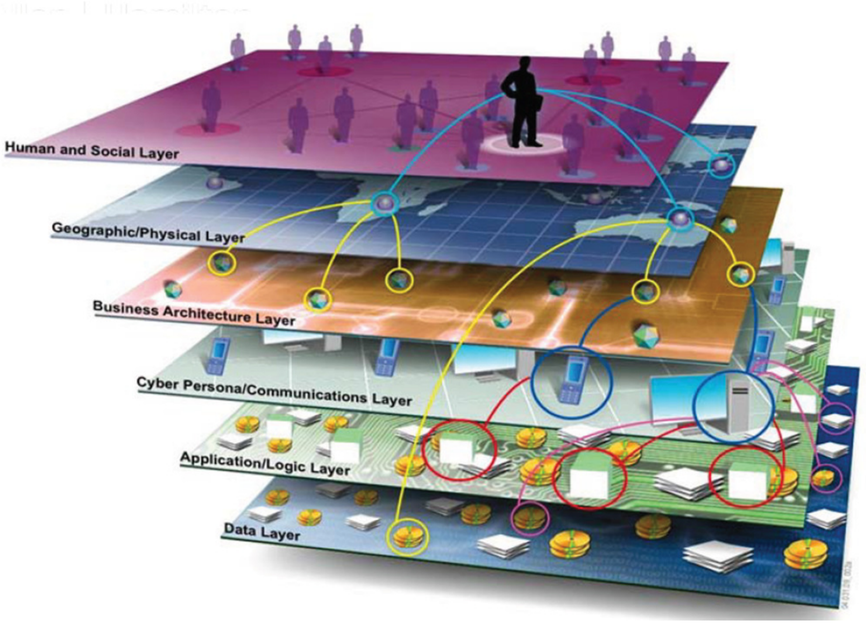
FIRMA
SECURITY PRESENTATION

Matthew Speare
SVP, Information Technology
M & T Bank

Layers of Security

Attacks against financial institutions and our customers can originate from multiple levels with differing attack vectors


Human and Social Layer
Geographic/Physical Layer
Business Architecture Layer
Cyber Persona/Communications Layer
Application/Logic Layer
Data Layer

Layer	Description
Human & Social	The science of Human Behavior and the propensity to commit crimes
Physical	The geographic and physical proximity which allow crime and fraud to be perpetrated
Business Architecture	The flaws in business processes which allow for a vulnerability to be exploited
Cyber Personal Communications	The plethora of devices and networks which provide a potential vector for exploit
Application Logic	The manner in which applications process and validate information which often leads to unintentional vulnerabilities
Data	Non-public personal and corporate financial information which can be leveraged for direct or indirect exploitation of customer finance

Federal Regulation, International Standards, and Association Guidelines

Security Layer	Corresponding Guidance
Human & Social	• Regulation H* • Sarbanes–Oxley Act
Physical	• Regulation H* • Payment Cards Industry Data Security Standards (PCI-DSS) • ISO 27001
Business Architecture	• ISO 27001
Cyber Personal Communications	• Federal Financial Institutions Examination Council (FFIEC)
Application Logic	• Gramm-Leach Bliley Act (GLBA)* • Federal Financial Institutions Examination Council (FFIEC) • Payment Cards Industry Data Security Standards (PCI-DSS) • ISO 27001
Data	• Regulation P • Gramm-Leach Bliley Act (GLBA)* • Federal Financial Institutions Examination Council (FFIEC) • Payment Cards Industry Data Security Standards (PCI-DSS) • ISO 27001

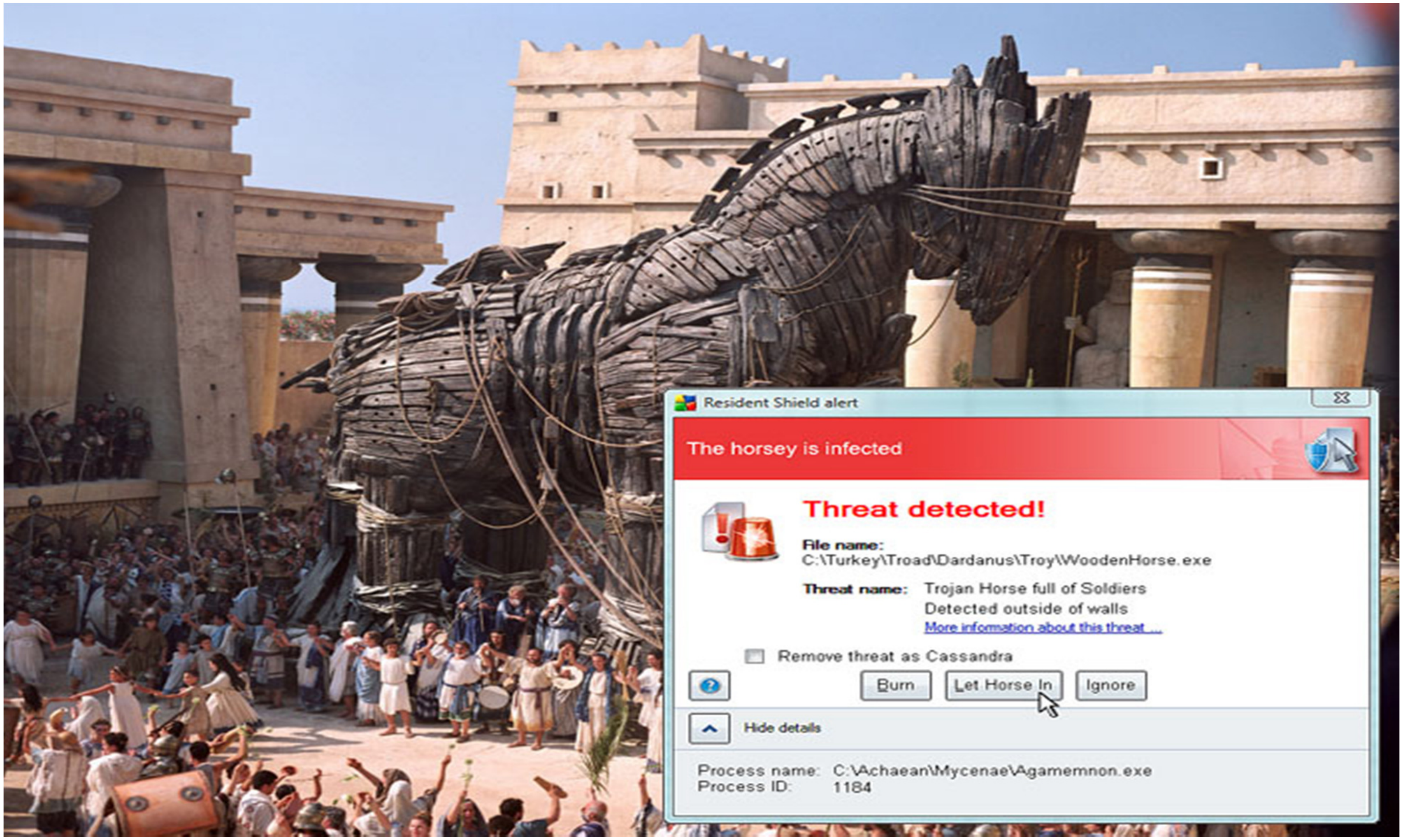
* Board oversight required

Security threats are continually evolving

Security Layer	Traditional Risks	Emerging Risks
Human & Social	• Someone calling branch pretending to be someone they are not	• Individuals signing up for "work from home" scams, but are really becoming "money mules"
Physical	• ATM Skimming	• ATM brute force attacks
Business Architecture	• Employee Misconduct	• Reconnaissance of Business Processes
Cyber Personal Communications	• Phishing E-mails • Virus' on PC's	• Hacker Collectives • Key Stroke Loggers • Multi-faceted attacks targeted to confuse/distract the banks • Proliferation of mobile devices provide new attack channels
Application Logic	• Attacks against database vulnerabilities in applications	• Denial of Service attacks against platforms
Data	• Credit Card Data used to conduct fraudulent transactions	• Personal identity information stolen and used to make fraudulent loans

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

Drawing some relevant correlations



Resident Shield alert

The horsey is infected

Threat detected!

File name:
C:\Turkey\Troad\Dardanus\Troy\WoodenHorse.exe

Threat name: Trojan Horse full of Soldiers
Detected outside of walls
More information about this threat ...

□ Remove threat as Cassandra

Process name: C:\Achaean\Mycenae\Agamemnon.exe
Process ID: 1184

Internet fraud is big business

- Heartland Payment Systems - 130 million cards

- RBS WorldPay - $9 million in 12 hours from 2,100 ATMs in 280 cities worldwide

- The Internet Crime Complaint Center 2011 annual report approximately 304,000 complaints relating to Internet fraud were filed in 2010.

- The risk to Critical National Infrastructure is real:
    - **“America's economic prosperity in the 21st century will depend on cyber security,” President Barack Obama**

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

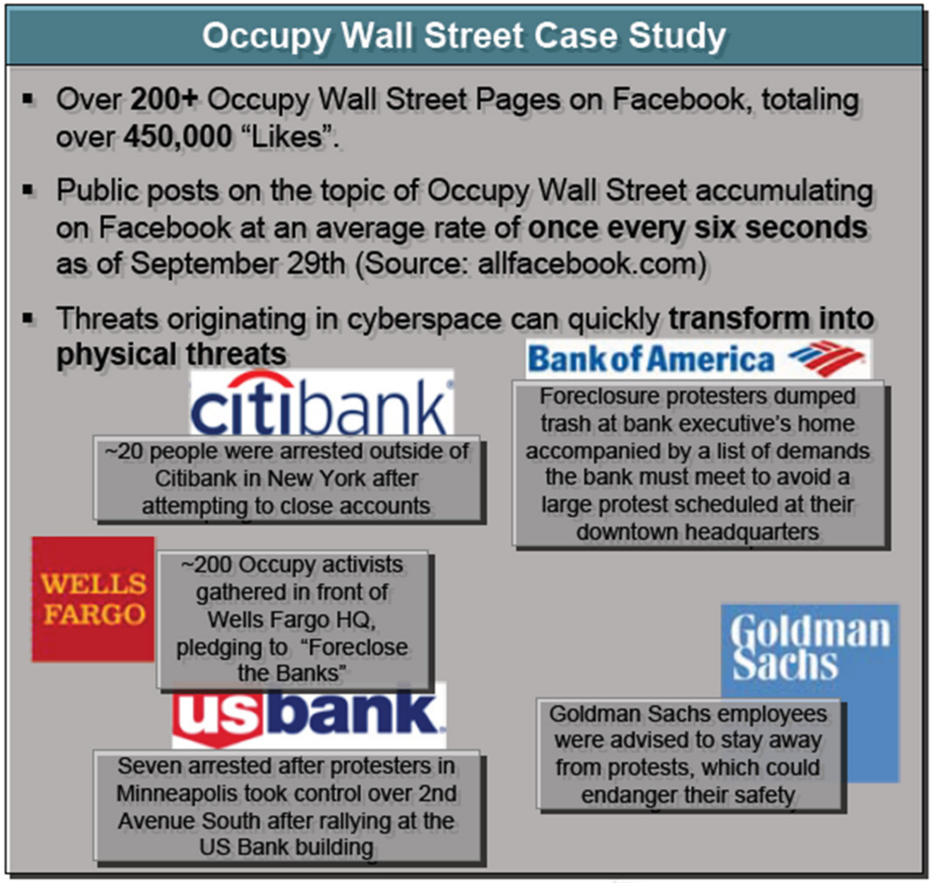
Began: Mid 2000s – evolving.

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.

Cyber Threats directed at Financial Services Industry



Occupy Wall Street Case Study

- Over **200+** Occupy Wall Street Pages on Facebook, totaling over **450,000** “Likes”.
- Public posts on the topic of Occupy Wall Street accumulating on Facebook at an average rate of **once every six seconds** as of September 29th (Source: allfacebook.com)
- Threats originating in cyberspace can quickly **transform into physical threats**

~20 people were arrested outside of Citibank in New York after attempting to close accounts

Foreclosure protesters dumped trash at bank executive’s home accompanied by a list of demands the bank must meet to avoid a large protest scheduled at their downtown headquarters

~200 Occupy activists gathered in front of Wells Fargo HQ, pledging to “Foreclose the Banks”

Seven arrested after protesters in Minneapolis took control over 2nd Avenue South after rallying at the US Bank building

Goldman Sachs employees were advised to stay away from protests, which could endanger their safety

Security is a Business Issue

- Effects Line of Business Profitability
- Failures Effect Customer Relationships

Rapidly Evolving Threats

- Hacker Collectives
- Business Process Knowledge
- Foreign Governments
- Global Coordination

Incident Response

- Internal Coordination
- Law Enforcement
- Industry Groups
- Vendor Partners

Emerging cyber threats direct at the financial services industry create enterprise risks

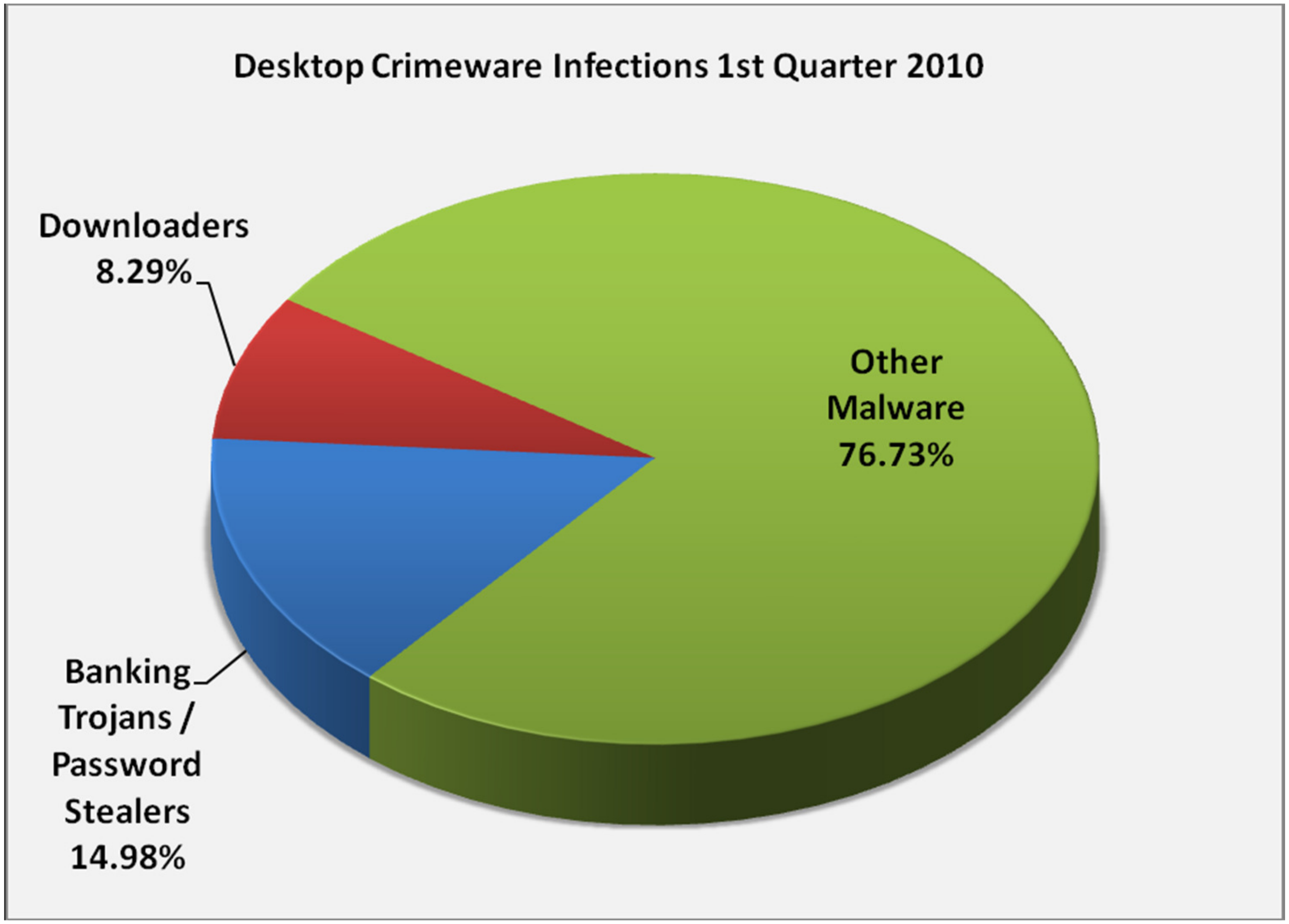
Physical Security
Fraud Prevention
Information Security

Fraudsters Continue to Target Business

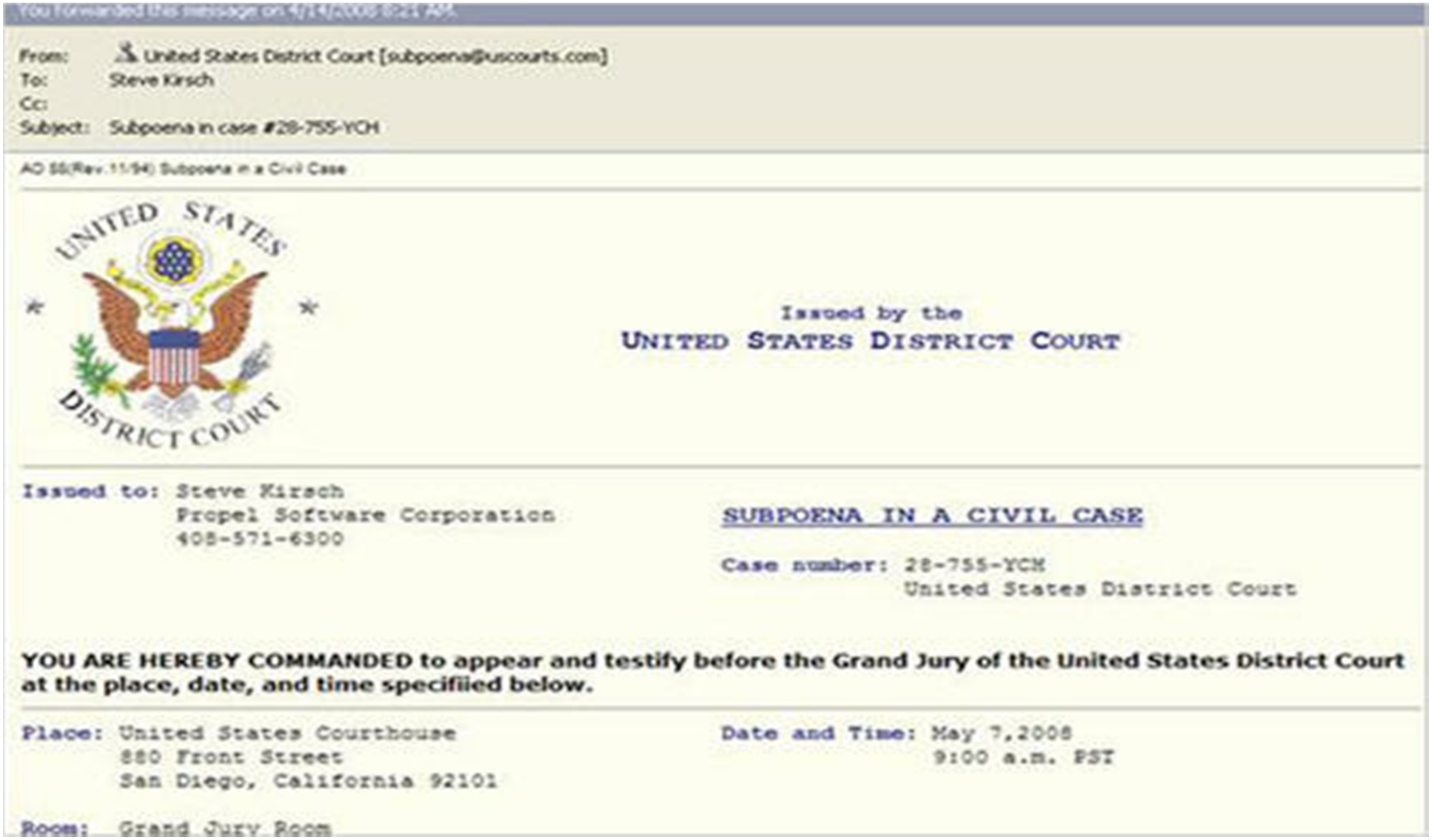
- Symantec indentified more than 90,000 unique versions of the Zeus/Zbot trojan crimeware in 2010 alone
- **There were more than *25 million new strains* of malware (crimeware) created in 2010**
- From Q4 2009 to Q1 2010, the total number of infected PCs grew from 10,305,805 to 11,384,640.
- Payments services continues to be most targeted sector by fraudsters in Q1, Q2 2009 and Q1, 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

Crimeware infections by the numbers



Crimeware infection - Spear phishing



You forwarded this message on 4/14/2008 8:21 AM.

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

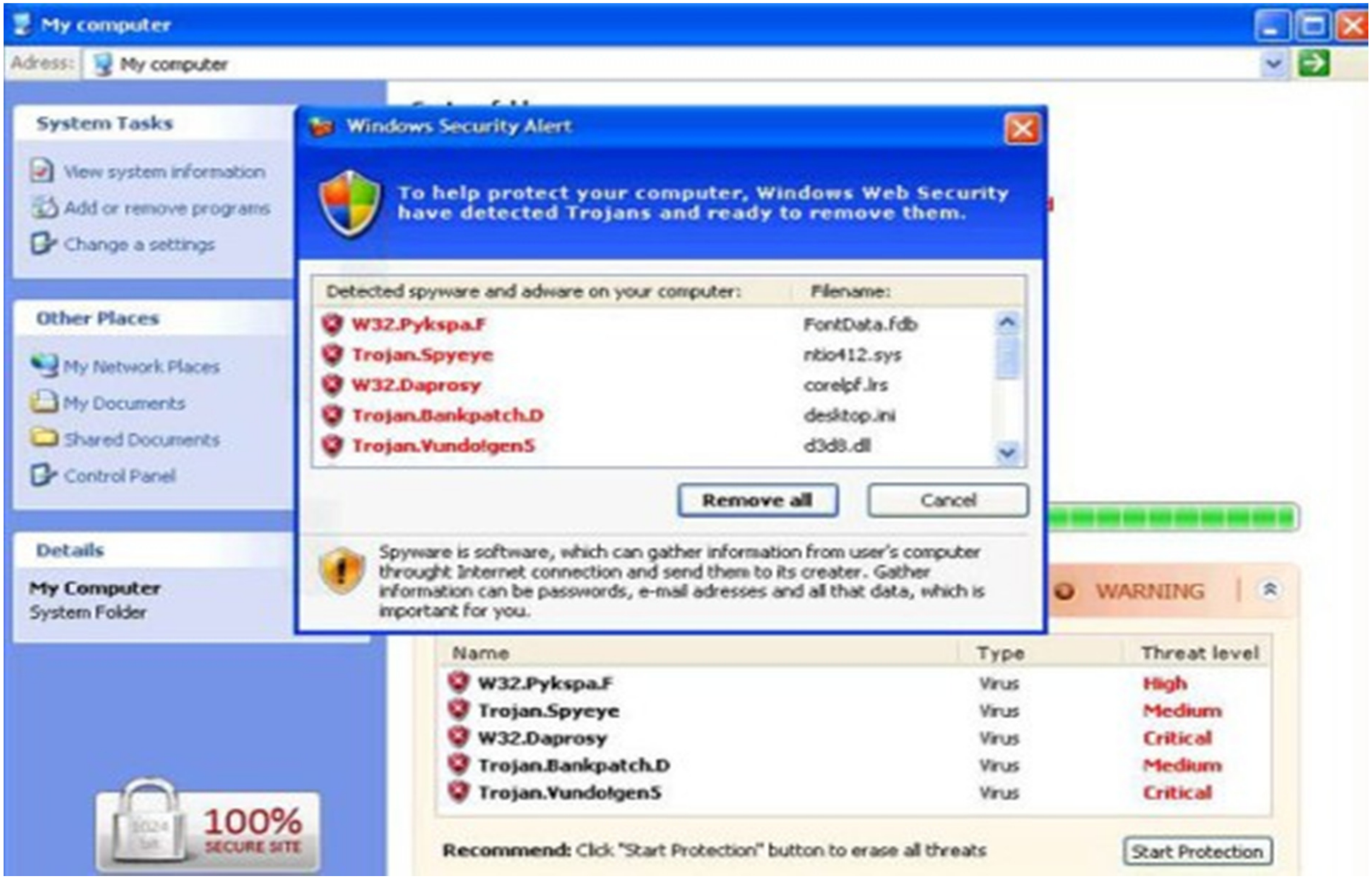
YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

Fake Anti-Virus Scam



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

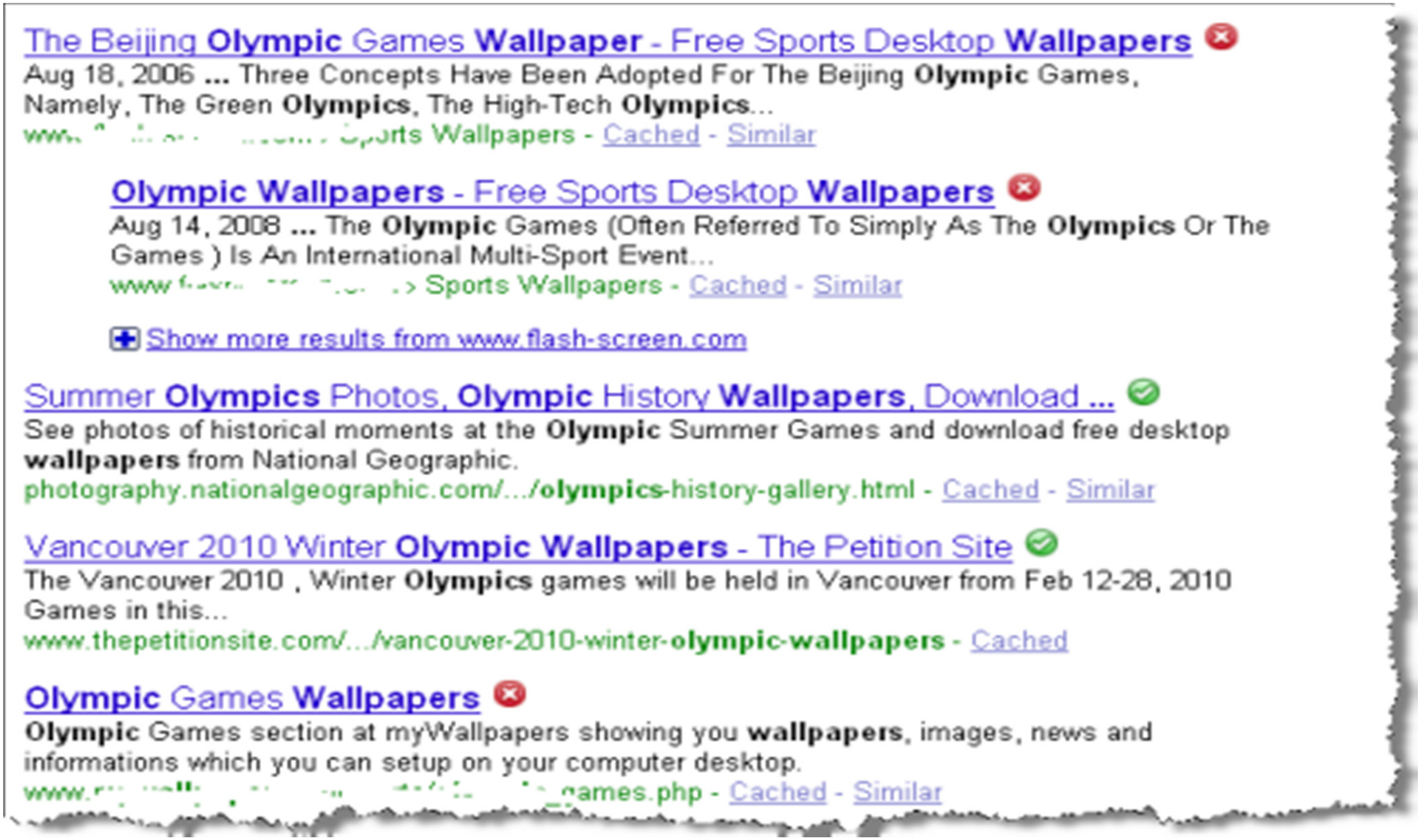
Detected spyware and adware on your computer:	Filename:
W32.Pykspa.F	FontData.fdb
Trojan.Spyeye	ntio412.sys
W32.Daprosy	corelpf.lrs
Trojan.Bankpatch.D	desktop.ini
Trojan.Vundo!gen5	d3d8.dll

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

Name	Type	Threat level
W32.Pykspa.F	Virus	High
Trojan.Spyeye	Virus	Medium
W32.Daprosy	Virus	Critical
Trojan.Bankpatch.D	Virus	Medium
Trojan.Vundo!gen5	Virus	Critical

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

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.[illegible] Sports Wallpapers - Cached - Similar

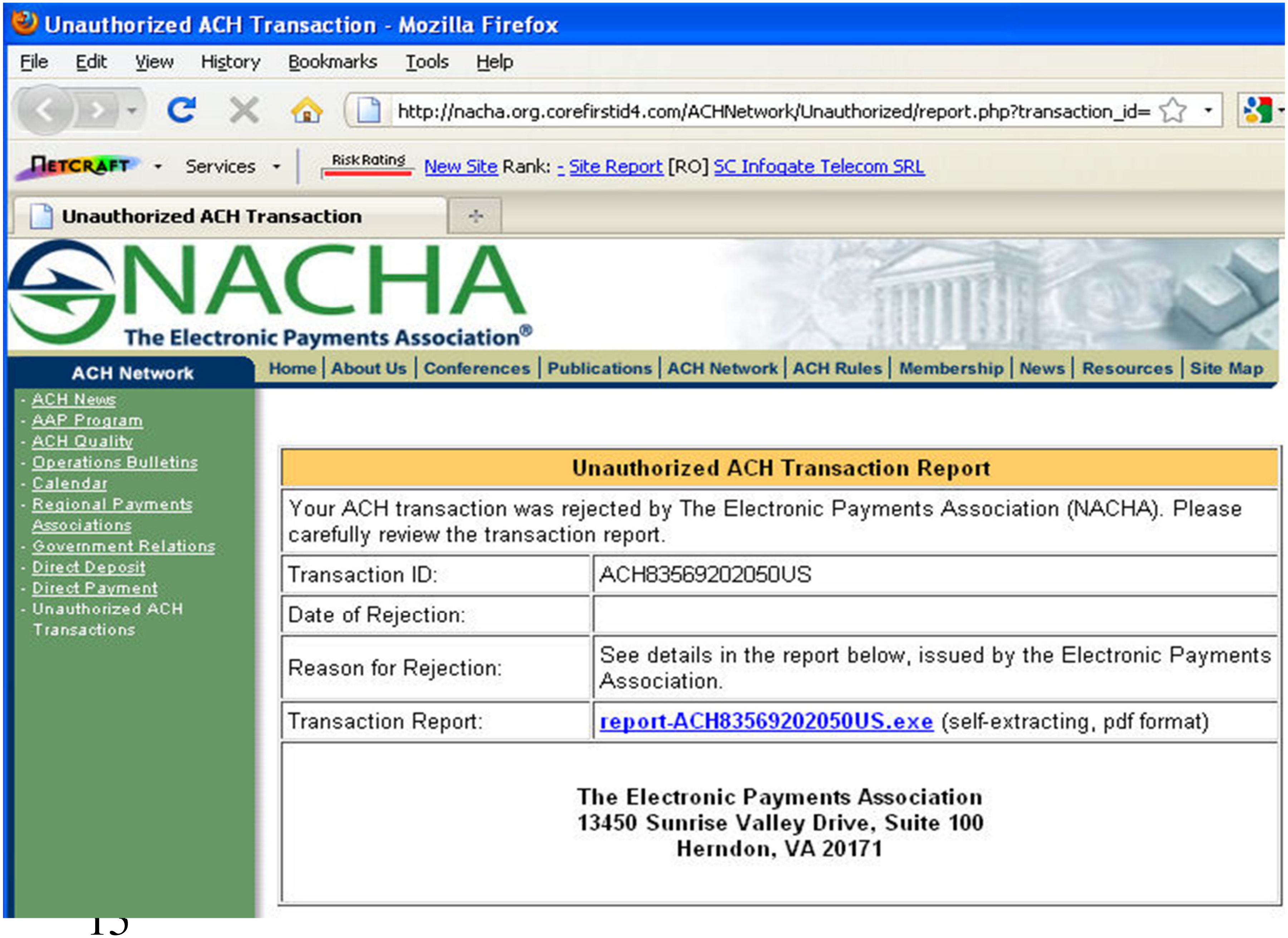
Olympic Wallpapers - Free Sports Desktop **Wallpapers** ✗
Aug 14, 2008 **...** The **Olympic** Games (Often Referred To Simply As The **Olympics** Or The Games) Is An International Multi-Sport Event...
www.[illegible] › Sports Wallpapers - Cached - Similar

⊞ 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 **Olympics** 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.[illegible]_games.php - Cached - Similar


Unauthorized ACH Transaction - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://nacha.org.corefirstid4.com/ACHNetwork/Unauthorized/report.php?transaction_id=
NETCRAFT
Services
Risk Rating
New Site Rank: - Site Report [RO] SC Infogate Telecom SRL
Unauthorized ACH Transaction
NACHA
The Electronic Payments Association®
ACH Network
Home
About Us
Conferences
Publications
ACH Network
ACH Rules
Membership
News
Resources
Site Map
- ACH News
- AAP Program
- ACH Quality
- Operations Bulletins
- Calendar
- Regional Payments Associations
- Government Relations
- Direct Deposit
- Direct Payment
- Unauthorized ACH Transactions

Unauthorized ACH Transaction Report

Your ACH transaction was rejected by The Electronic Payments Association (NACHA). Please carefully review the transaction report.

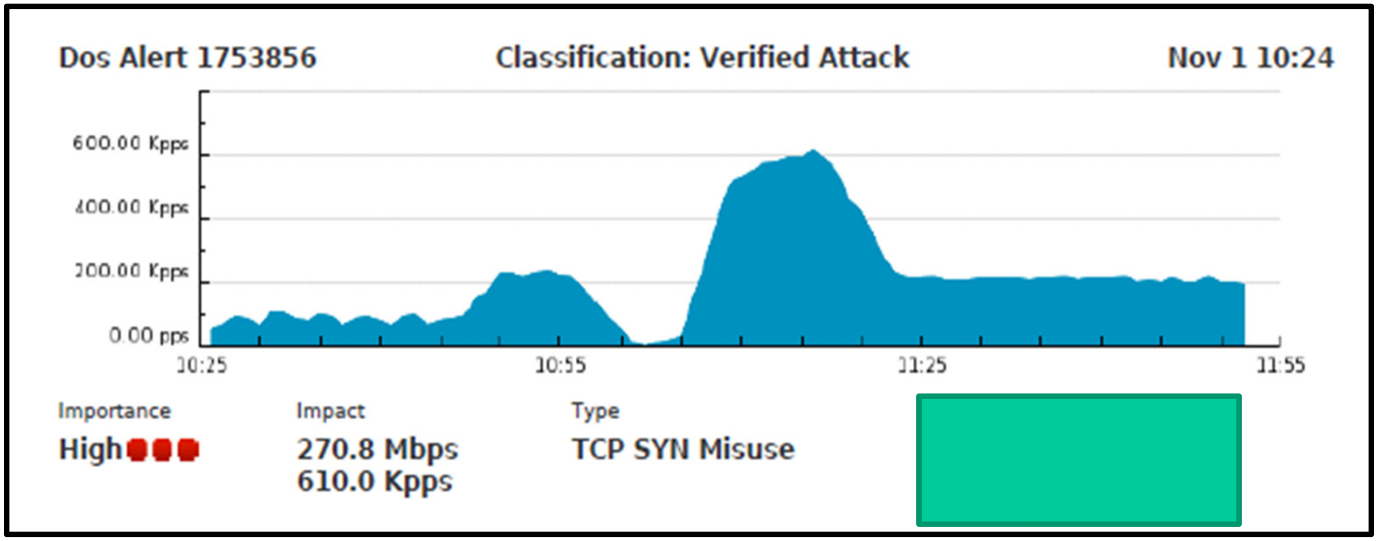
Transaction ID:	ACH83569202050US
Date of Rejection:	
Reason for Rejection:	See details in the report below, issued by the Electronic Payments Association.
Transaction Report:	report-ACH83569202050US.exe (self-extracting, pdf format)

The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, VA 20171

Cyber Attack Event

- During the 74 day period from August 20, 2011 until November 2, 2011, Bank A experienced **119** ($5.8MM) fraud attempts against Commercial customers as compared to **58** ($1.5MM) fraud attempts in all of 2010 and **13** ($.88MM) fraud attempts in 2009.

- During the coordinated fraud effort to cover the underlying Wire fraud attempt, Bank A experienced a Denial of Service attack consisting of > 46,000% increase in Internet traffic as compared to a typical business day.



Dos Alert 1753856 Classification: Verified Attack Nov 1 10:24

Importance
High ●●●

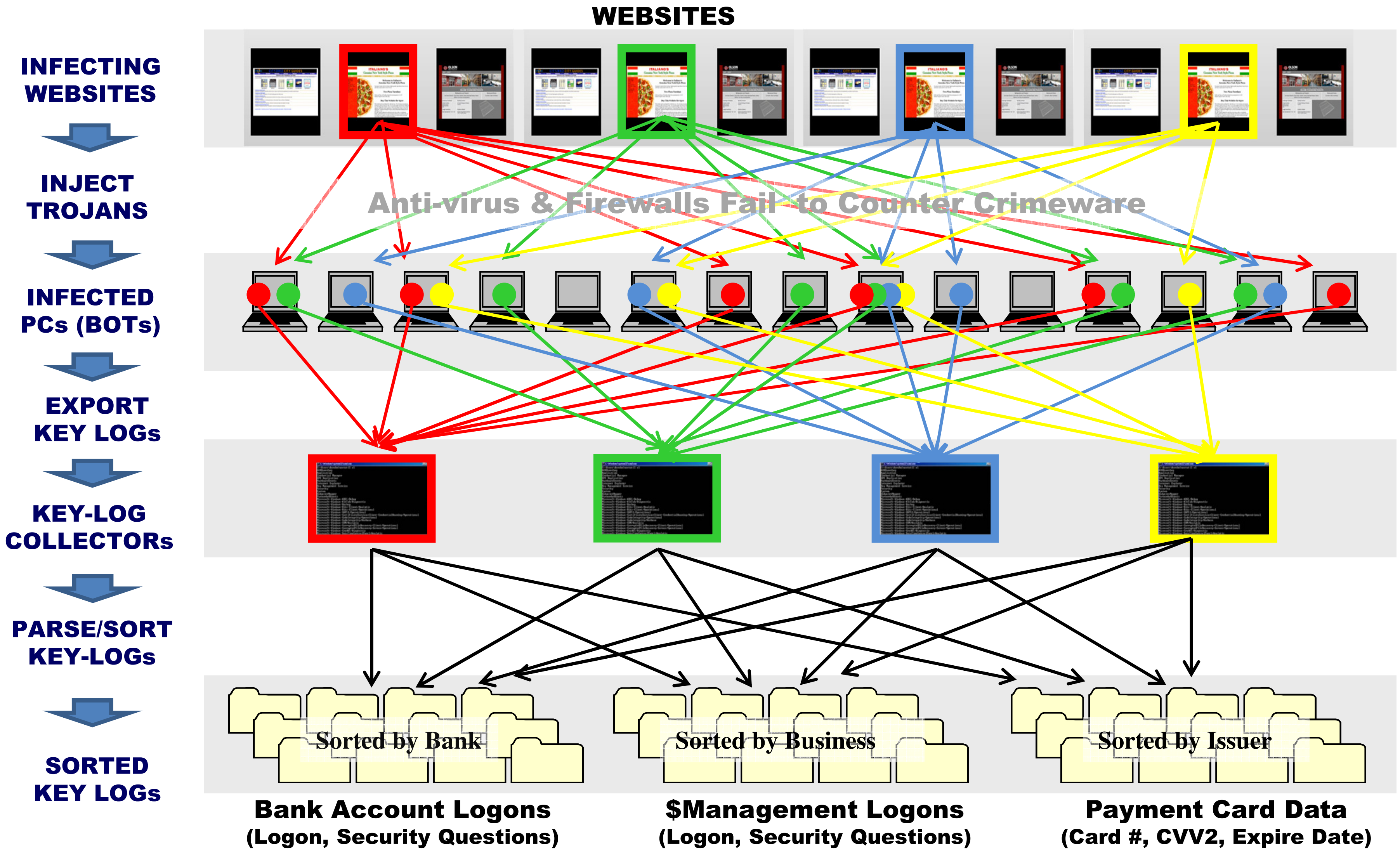
Impact
270.8 Mbps
610.0 Kpps

Type
TCP SYN Misuse

[redacted]

Physical Security → Fraud Prevention → Information Security

“Crimeware Data Harvesting”



WEBSITES

INFECTING WEBSITES

INJECT TROJANS

INFECTED PCs (BOTs)

EXPORT KEY LOGs

KEY-LOG COLLECTORs

PARSE/SORT KEY-LOGs

SORTED KEY LOGs

Anti-virus & Firewalls Fail to Counter Crimeware

Sorted by Bank

Sorted by Business

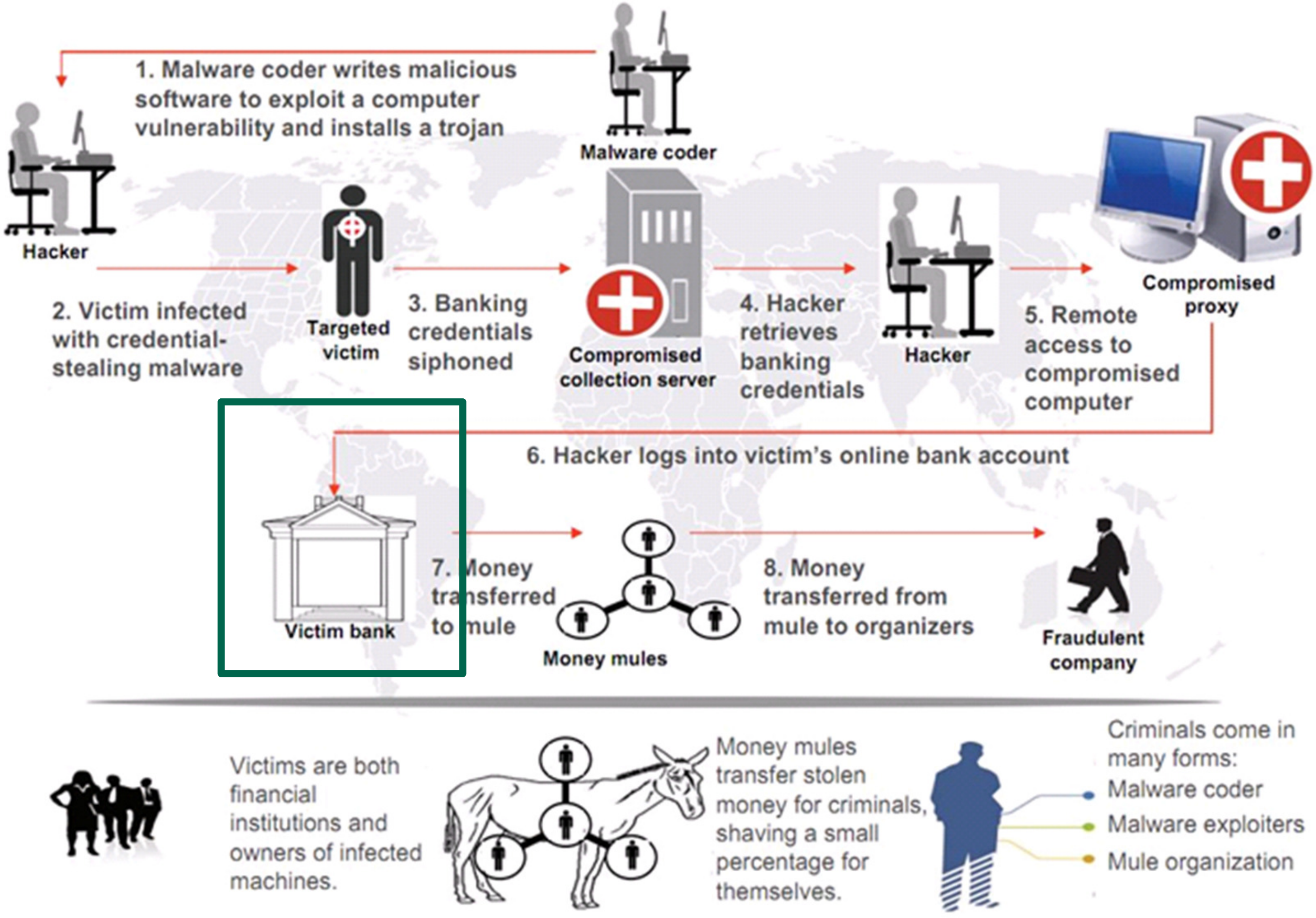
Sorted by Issuer

Bank Account Logons
(Logon, Security Questions)

$Management Logons
(Logon, Security Questions)

Payment Card Data
(Card #, CVV2, Expire Date)

How the Fraud Syndicate Works



1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan

Malware coder

Hacker

2. Victim infected with credential-stealing malware

Targeted victim

3. Banking credentials siphoned

Compromised collection server

4. Hacker retrieves banking credentials

Hacker

5. Remote access to compromised computer

Compromised proxy

6. Hacker logs into victim's online bank account

Victim bank

7. Money transferred to mule

Money mules

8. Money transferred from mule to organizers

Fraudulent company

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:

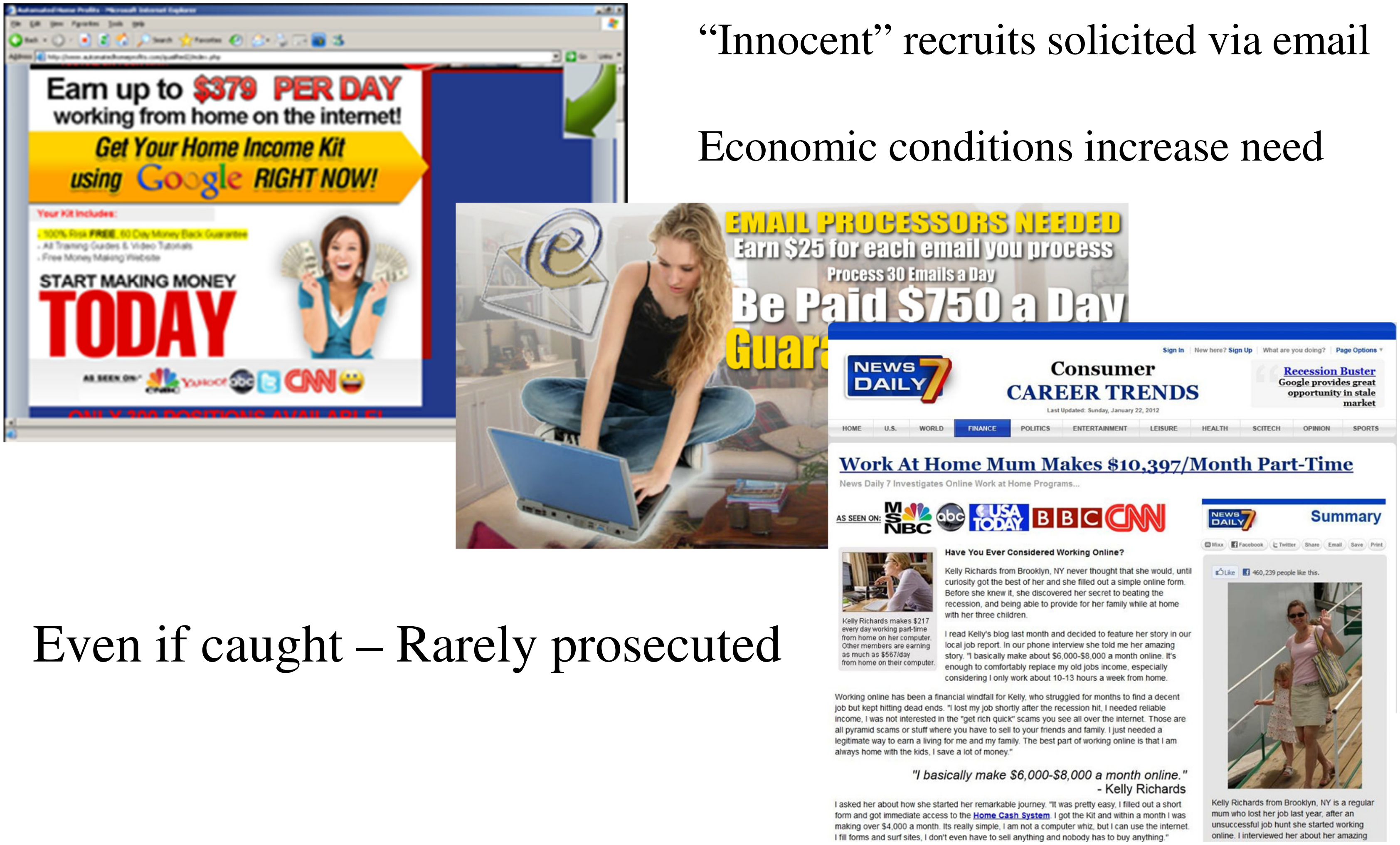
- Malware coder
- Malware exploiters
- Mule organization

Physical Security | Fraud Prevention | Information Security

Recruiting “Money Mules”

“Innocent” recruits solicited via email

Economic conditions increase need



Consumer
CAREER TRENDS

Last Updated: Sunday, January 22, 2012

Recession Buster
Google provides great opportunity in stale market

Work At Home Mum Makes $10,397/Month Part-Time

News Daily 7 Investigates Online Work at Home Programs...

Have You Ever Considered Working Online?

Kelly Richards makes $217 every day working part-time from home on her computer. Other members are earning as much as $567/day from home on their computer.

Kelly Richards from Brooklyn, NY never thought that she would, until curiosity got the best of her and she filled out a simple online form. Before she knew it, she discovered her secret to beating the recession, and being able to provide for her family while at home with her three children.

I read Kelly's blog last month and decided to feature her story in our local job report. In our phone interview she told me her amazing story. "I basically make about $6,000-$8,000 a month online. It's enough to comfortably replace my old jobs income, especially considering I only work about 10-13 hours a week from home.

Working online has been a financial windfall for Kelly, who struggled for months to find a decent job but kept hitting dead ends. "I lost my job shortly after the recession hit, I needed reliable income, I was not interested in the "get rich quick" scams you see all over the internet. Those are all pyramid scams or stuff where you have to sell to your friends and family. I just needed a legitimate way to earn a living for me and my family. The best part of working online is that I am always home with the kids, I save a lot of money."

"I basically make $6,000-$8,000 a month online."
- Kelly Richards

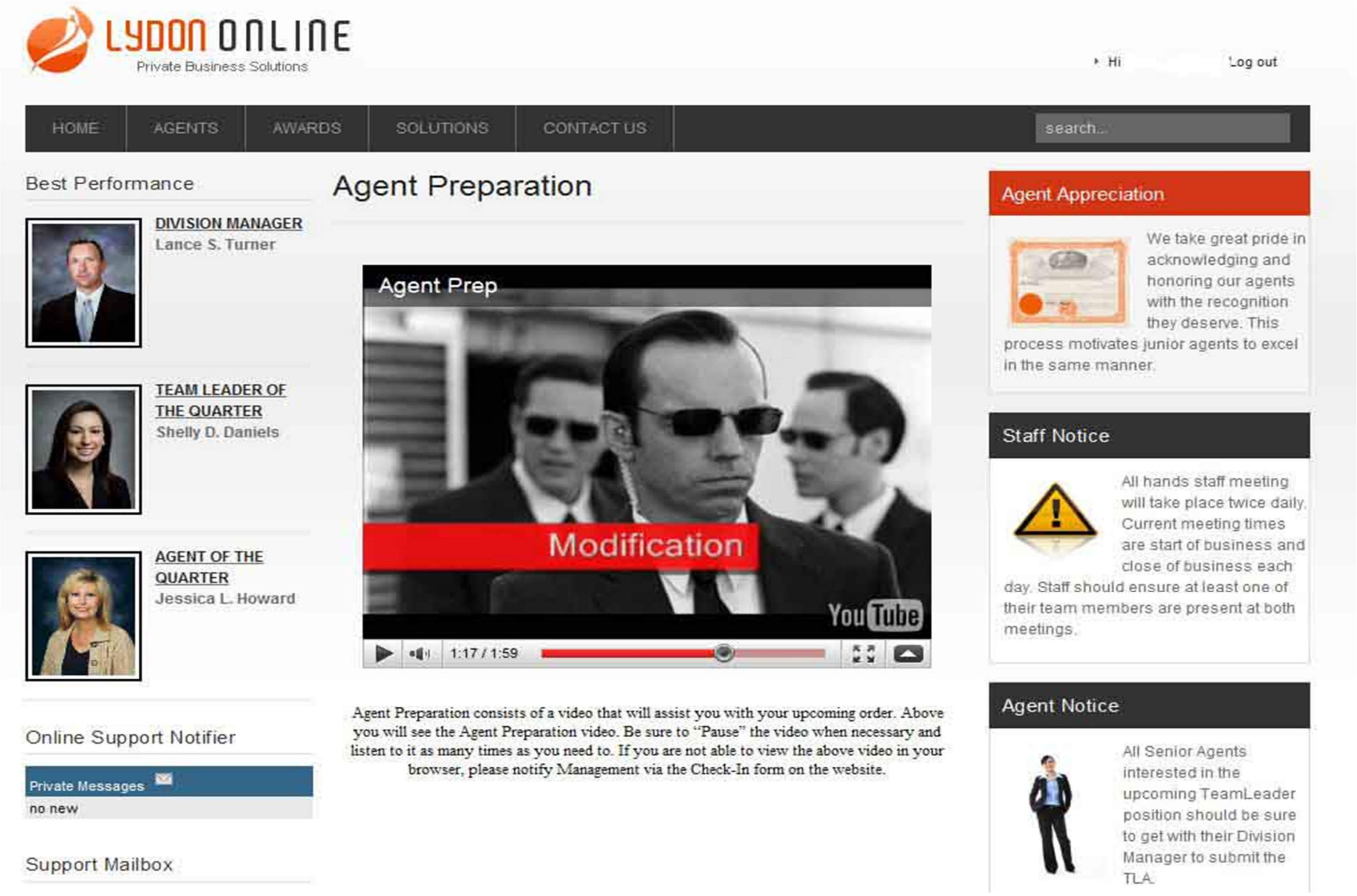
I asked her about how she started her remarkable journey. "It was pretty easy, I filled out a short form and got immediate access to the Home Cash System. I got the Kit and within a month I was making over $4,000 a month. Its really simple, I am not a computer whiz, but I can use the internet. I fill forms and surf sites, I don't even have to sell anything and nobody has to buy anything."

Kelly Richards from Brooklyn, NY is a regular mum who lost her job last year, after an unsuccessful job hunt she started working online. I interviewed her about her amazing

Even if caught – Rarely prosecuted

Physical Security → Fraud Prevention → Information Security

Full-service money mule website



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

Support Mailbox

Agent Preparation

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.

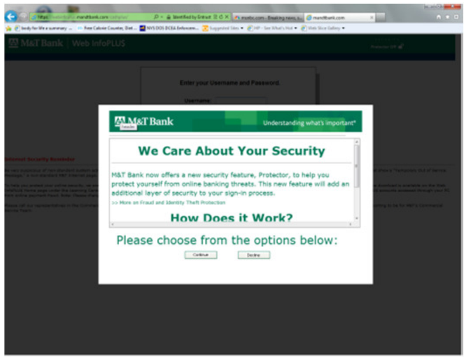
Agent Notice

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

Wire Fraud Prevention Efforts

People

- Customer Education and Awareness
  - Over 60 customer education events held in 2011
  - Online reminders for customers
- Internal Employee Education and Awareness
  - Annual Information Security Training
  - Targeted Commercial and Retail Bank communications
- Increase in staffing to monitor and conduct validation of Wire Transfers


M&T Bank | Web InfoPLU$
Enter your Username and Password.
Username:
M&T Bank
Understanding what's important®

We Care About Your Security

M&T Bank now offers a new security feature, Protector, to help you protect yourself from online banking threats. This new feature will add an additional layer of security to your sign-in process.

>> More on Fraud and Identity Theft Protection

How Does it Work?

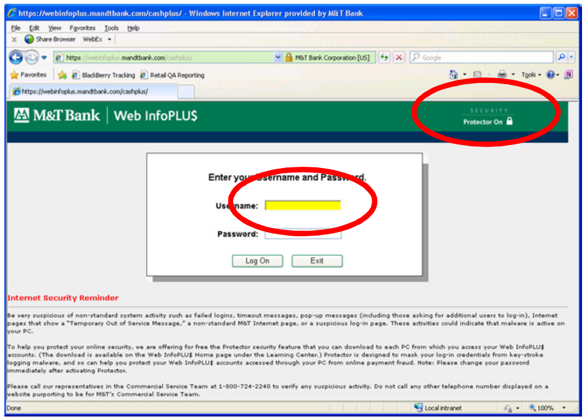
Please choose from the options below:

Processes

- Enhanced monitoring of Wire Transfers and ACH transactions
- Call back procedures for Wire Transfers and ACH transactions
- Escalation and Fraud Steering Committee Review

Technology

- Data Leak Prevention software implemented to enhance internal monitoring of appropriate data use
- Anti-Key Stroke Logger software implemented for WebInfoPlu$


https://webinfoplus.mandtbank.com/cashplus/ - Windows Internet Explorer provided by M&T Bank
File Edit View Favorites Tools Help
Share Browser WebEx
https://webinfoplus.mandtbank.com/cashplus/
M&T Bank Corporation [US]
Google
Favorites
BlackBerry Tracking
Retail QA Reporting
Tools
https://webinfoplus.mandtbank.com/cashplus/
M&T Bank | Web InfoPLU$
SECURITY
Protector On
Enter your Username and Password.
Username:
Password:
Log On
Exit
Done
Local intranet
100%

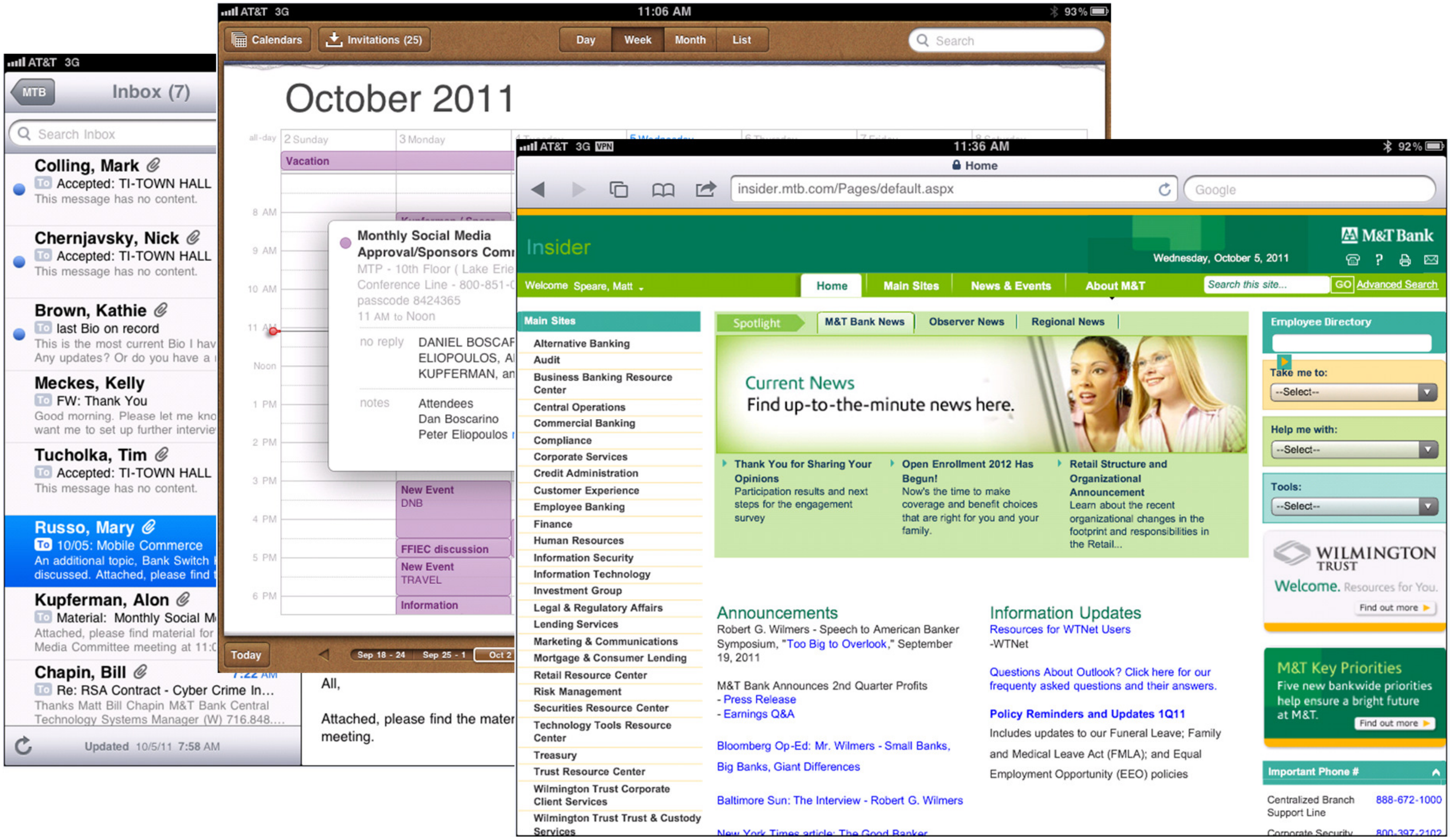
Internet Security Reminder

Be very suspicious of non-standard system activity such as failed logins, timeout messages, pop-up messages (including those asking for additional users to log-in), Internet pages that show a "Temporary Out of Service Message," a non-standard M&T Internet page, or a suspicious log-in page. These activities could indicate that malware is active on your PC.

To help you protect your online security, we are offering for free the Protector security feature that you can download to each PC from which you access your Web InfoPLU$ accounts. (The download is available on the Web InfoPLU$ Home page under the Learning Center.) Protector is designed to mask your log-in credentials from key-stroke logging malware, and so can help you protect your Web InfoPLU$ accounts accessed through your PC from online payment fraud. Note: Please change your password immediately after activating Protector.

Please call our representatives in the Commercial Service Team at 1-800-724-2240 to verify any suspicious activity. Do not call any other telephone number displayed on a website purporting to be for M&T's Commercial Service Team.

iPad/iPhone



Colling, Mark
To Accepted: TI-TOWN HALL
This message has no content.

Chernjavsky, Nick
To Accepted: TI-TOWN HALL
This message has no content.

Brown, Kathie
To last Bio on record
This is the most current Bio I hav
Any updates? Or do you have a

Meckes, Kelly
To FW: Thank You
Good morning. Please let me kno
want me to set up further intervie

Tucholka, Tim
To Accepted: TI-TOWN HALL
This message has no content.

Russo, Mary
To 10/05: Mobile Commerce
An additional topic, Bank Switch
discussed. Attached, please find

Kupferman, Alon
To Material: Monthly Social M
Attached, please find material for
Media Committee meeting at 11:0

Chapin, Bill 7:22 AM
To Re: RSA Contract - Cyber Crime In...
Thanks Matt Bill Chapin M&T Bank Central
Technology Systems Manager (W) 716.848....

Updated 10/5/11 7:58 AM

All,

Attached, please find the mater
meeting.

October 2011

Monthly Social Media
Approval/Sponsors Comi
MTP - 10th Floor (Lake Erie
Conference Line - 800-851-
passcode 8424365
11 AM to Noon

no reply DANIEL BOSCAR
ELIOPOULOS, A
KUPFERMAN, an

notes Attendees
Dan Boscarino
Peter Eliopoulos

Main Sites

- Alternative Banking
- Audit
- Business Banking Resource Center
- Central Operations
- Commercial Banking
- Compliance
- Corporate Services
- Credit Administration
- Customer Experience
- Employee Banking
- Finance
- Human Resources
- Information Security
- Information Technology
- Investment Group
- Legal & Regulatory Affairs
- Lending Services
- Marketing & Communications
- Mortgage & Consumer Lending
- Retail Resource Center
- Risk Management
- Securities Resource Center
- Technology Tools Resource Center
- Treasury
- Trust Resource Center
- Wilmington Trust Corporate Client Services
- Wilmington Trust Trust & Custody Services

Current News
Find up-to-the-minute news here.

Thank You for Sharing Your Opinions
Participation results and next steps for the engagement survey

Open Enrollment 2012 Has Begun!
Now's the time to make coverage and benefit choices that are right for you and your family.

Retail Structure and Organizational Announcement
Learn about the recent organizational changes in the footprint and responsibilities in the Retail...

Announcements

Robert G. Wilmers - Speech to American Banker Symposium, "Too Big to Overlook," September 19, 2011

M&T Bank Announces 2nd Quarter Profits
- Press Release
- Earnings Q&A

Bloomberg Op-Ed: Mr. Wilmers - Small Banks, Big Banks, Giant Differences

Baltimore Sun: The Interview - Robert G. Wilmers

New York Times article: The Good Banker

Information Updates

Resources for WTNet Users
-WTNet

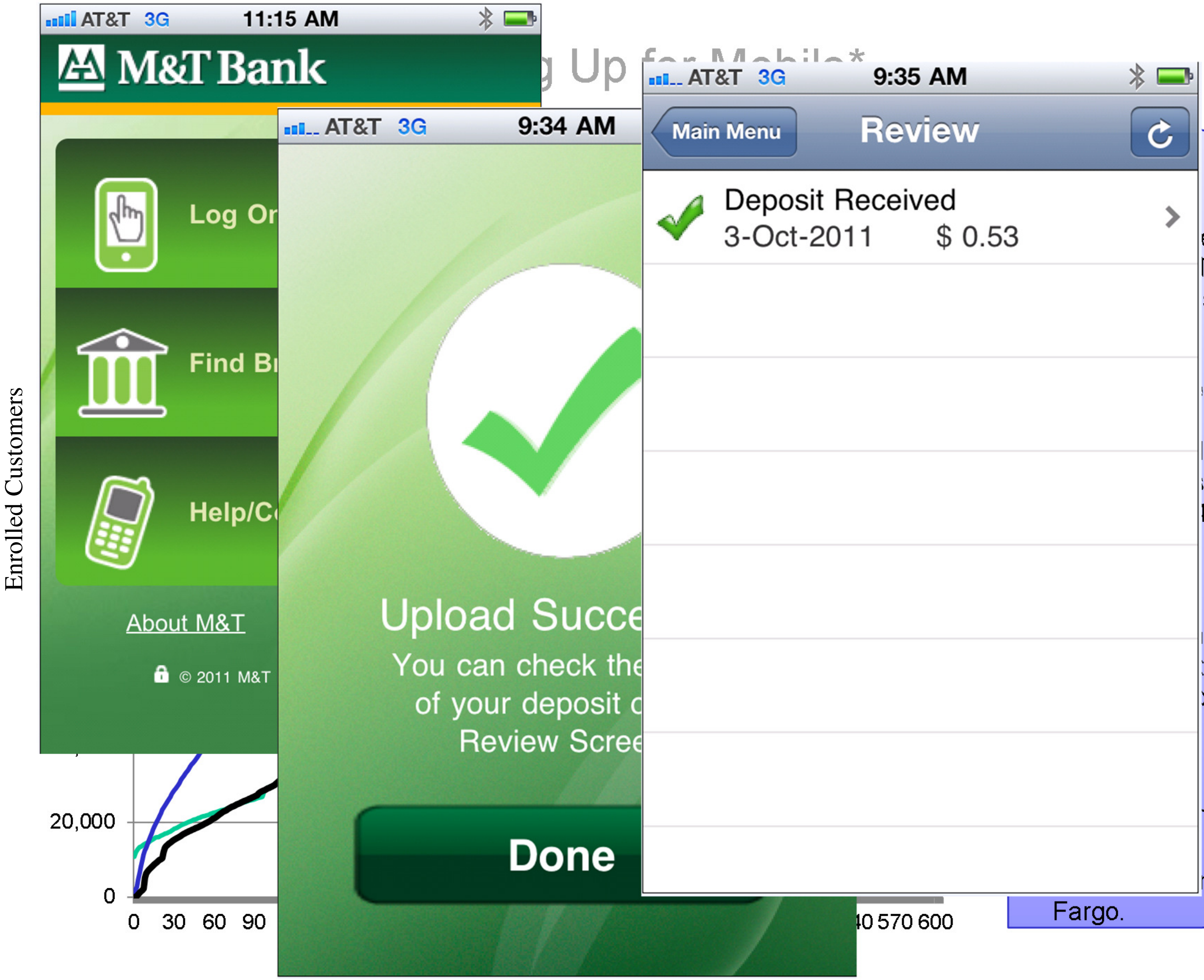
Questions About Outlook? Click here for our frequenty asked questions and their answers.

Policy Reminders and Updates 1Q11
Includes updates to our Funeral Leave; Family and Medical Leave Act (FMLA); and Equal Employment Opportunity (EEO) policies

Important Phone #

Centralized Branch Support Line	888-672-1000
Corporate Security	800-397-2102

g Up for Mobile*



Upload Succe

You can check the
of your deposit c
Review Scree

Deposit Received
3-Oct-2011 $ 0.53

Facts

every two
T gains a
ser.

and HSBC
mobile.

lobile Web
e an Apple
4% use a
access the

obile
take place on
or our App. A
had

T's app was a
load on
nd Wells
Fargo.

IT Risk Assessment

Severity	Very Low (<$50,000)	Low ($50,000-$250,000)	Moderate ($251,000-$1 million)	High ($1-5 million)	Critical (>$5 million)		Very Low (<$50,000)	Low ($50,000-$250,000)	Moderate ($251,000-$1 million)	High ($1-5 million)	Critical (>$5 million)
Probability	Inherent Risk						Residual Risk				
High (50-100%)	🟩	🟨	🟨 4	🟥 4	🟥 60		🟩	🟨	🟨	🟥	🟥
Medium (11-49%)	🟩	🟩 2	🟨 5	🟨 2	🟥 19		🟩	🟩	🟨	🟨	🟥
Low (0-10%)	🟩 7	🟩 8	🟩 3	🟨 1	🟥		🟩 7	🟩 10	🟩 12	🟨 7	🟥 79

Basel Category	Risk Count
Damage to Physical Assets	2
Business Disruption and System Failures	20
Execution, Delivery and Process Management	58
Internal Fraud	27
External Fraud Count	7
Clients, Products and Business Practices	1

Based upon Industry-Standard Measures
FFIEC Examination Booklets
Control Objectives for IT (CoBIT)
Sarbanes-Oxley Section 404
IT Infrastructure Library (ITIL)
ISO 17799/27001
Payment Card Industry DSS

Physical Security

Fraud Prevention

Information Security

Conclusion

- The current threat environment targets the personal computers, including customers and bank employees.

- Customers infect their computers by opening emails or visiting non-M&T Bank web sites with malware that embeds itself onto the customer's computers, unbeknownst to them (or the Bank). This malware can allow the criminals to assume the customer's identity and make attempts to process transactions ("man in the middle attacks").

- While technical solutions have come to market, few appear to provide a single guaranteed solution. As such, financial institutions have implemented layered security practices to help thwart fraudulent transactions from these malware account takeovers.

- Further adding to the challenge is that malware technologies continue to progress and adapt to changes in the marketplace at an astonishing speed.

- Organized crime is responsible for much of the cybercrime we encounter today. Organized crime breaks crime down into its component parts and outsources it to specialized technical teams. There are people who write the malware, people who deploy it, people who control and rent the botnets, people who receive goods bought with stolen credit cards, and people who do the money laundering.

- There are no silver bullets. An active monitoring and flexible incident response is fundamental to our defense.

> "Virtually every authentication technique can be compromised…"
> – FFIEC Supplemental Guidance (2011)