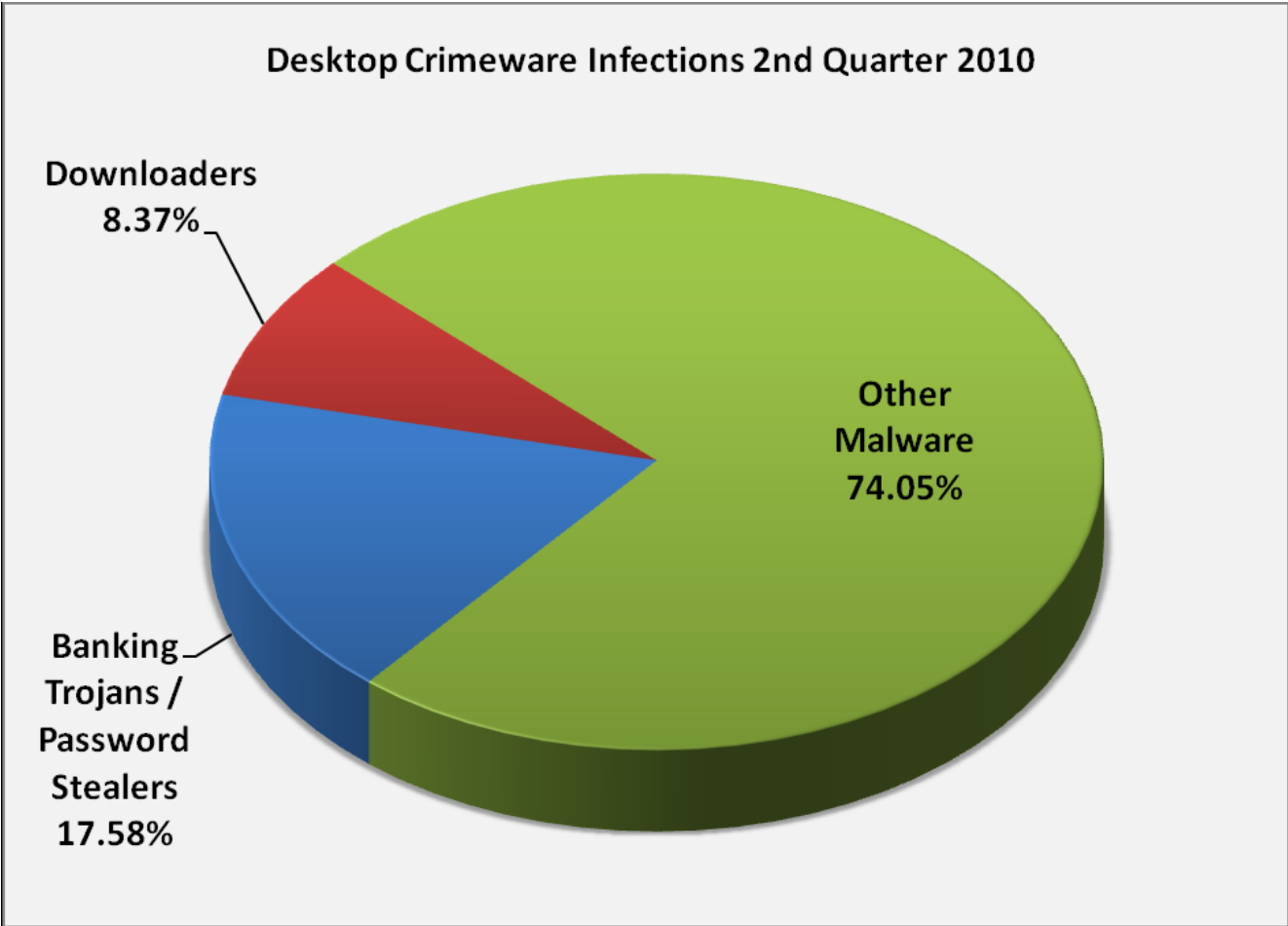
**logons
credit cards
purchases
passwords
bank accounts
retirement accounts
\$management
insurance policies**

Key-loggers

How the Fraud Works

- Business' PC is the weak link in the security chain
- Fraudsters recruit “money mules” to move funds
- Hackers secretly record keystrokes on PC and in some cases relay to fraudsters in real-time
- Once credentials are compromised, hackers use stolen authentication data to perform unauthorized transactions
- Current version of crimeware may be able to defeat some traditional anti-virus and firewalls

Crimeware Infections by the Numbers



Crimeware Infection - Spear Phishing



Fake Anti-Virus Scam

Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
W32.Pykspa.F	FontData.fdb
Trojan.Spyeye	nbio412.sys
W32.Daprosy	corelpf.lrs
Trojan.Bankpatch.D	desktop.ini
Trojan.Vundolgen5	d3d8.dll

Remove all **Cancel**

WARNING

Name	Type	Threat level
W32.Pykspa.F	Virus	High
Trojan.Spyeye	Virus	Medium
W32.Daprosy	Virus	Critical
Trojan.Bankpatch.D	Virus	Medium
Trojan.Vundolgen5	Virus	Critical

Recommend: Click "Start Protection" button to erase all threats

Start Protection

Drive by Download – BlackHat SEO

[The Beijing Olympic Games Wallpaper - Free Sports Desktop Wallpapers](#)

Aug 18, 2006 ... Three Concepts Have Been Adopted For The Beijing Olympic Games, Namely, The Green Olympics, The High-Tech Olympics...

[www.flash-screen.com/.../Sports Wallpapers](#) - [Cached](#) - [Similar](#)

[Olympic Wallpapers - Free Sports Desktop Wallpapers](#)

Aug 14, 2008 ... The Olympic Games (Often Referred To Simply As The Olympics Or The Games) Is An International Multi-Sport Event...

[www.flash-screen.com/.../Sports Wallpapers](#) - [Cached](#) - [Similar](#)

[+ Show more results from www.flash-screen.com](#)

[Summer Olympics Photos, Olympic History Wallpapers, Download ...](#)

See photos of historical moments at the Olympic Summer Games and download free desktop **wallpapers** from National Geographic.

[photography.nationalgeographic.com/.../olympics-history-gallery.html](#) - [Cached](#) - [Similar](#)

[Vancouver 2010 Winter Olympic Wallpapers - The Petition Site](#)

The Vancouver 2010 , Winter Olympic games will be held in Vancouver from Feb 12-28, 2010 Games in this...

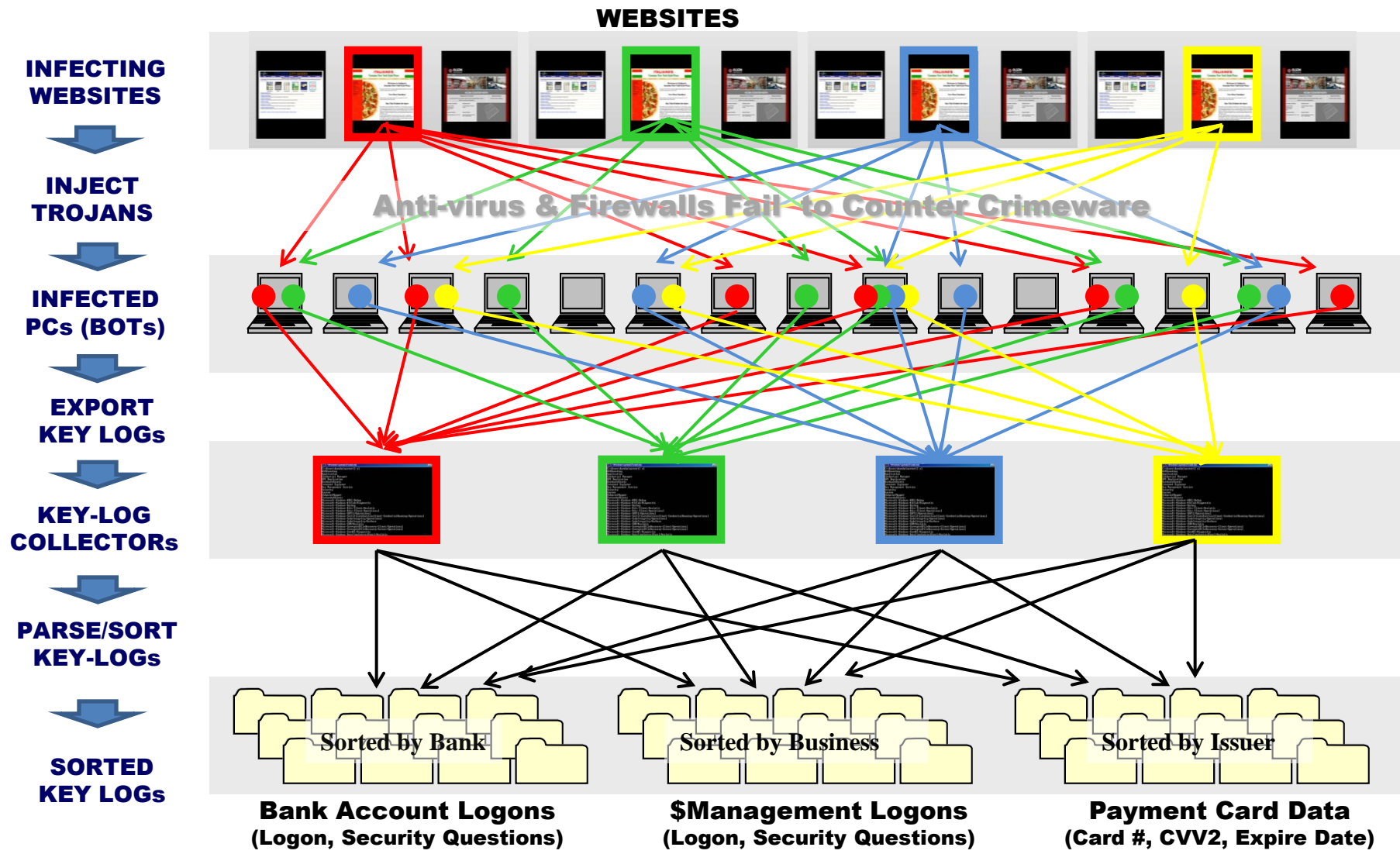
[www.thepetitionsite.com/.../vancouver-2010-winter-olympic-wallpapers](#) - [Cached](#)

[Olympic Games Wallpapers](#)

Olympic Games section at myWallpapers showing you **wallpapers**, images, news and informations which you can setup on your computer desktop.

[www.mywallpapers.com/.../olympic-games.php](#) - [Cached](#) - [Similar](#)

“Crimeware Data Harvesting”



Understanding Crimeware?

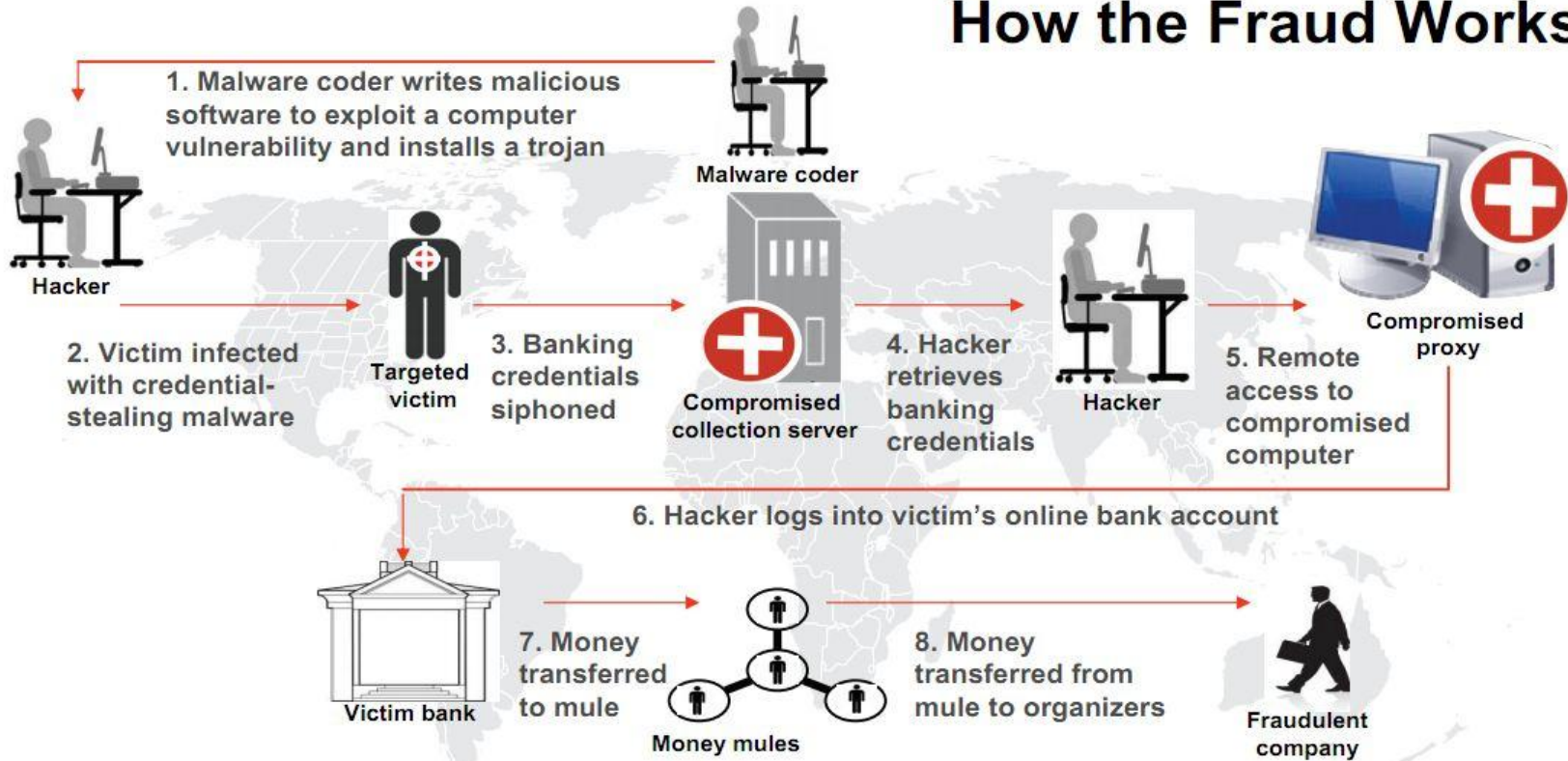
- Crimeware is a **highly-sophisticated piece of software** built to perform mass credential and information theft
- Crimeware can act like a virus, but has advanced features: trojan horse, keystroke logging, remote control, screen capture, instant messaging.
- Machine infected with Crimeware is “owned” by fraudsters and can be used to steal customer log-on and account information and any data on system.
- Zeus, Clampi, Gozi, Spynet: - Fast-growing family of crimeware in use today by organized crime rings

How Fraud with Zeus Crimeware Works

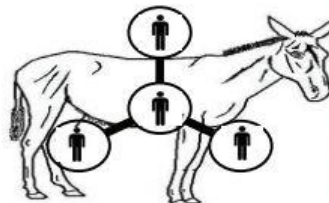
- Client PC is infected with crimeware by either e-mail or web browsing vector
- Fraudsters recruit “money mules” to move stolen funds via work at home scams
- Hackers use Zeus to record keystrokes (usernames/passwords) on victim PC and gather stolen information to logon on as the victim
- Using stolen credentials, hackers perform unauthorized transactions and send funds to mules
- Mules withdraw funds and send to “company” they are working for, keeping portion for service.

Corporate Account Takeover Fraud

How the Fraud Works



Victims are both financial institutions and owners of infected machines.



Money mules transfer stolen money for criminals, shaving a small percentage for themselves.



Criminals come in many forms:

- Malware coder
- Malware exploiters
- Mule organization

Full-Service Money Mule Website



Hi Log out

HOME AGENTS AWARDS SOLUTIONS CONTACT US

Best Performance



DIVISION MANAGER
Lance S. Turner



TEAM LEADER OF THE QUARTER
Shelly D. Daniels



AGENT OF THE QUARTER
Jessica L. Howard

Online Support Notifier

Private Messages
no new

Support Mailbox

Agent Preparation

Agent Prep

1:17 / 1:59

Agent Preparation consists of a video that will assist you with your upcoming order. Above you will see the Agent Preparation video. Be sure to "Pause" the video when necessary and listen to it as many times as you need to. If you are not able to view the above video in your browser, please notify Management via the Check-In form on the website.

Agent Appreciation



We take great pride in acknowledging and honoring our agents with the recognition they deserve. This process motivates junior agents to excel in the same manner.

Staff Notice



All hands staff meeting will take place twice daily. Current meeting times are start of business and close of business each day. Staff should ensure at least one of their team members are present at both meetings.

Agent Notice



All Senior Agents interested in the upcoming TeamLeader position should be sure to get with their Division Manager to submit the TLA.



How to Help Your Clients Protect Their Businesses

- Ensure internal staff is aware of the best practices in the industry – provide your client's with M&T's "Payment Fraud and Risk Management" Handout that will be posted to the VSCPA's website
- Be aware what your banking sites normally look like
- Run **up-to-date** Anti-Virus/Spyware
- Run **up-to-date** host based firewall software
- Patch third-party software – Adobe, Java, Quicktime
- Activate a "pop-up" blocker on Internet browsers to help prevent web-based intrusions

How to Help Your Clients Protect Their Businesses, Con't.

- Review your credit report/banking transactions regularly
- Use various ACH and Check Payment Filter and/or Block services
- Limit staff Administrative access to privileges on the PC and bank products used to conduct transactional activity
- Use a stand-alone PC for banking transactions
- Add Dual Administration for information reporting to reduce internal fraud with better control over user permissions
- If you accept credit/debit card payments, become and remain compliant with Payment Card Industry standards

Business Fraud Prevention & Risk Reduction Checklist

Customer Fraud Prevention and Risk Reduction Checklist	
	Paper
<input type="radio"/>	<input checked="" type="checkbox"/> Train accounting employees and staff to understand the risk of payment fraud and the steps they can take to reduce fraud
	<input checked="" type="checkbox"/> Separate financial and administrative duties - ensure the staff who make check, ACH and other payments are not the same people who reconcile bank accounts and confirm accurate payments
	<input checked="" type="checkbox"/> Implement policies and restrictions for establishing new bank accounts, check signing, ACH and wire authorizations; use dual review/authorization where possible
	<input checked="" type="checkbox"/> Mail checks from the post office and not from a location where others would have the opportunity to steal a check while it is waiting for postal pickup
	<input checked="" type="checkbox"/> Create a policy for handling check fraud - notify the Bank, close the account, destroy old check stock, notify unpaid payees, issue new checks, perform periodic audits to ensure no further fraud has occurred
	<input checked="" type="checkbox"/> Secure check stock, deposit slips, bank statements, cancelled checks and other types of payment identification so unauthorized personnel cannot access account number information
	<input checked="" type="checkbox"/> Review daily balances and checks clearing through your bank's information reporting tools, reconcile your check disbursements and deposits when you receive your bank statement
	<input checked="" type="checkbox"/> Avoid using a rubber stamp for check signatures as the stamps are easily stolen or copied
<input type="radio"/>	<input checked="" type="checkbox"/> Never publish the signature of your authorized check signer on the Internet or in your annual report

Fraud Risks and Solutions

Liability for Payment Fraud

- Uniform Commercial Code (UCC) for Checks
 - The laws governing who takes the loss for check fraud are complex and liability will often depend on the factual context in which the check fraud arose. As such, a client cannot assume its bank or some other party will ultimately be responsible for the loss
 - Clients are required by both applicable law and their account agreement with their bank to examine their bank statements and to provide prompt notification of any fraudulent payments
 - Failure to examine bank statements and promptly report fraudulent activity may greatly increase a customer's exposure to potential losses
- NACHA Rules for ACH
 - Clients that fail to closely monitor and report suspected fraudulent activity on their accounts are at risk of sustaining financial losses

Fraud Risks and Solutions

Business Best Practices

- Check Fraud – You should utilize bank Positive Pay products that allow you to verify and confirm checks as they are being presented against your client's account. This can...
 - assure only correct suppliers, payroll, taxes, etc. payments are made
 - Help avoid losses and lost administrative time resulting from the payment of a fraudulent check. Why not try to reduce the risk that you will sustain a loss of \$5,000 or \$50,000 or \$500,000 due to a fraudulent check?
- ACH Fraud – You should verify and confirm questionable ACH debits that are presented against your accounts
 - Receivers of corporate ACH debits should report unauthorized ACH debits as soon as possible
 - 48 hours

Fraud Risks and Solutions

Protection Solutions

- Payee Positive Pay Reporting – Allows you to review a daily report of any “suspicious checks” and make an educated ‘Pay’ or ‘No Pay’ decision
- Check Block – Automatically returns ALL checks presented against your account
- ACH Debit Review Reject Report – With ACH Debit Review Level II, you can identify unauthorized rejected ACH debits
- ACH Debit Reporting – You can monitor ACH debits on the Previous Day Detail Reporting so that you can identify any unauthorized debits quickly
- ACH UPIC Protection – A unique number assigned to a commercial checking account that “masks” the true bank account information for protection. You can distribute the UPIC payment information to vendors and other parties that make ACH payments to your account
- Dynamic (Secondary) Approvals – With Positive Pay service, you may require two users to approve final payment of suspect items; with ACH payment origination service, you can require up to five users to approve each ACH transaction

Contact Information

Carl L. Hairston
Regional Manager, Capital Region
202.434.7026
chairston@mtb.com

Rich Sobonya
Relationship Manager, Capital Region
703.519.2880
rsobonya@mtb.com

Q&A Period

Useful Links:

browsercheck.qualys.com

www.ic3.gov

