Financial Influenza:

Cyber Crime and Check Fraud

- Vaccines For Your Organization

Greg Litster
SAFEChecks
(800) 949-2265

This file contains 159 slides on Cyber Crime, Check Fraud, and ATM Fraud.

Cyber Crime starts with Slide 3

Check Fraud starts with Slide 71

ATM Fraud starts with Slide 141

Cyber Crime

Download this presentation at:

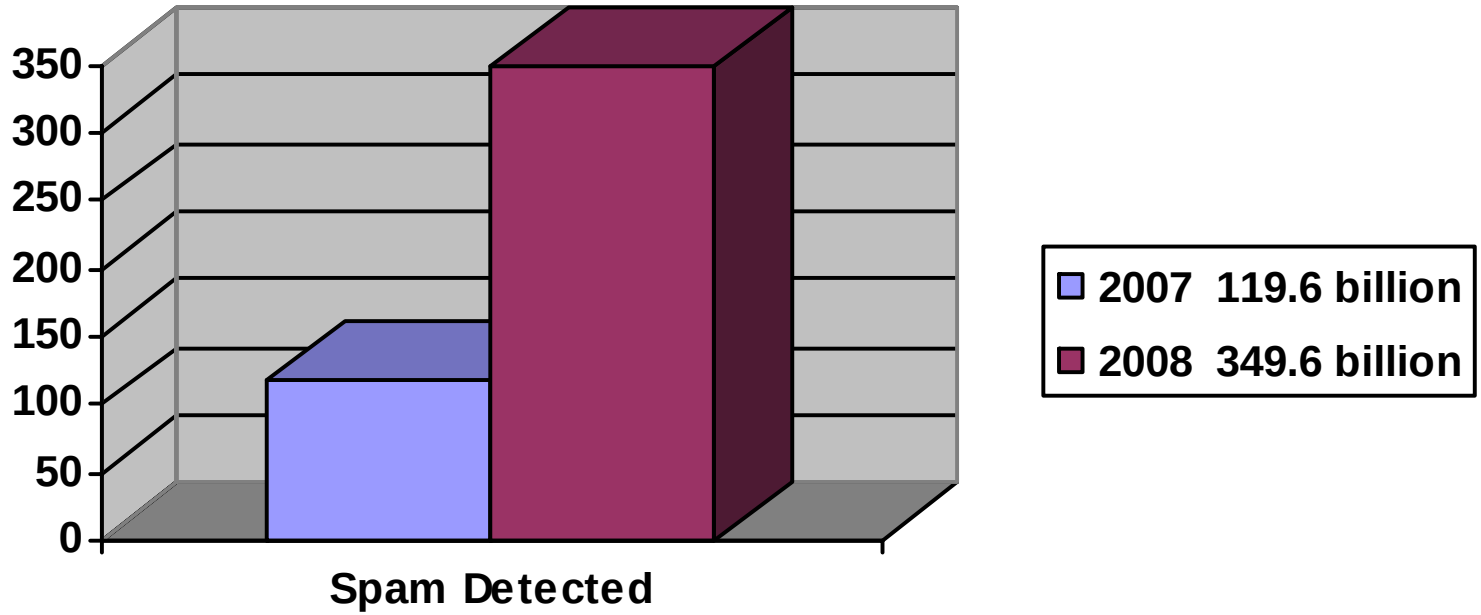
www.safechecks.com/services/fraudprevention.html

Resources

1. Symantec Global Internet Security Threat Report (2009)
2. Verizon 2009 Data Breach Investigations Report 2008 CSI
3. Computer Crime and Security Survey
4. OnGuardOnline.gov
5. FBI.gov/cyberinvest/protect_online.htm
6. getnetwise.org
7. pcisecuritystandards.org
8. PC Magazine (pcmag.com)
9. CNET Networks (cnet.com)
10. “Small Business Security, New Entrepreneurial Solutions”

    Brigham Young University, Marriott School of Management Alumni Magazine, Fall 2008

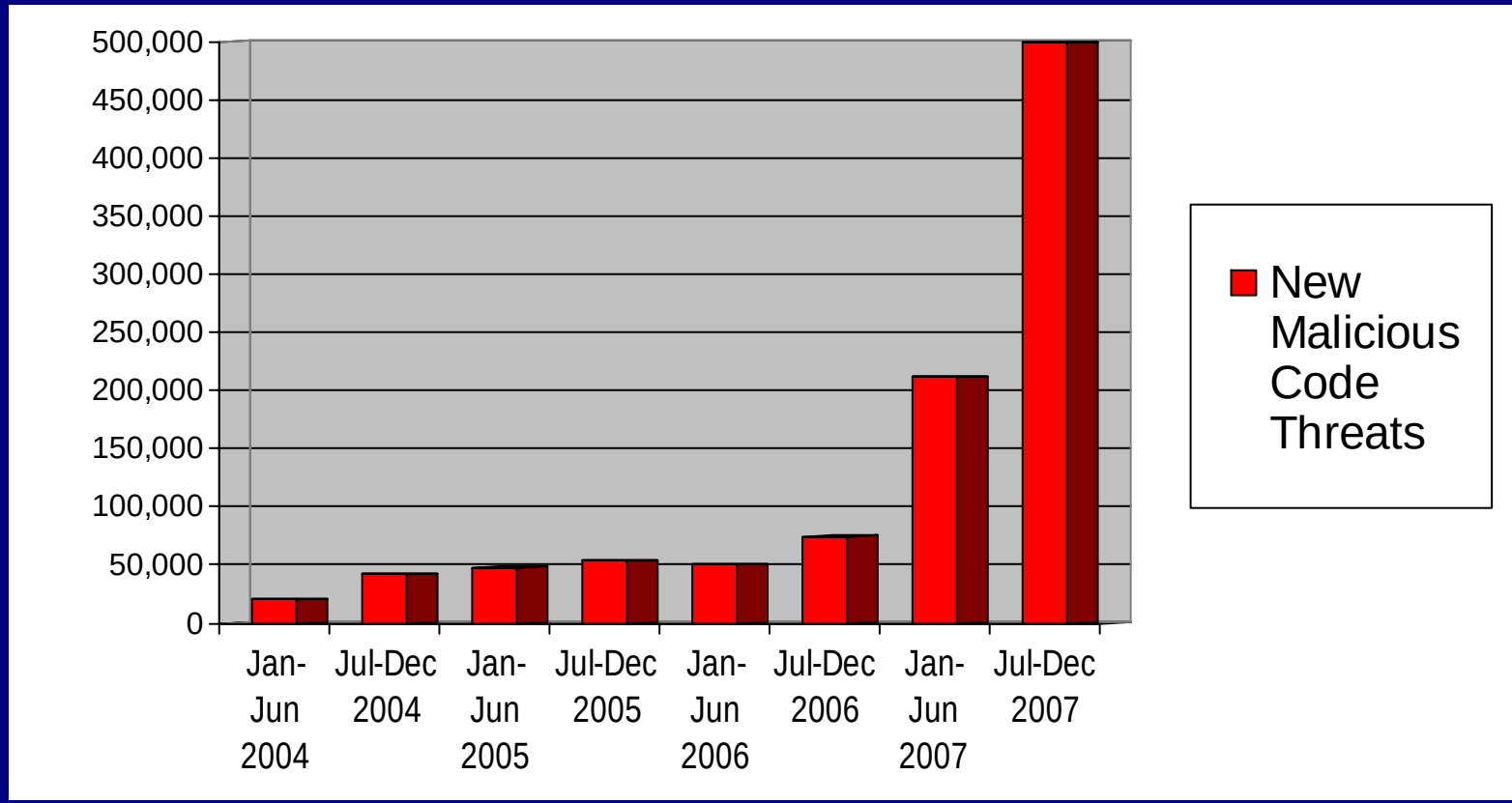
Internet Spam



Symantec observed a 192% increase in spam across the Internet, from 119 billion messages in 2007 to 349 billion in 2008.

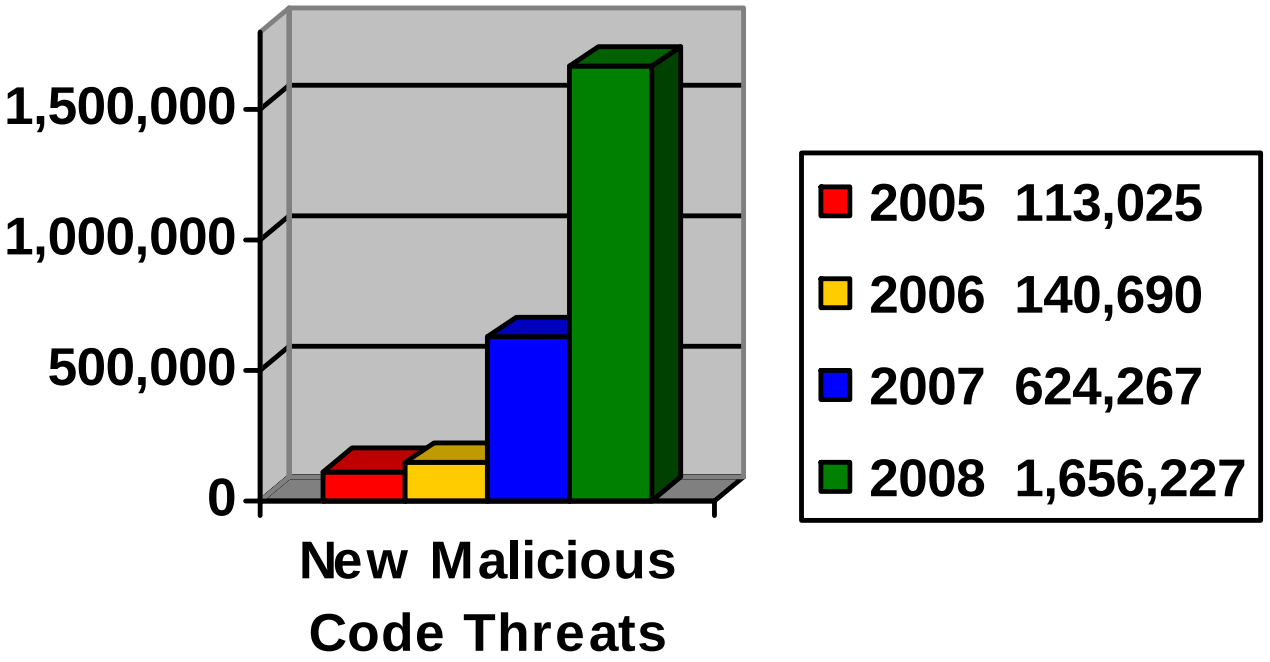
Bot networks were responsible for 90% of all spam.

Malicious Code Threats



2/3 of ALL malicious code thru 2007 was created in 2007

Malicious Code Threats



The trend today is to “customize” code to target a specific organization or industry

Symantec:

12,885 documented

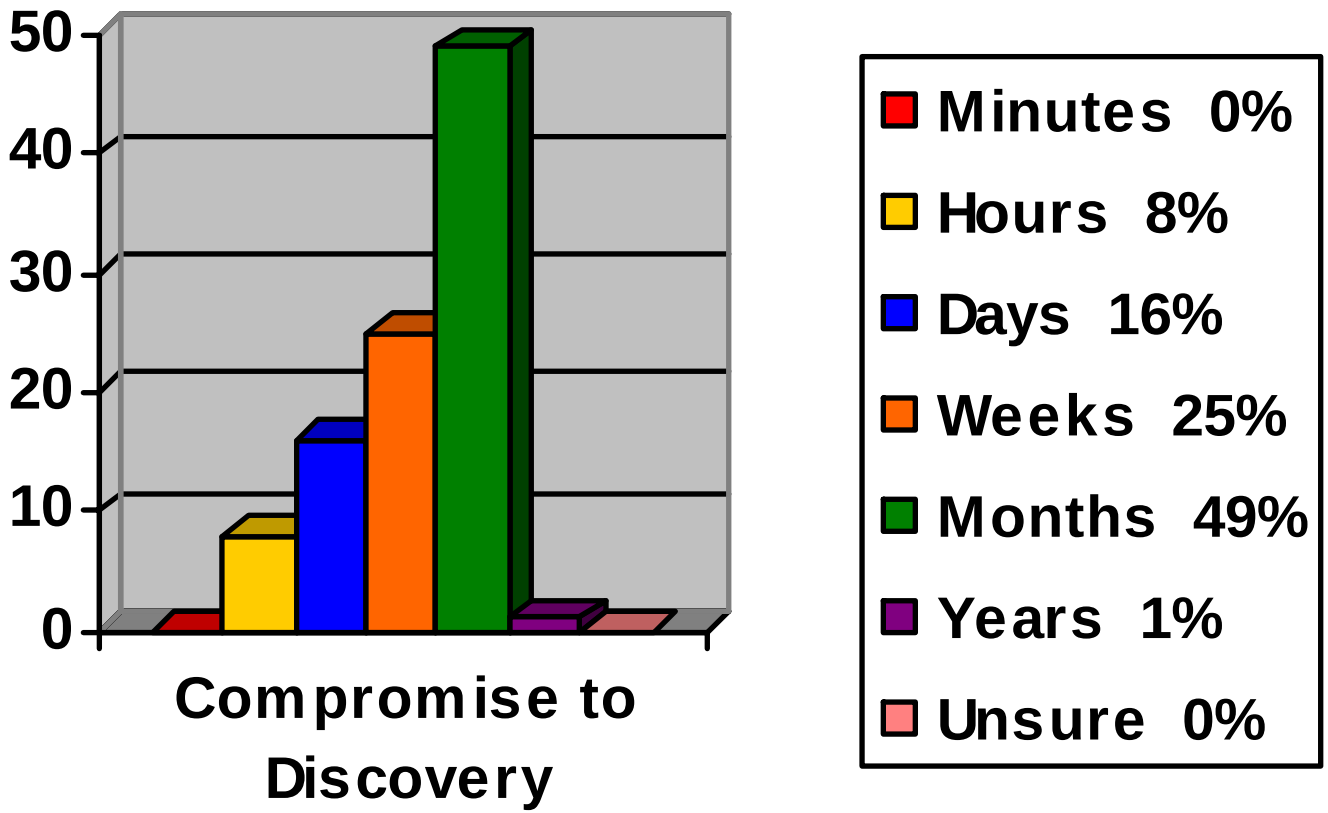
site-specific vulnerabilities

Data Breach: Cost

In 2008 the average cost per data breach incident in the United States was $6.7 million.

Lost business was $4.6 million.

Data Breach: Compromise to Discovery



Continuing types of attacks ....

Phishing

Attackers lure Web users to fake websites by using authentic-looking emails and real logos

Purpose: Steal user names, passwords, personal info, introduce a virus attack

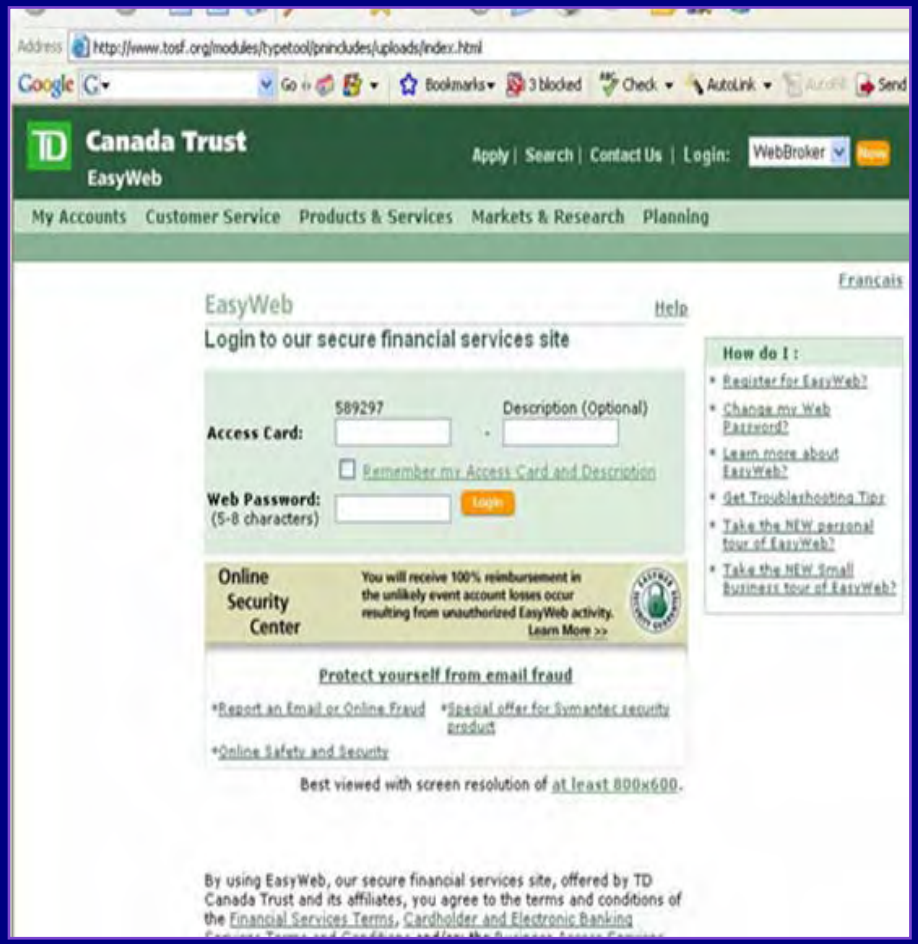
Phishing Hosts

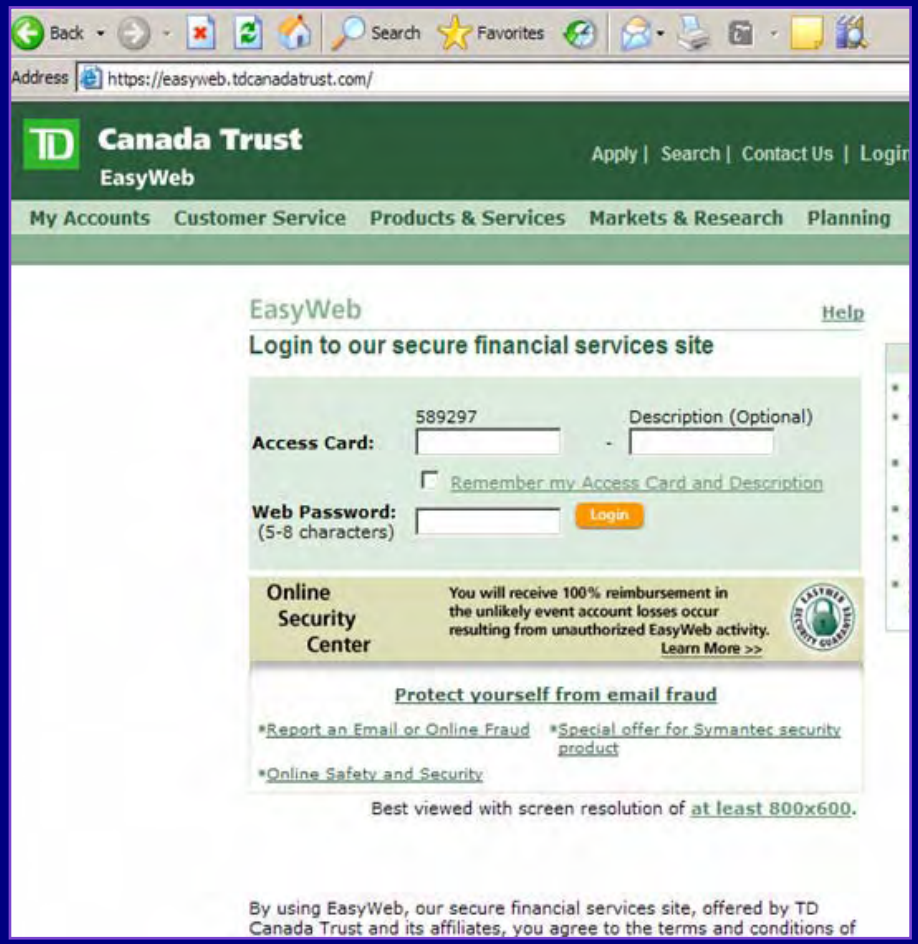
Symantec:

80% of brands used in phishing attacks

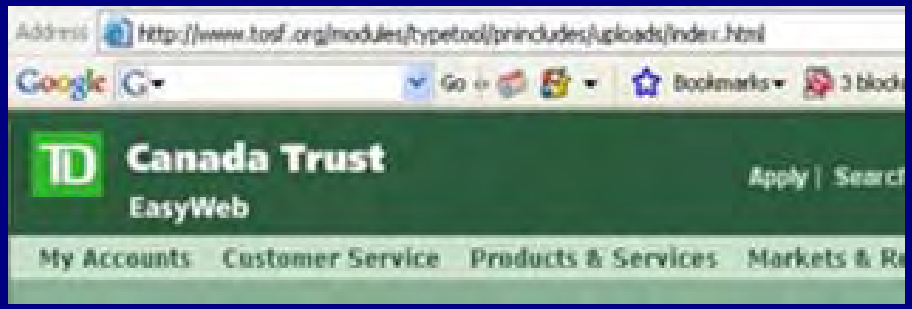
are financial services companies (banks)

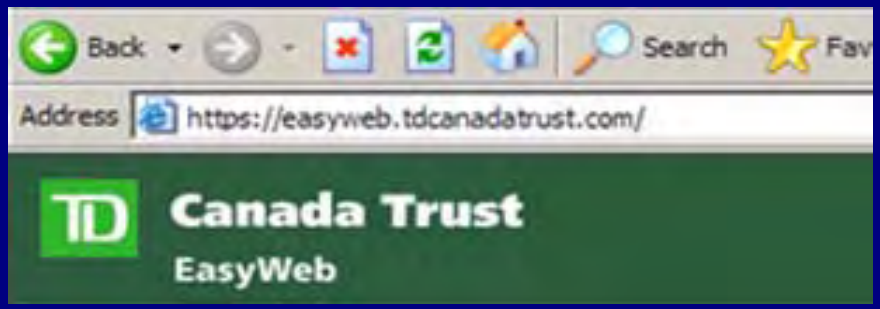
Phishing Hosts





Phishing Hosts





Hard to tell the difference?

The primary difference is URL address.

Pharming

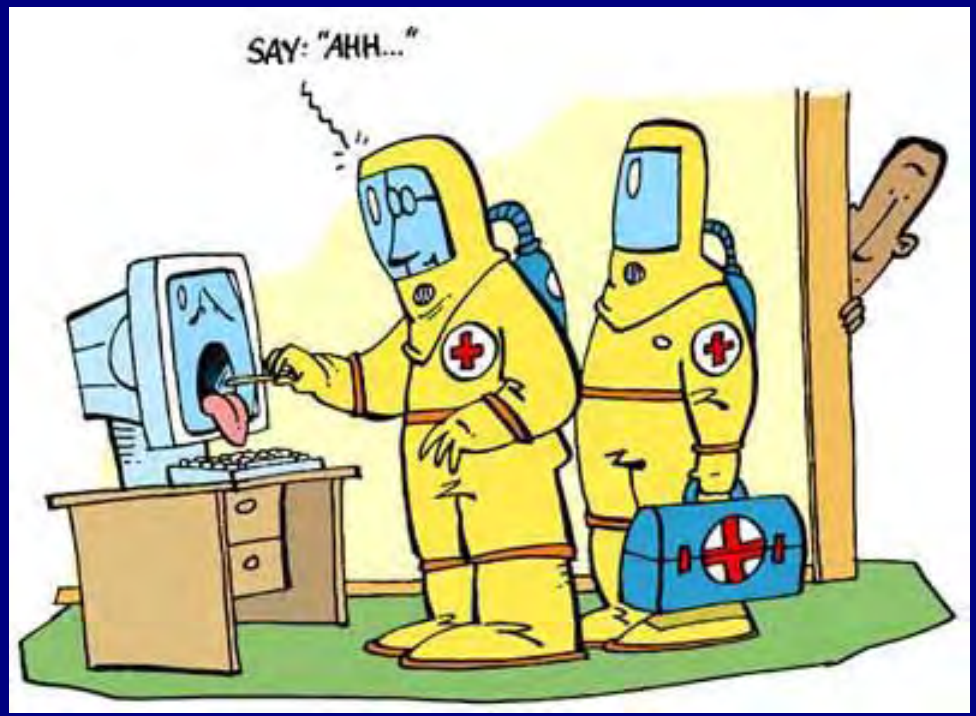
Hacker's attack to redirect a legitimate website's traffic to a fraudulent website.

Hacker gets paid by the click.

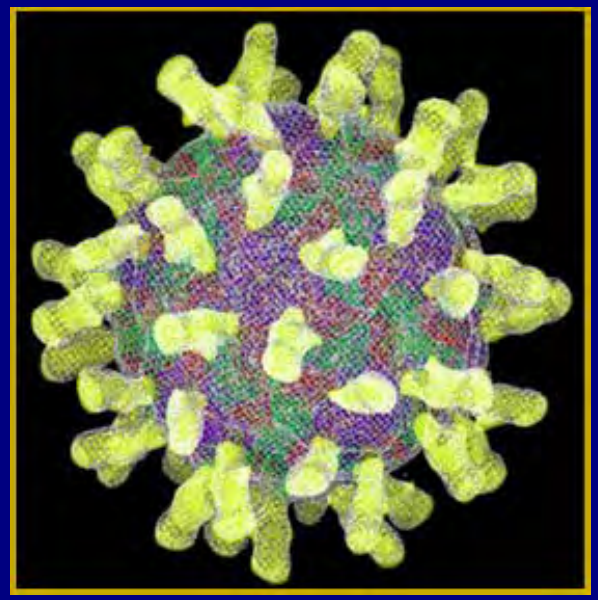
Malware

Malware – **MAL** icious soft **WARE**
Designed to infiltrate and damage a computer system

- **Viruses**
- **Trojan Horses**
- **Spyware**
- **Worms**



Virus



Virus – a computer program that infects a computer and copies itself.

A virus spreads:

- Network or Internet (email, Web sites)
- Infected files on a file network system
- Floppy Disk, CD or USB drive

Trojan Horse

Trojan Horse - a malicious program concealed in something innocuous or desirable (free music downloads)

Invites user to run it, but conceals a harmful payload, **such as a keystroke logger**

Six main types of Trojan Horse Payloads:

- Remote Access
- Data Destruction
- Downloader
- Server Trojan
- Security Software Disabler
- Denial of Service Attack

Spyware

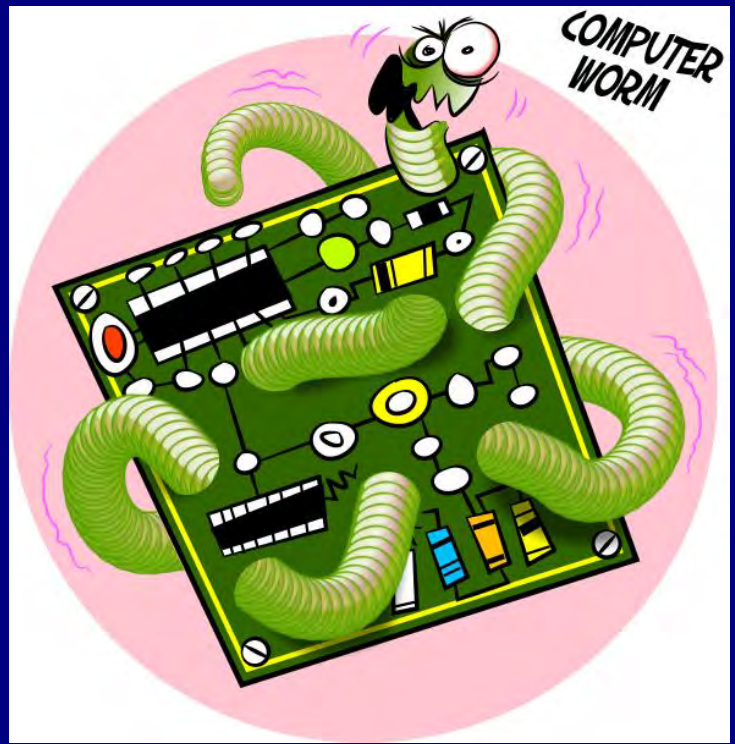
Spyware – program that secretly monitors the user's Internet behavior

Examples include:

- Monitoring Internet surfing habits
- Installing additional software
- Redirecting web browser activity
- Change computer settings

Worms

- A self-replicating computer program
- Uses a network to make copies of itself onto other networks
- Causes harm to a network, not an individual computer
- Does not need to attach itself to an existing program



Clear and Present Danger

is in the

New Trends

Criminals now target

- End users on individual computers through the Web
- Specific websites
- Social networking websites, e.g. MySpace, Facebook
- Specific organizations
- Industry segments

Why Attack Websites?

1. Websites & end users' computers are less likely to be found and quickly fixed

2. Look at the NUMBERS!

Facebook has 400,000,000 members!

MySpace has 100,000,000+

Facebook Exploitation

“Computer users have been conditioned not to open an attachment from an e-mail or click a link found within, but won't think twice about checking out a hot new video linked to by a trusted friend on Facebook."

USA TODAY

March 4, 2010

How cyber-criminals invade social networks, companies

“"Hey Alice, look at the pics I took of us last weekend at the picnic. Bob"

“That Facebook message, sent last fall between co-workers at a large U.S. bank, rang true enough. Alice had attended a picnic with Bob, who mentioned the outing on his Facebook page.

“So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from thieves who had hijacked Bob's Facebook account. And the link carried an infection, a keystroke logger designed to save everything she typed at her keyboard. Once an hour it sent a text file of her keystrokes to a free Gmail account controlled by the attacker.

www.usatoday.com/money/industries/technology/2010-03-04-1Anetsecurity04_CV_N.htm

“Later, the cyber-criminals used Alice's company logon to slip deep inside the financial firm's network, where they roamed for two weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

“The attackers reviewed the hourly keystroke reports from Alice's laptop and took note when she logged into a virtual private network account to access her company's network. With her username and password, the attackers logged on to the bank’s network and roamed around it for two weeks.

“First they ran a program, called a port scan, to map out key network connection points. Next they systematically scanned all of the company's computer servers looking for any that were not current on Windows security patches. Companies often leave servers unpatched, relying on perimeter firewalls to keep intruders at bay. The attackers eventually found a vulnerable server, and breached it, gaining a foothold to go deeper when they were discovered.”

Facebook Exploitation

“Stolen credentials flow into eBay-like hacking forums where a batch of 1,000 Facebook user name and password pairs, guaranteed valid, sells for $75 to $200, depending on the number of friends tied to the accounts.

“From each account, Cyber-scammers can scoop up e-mail addresses, contact lists, birth dates, hometowns, mothers' maiden names, photos and recent gossip — all useful for targeting specific victims and turning his or her PC into an obedient bot.”

Black Market Advertising

Goods and Services	Current Rank	Current %	Previous Rank	Previous %	Price Range
Bank accounts	1	22%	2	21%	$10 – $1000
Credit cards	2	13%	1	22%	$0.40 – $20
Full identities	3	9%	7	6%	$1 – $15
Online auction site accounts	4	7%	N/A	N/A	$1 – $8
Scams	5	7%	8	6%	$2.50 – $50 per week for hosting; $25/ design
Mailers	6	6%	4	8%	$1 – $10
Email addresses	7	5%	5	6%	$0.83 – $10 per Mb
Email passwords	8	5%	3	8%	$4–$30
Drop (request or offer)	9	5%	N/A	N/A	10% – 50% of total amount
Proxies	10	5%	6	6%	$1.50 – $30

Bots and Botnets

Bots

Bots are programs secretly installed on a computer, allowing a malicious user to control it remotely.

How Computers Become Bots

Attackers scan the Internet to find computers that are unprotected, and then install software through “open doors.”

How Computers Become Bots

Visiting a website, downloading files, opening attachments, links or images in spam email can install hidden “bot” software

Bots Statistics

Symantec: Bot-infected computers

Year End 2007 = 5,000,000

Year End 2008 = 10,000,000

Year End 2009 = Mooooooore!

Botnets

Botnets are a large number of computers

- Controlled by a single attacker
- Can be used to launch coordinated attacks

- Can be updated to perform new functions

Future Trends

1. The release rate of malicious code may exceed that of legitimate software applications
2. Portable storage devices
   - USB flash thumb drives,
   - Portable audio and video players
   - Digital picture frames with Internet connectivity
3. **Thieves aim to get into manufacturing stream**
4. Now, 40% of malicious code copy themselves to removable media

Reported March 5, 2009

Koobface worm

- Searches for cookies created by online social networks (Facebook)
- Connects to these Web sites using the user login session stored in the cookies
- Navigates through pages to search for the user's friends
- Sends a message to the friend to link to a video; malware is passed along inside video

Reported March 4, 2010

"Koobface Goldmine"

- At its peak August 2009, more than 1 million Koobface-infected PCs inside North American companies were taking instructions from criminal controllers to carry out typical botnet activities.

- Kaspersky Labs estimates that today there are 500,000 Koobface-controlled PCs active on the Internet on an average day, 40% of which are in the U.S., 15% in Germany and the rest scattered through 31 other nations.

Identity thieves take aim at Facebook users | Zero Day | ZDNet.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://blogs.zdnet.com/security/?p=3276

Most Visited Getting Started Latest Headlines

Reported April 29, 2009

BNET BUSINESS NETWORK: BNET | TECHREPUBLIC | ZDNET

ZDNet

Search: Search in Blogs

Members Log In | Newsletters | Site Assistance | RSS Feeds

Home | News & Blogs | Videos | White Papers | Downloads | Reviews | Popular

Zero Day

Ryan Naraine and Dancho Danchev

Get Zero Day via: Mobile RSS Email Alerts Bios: Ryan's Bio Dancho's Bio

Pick a blog category view

→→→

April 29th, 2009

Identity thieves take aim at Facebook users

Posted by Ryan Naraine @ 1:04 pm

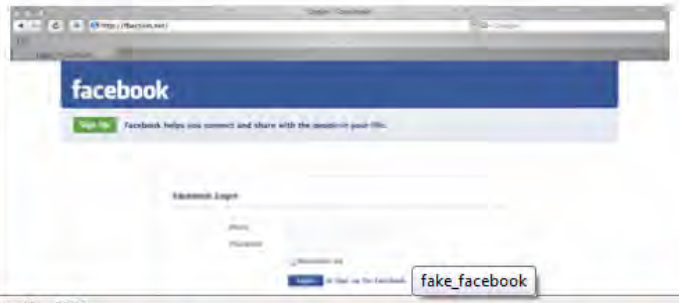
Categories: Anti Virus, Browsers, Data theft, Exploit code, Facebook...

Tags: Facebook, Identity Thieve, Social Networking, Phishing, Security...

TalkBack ADD YOUR OPINION | SHARE | PRINT | E-MAIL | WORTHWHILE? +3 3 VOTES

Identity thieves are currently launching a massive attack on Facebook, using fake log-in pages to hijack usernames and passwords.

The attackers are using Facebook's mail system to send a one-line message luring users to "fbaction.net," a site that clones the social networking site's log-in screen.



SPONSORED BY

Essential Topics

- Do you need to re-evaluate your data protection strategies?
- New backup and recovery methods using data de-duplication
- EMC Avamar: Data de-duplication technology
- Learn how to solve data center problems

Sponsored Links

The HOT Spot

CIO Sessions

Check out our video interviews with leading CIOs today!

Designing the next killer product
CIO of Sony Electronics: Drew Martin
8:05

Developing new ways to collaborate
CIO of Adobe: Gerri Martin-Flickinger
9:24

Overseeing IT operations across a global organization
CIO of Turner Broadcasting System: Dan Darling
6:48

The biggest security threats facing companies in 2009
Verisign CTO:

http://blogs.zdnet.com/security/?p=3276

Type X1 search 6:15 PM

How cybercriminals invade social networks, companies - USATODAY.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.usatoday.com/money/industries/technology/2010-03-04-1Anetsecurity04_CV_N.htm

Most Visited Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Reported March 4, 2010

USA TODAY Home News Travel Money Sports Life Tech Weather

Money Markets Economy Companies/Execs Personal Finance Taxes Media Cars Real Estate Small Business

GET A QUOTE: Enter symbol(s) or Keywords GO DJIA 10,552.52 -13.68 NASDAQ 2,332.21 +5.86 as of close 3/8/2010

How cybercriminals invade social networks, companies

Updated 4d 11h ago | Comments 120 | Recommend 83 E-mail | Save | Print | Reprints & Permissions | RSS

Enlarge By Jeff Dionise and Sam Ward, USA TODAY

By Byron Acohido, USA TODAY

SAN FRANCISCO — "Hey Alice, look at the pics I took of us last weekend at the picnic. Bob"

That Facebook message, sent last fall between co-workers at a large U.S. financial firm, rang true enough. Alice had, in fact, attended a picnic with Bob, who mentioned the outing on his Facebook profile page.

HOMELAND SECURITY: Seeks citizen cybercrime fighters
SLIPPERY WORM: Koobface changes its tricks

So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from thieves who had hijacked Bob's Facebook account. And the link carried an infection. With a click of her mouse, Alice let the attackers usurp control of her Facebook account and company laptop. Later, they used Alice's company logon to slip deep inside the financial firm's network, where they roamed for weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

Intrusions like this one — investigated by network infrastructure provider Terremark — can expose a company to theft of its most sensitive data. Such attacks illustrate a dramatic shift underway in the Internet underground. Cybercriminals are moving aggressively to take advantage of an unanticipated chink in corporate defenses: the use of social networks in workplace settings. They are taking tricks honed in the spamming world and adapting them to what's driving the growth of social networks: speed and openness of individuals communicating on the Internet.

"Social networks provide a rich repository of information cybercriminals can use to refine their phishing attacks," says Chris Day, Terremark's chief security architect.

This shift is gathering steam, tech security analysts say. One sign: The volume of spam and phishing scams — like the

Share
Yahoo! Buzz
Add to Mixx
Facebook
Twitter
More

Subscribe
myYahoo
iGoogle
More

USER SAFETY TIPS

Twitter and Facebook offer similar advice for dealing with bad links and compromised social-networking accounts. Twitter warns: If you receive a message with a phrase like "This you??" or "LOL is this you" followed by a link, do not click through; there's a phishing site on the other side. Suspicious links can show up in spam messages or via faked status updates.

What to do if you've been hit:

- Run anti-virus software, and be sure to use the most current version of your Web browser, which contains the most up-to-date protection features.
- Reset your password.
- Never click suspicious links, even if they appear to come from a friend. Do not run any ".exe" files on your computer without knowing what they are.

For more information: help.twitter.com; www.facebook.com/help. Or try www.antiphishing.org/consumer_recs.html and

Featured video


The Hurt Locker
U.S. troops give mixed reviews for the Oscar winner.


Disappearance
Texas CEO vanishes in New Orleans.


Iditarod begins
Hundreds of sled dogs, fans lined up in Anchorage.

More: Video

Done

start Microsoft PowerPoint ... PwrPoint Presentations new data - 2010 How cybercriminals in... How cybercriminals in... New research 2010 - ... 10:15 PM

USA TODAY

February 19, 2010

Trove of 68,000 stolen log-ons in hands of 'amateur' hackers

"In four weeks in early 2010, cyber-thieves' known as the Kneber gang, pilfered 68,000 account log-ons from 2,411 companies, including user names and passwords for 3,644 Facebook accounts."

www.usatoday.com/money/industries/technology/2010-03-04-1Anetsecurity04_CV_N.htm

Verizon: "End-users and IT administrators continue to be the culprits behind most internal breaches. two-thirds were the result of deliberate action and the rest were unintentional. While it's tempting to infer that administrators acted more deliberately and maliciously than end-users and other employees, the evidence does not support this conclusion. The ratio was roughly equal between them.

"It is worth noting that both cases involving senior management were the result of deliberate action which was taken after the person was terminated. We also noticed several other breaches in the caseload were perpetrated by recently terminated employees.

Why Does It Matter?

They will steal your money. And your life!

- Company in the Midwest
- CFO got a virus; had her keystrokes captured
- Thief logged into bank using CFO's bank log on
- Sent $160,000 ACH credits to controlled accts
- Money was wired out of country the next day
- Company discovered the transfer 11 days later
- Bank denied their claim for reimbursement

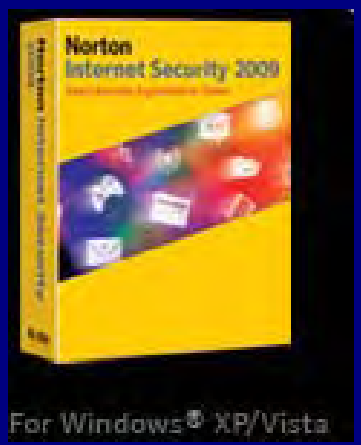
Solutions

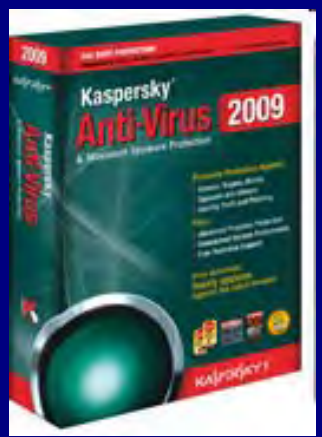
Anti-Virus, Anti-Spyware Software

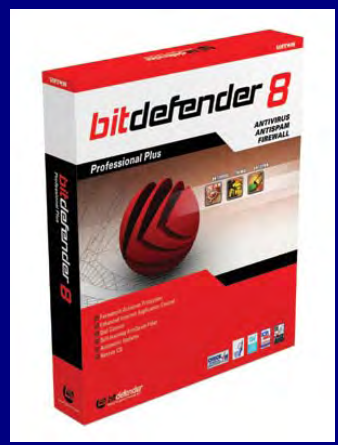
Software to identify, neutralize or eliminate malicious code

- Monitors behavior of all programs. If one tries to activate an executable program, it will alert the user

AVG, Webroot Spy Sweeper, Kaspersky, BitDefender, Norton Internet Security 2009 is no longer a resource hog!







FIREWALLS

A firewall is different than anti-virus and anti-spyware software, which removes or quarantines viruses.

A properly-configured firewall helps make you invisible on the Internet and blocks incoming communications from unauthorized sources.

Authentication Tools

Multi-Factor Authentication: Using more than one factor to identify users accessing computers, networks and applications

- Encryption
- Digital Certificates
- Tokens
- Biometrics
- Knowledge-based options

Encryption

Encryption: Uses algorithms to convert data into a form that cannot be easily deciphered or understood by unauthorized people. All sensitive data stored electronically in a company should be encrypted.

Algorithm: A sequence of finite instructions, including randomness, for calculation and data processing

SSL: Secure Socket Layer – Protocol that uses a cryptographic system for transmitting documents via Web

-Uses a "**public key"** to encrypt the message; and a "**private key"** known only to the recipient who deciphers the message

URLs containting SSL will start with https:, not http:

Digital Certificates

Digital Certificates: an electronic "credit card" issued by a certification authority that establishes your credentials when doing business on the Web

- It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key, and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real

- It is specific to the computer on which it is installed

Hard Tokens

One-Time Password token, key-fob size

- Randomly generates OTP's every 60 seconds
- Logs require the OTP, user name and password

Soft Tokens

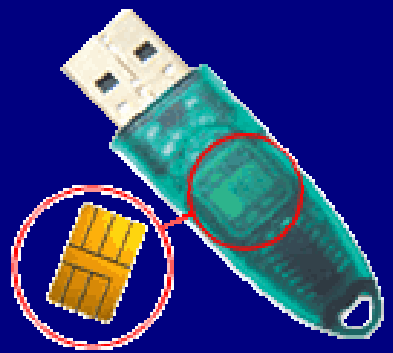
-Software version of the hard token

- Typically generated by a central server that runs security software
- Sent to users' cell phones, PDAs, laptops for access to the network
- Most still require a user name and password

USB Smartcard Tokens

USB Smartcard Token:

- Combines encryption capabilities with the versatility of tokens
- Stores user digital certificates and keys, allowing users to plug their tokens into **ANY** computer

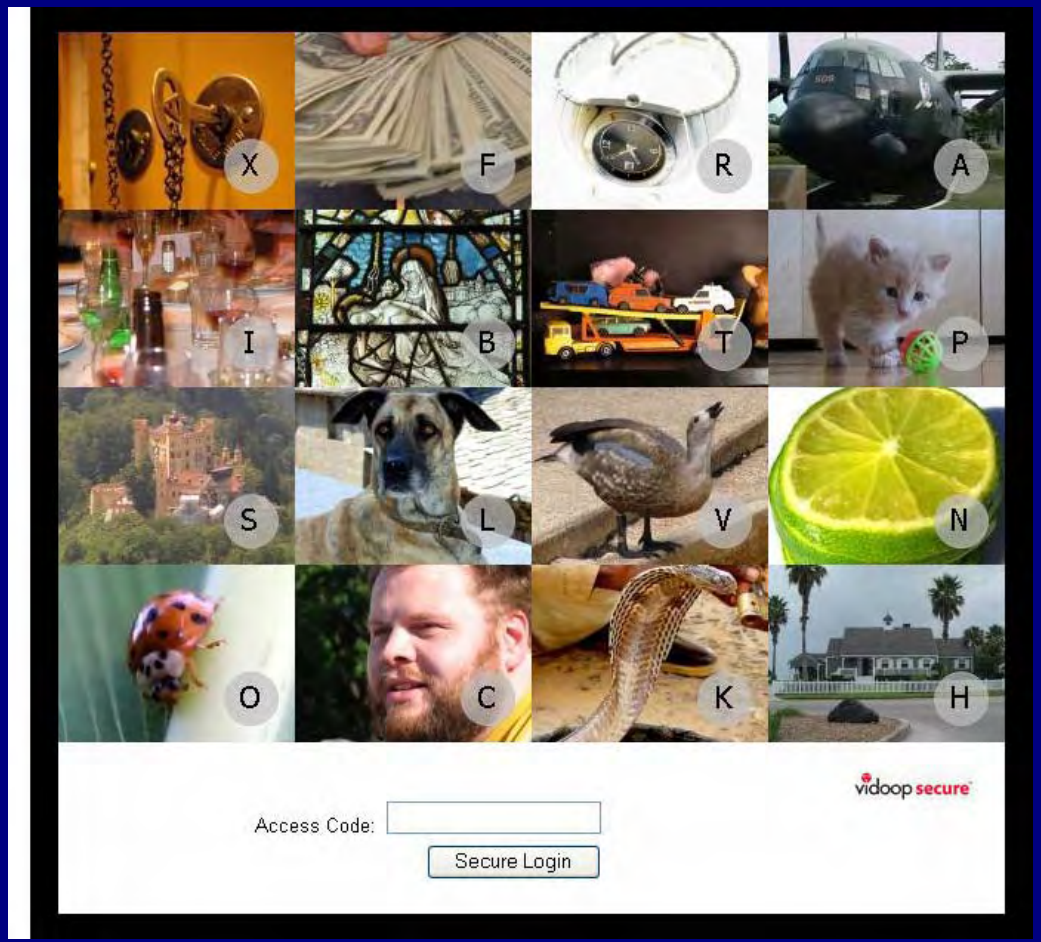


Biometrics

Biometrics:

- Technologies that measure and analyze human body characteristics for authentication purposes
- Uses an algorithm to match points in a database and translate this information into a numeric value

Knowledge-Based Options



Cyber Crime Tips

Found in Frank Abagnale's

Check Fraud, Identity Theft, Holder in Due Course and Cyber Crime, Vol. 8

Page 15: Cyber Crime Prevention

Cyber Crime Tips

INDIVIDUALS

Don’t follow links imbedded in emails from unknown sources. They may link to spoofed Web sites

Manually type the URL into your browser bar

Cyber Crime Tips

Unplug your Internet connection when you're away.

Cyber Crime Tips

Never reply to an email, text, or pop-up that asks for personal information

Scan all email attachments before opening. Don’t open an attachment unless you know what it contains

Cyber Crime Tips

Restrict the applications you install on social networks.

Never install a codec from
a random Web site.

Cyber Crime Tips

Don’t send sensitive files over a Wi-Fi network unless it is secure.

Public “hot spots” are not secure.

When you’re not using Wi-Fi, turn off the wireless connection to your laptop.

Track Your Kids

Track Your Kids

Spector Pro: You can track your child's keystrokes, emails, MySpace, Facebook, IM, and websites visited with Spector Pro (spectorsoft.com).

eBlaster forwards their emails to you

Track Your Kids

Home and Office

SPECTOR PRO 2009

Powerful Monitoring, Extreme Ease of Use

Records Every Exact Detail of Their Computer and Internet Activity.

Win For Windows Mac For Mac OS

eBLASTER 2009

Remote Monitoring Software

Knowing **EVERYTHING** They Do Online is as Easy as Checking Your Email.

Track Your Kids

Verizon "Chaperone," Sprint:
Child locator (cell phone)

- Location address (map) within 100 ft
- Direction of travel
- Velocity (speed)

Cyber Crime Tips

ORGANIZATIONS

Create Zones of Protection

"What data is being stored and where is it being stored?"
(Many companies don't know!)

Prioritize which data is most sensitive, build defenses around that first.

Cyber Crime Tips

Restrict unauthorized access to sensitive data.

Require that all sensitive data be encrypted or password protected before transmission.

Cyber Crime Tips

Install software to limit the sites users may access.

Maintain a whitelist of trusted Web sites, and disable individual plug-ins and scripting capabilities for other sites.

Cyber Crime Tips

Use a network-based Intrusion Prevention System (IPS)

Cyber Crime Tips

When employees leave the company, immediately disconnect their access to the company's network and building, shut down remote connections, and collect their cell phones, iPDAs, smartphones, etc.

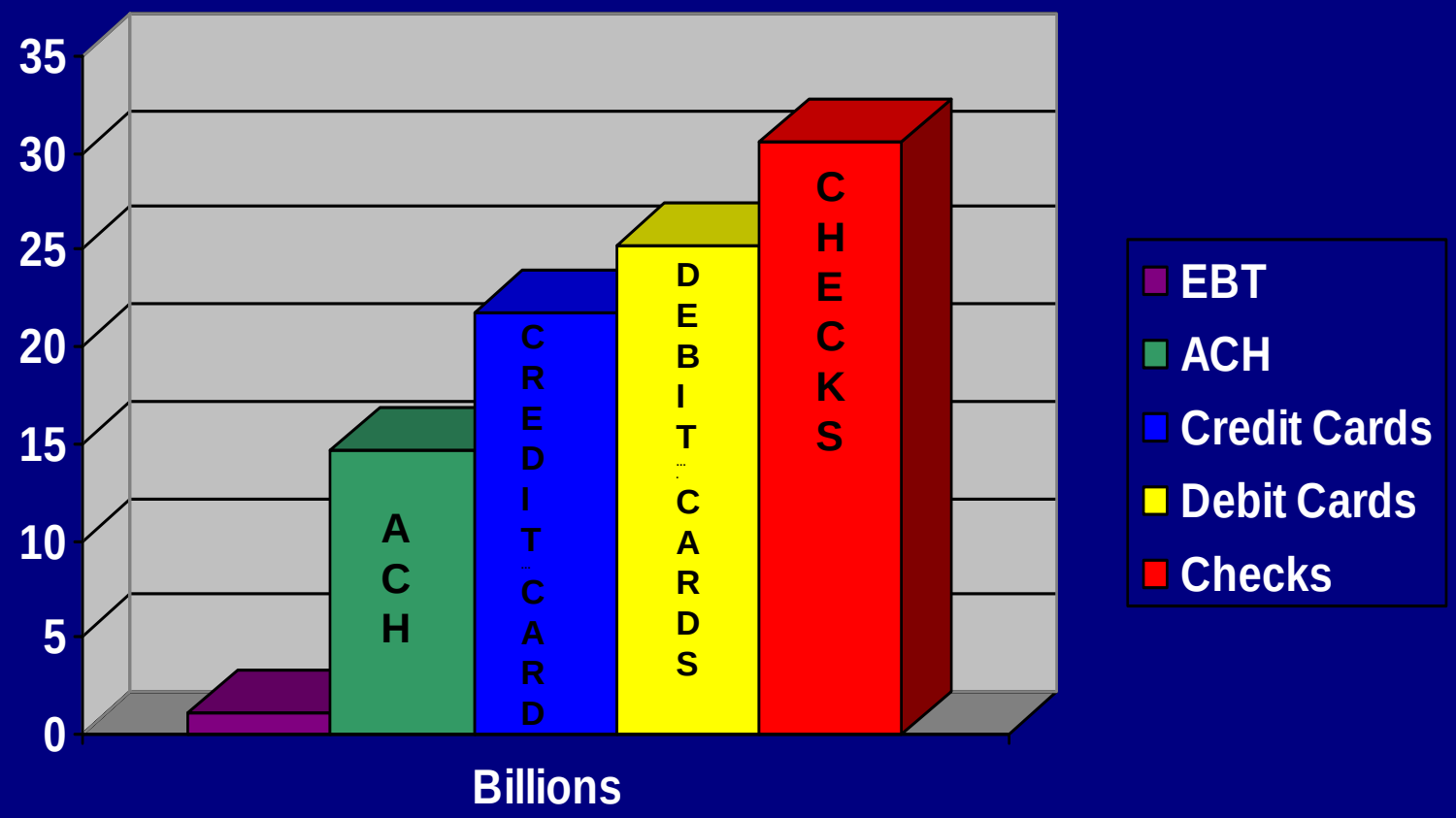
(More than half of employees said if they ever lost their jobs, they'd take sensitive company data with them.
They also said this would be relatively easy to do.)

Check Fraud...

Why talk about Check Fraud?

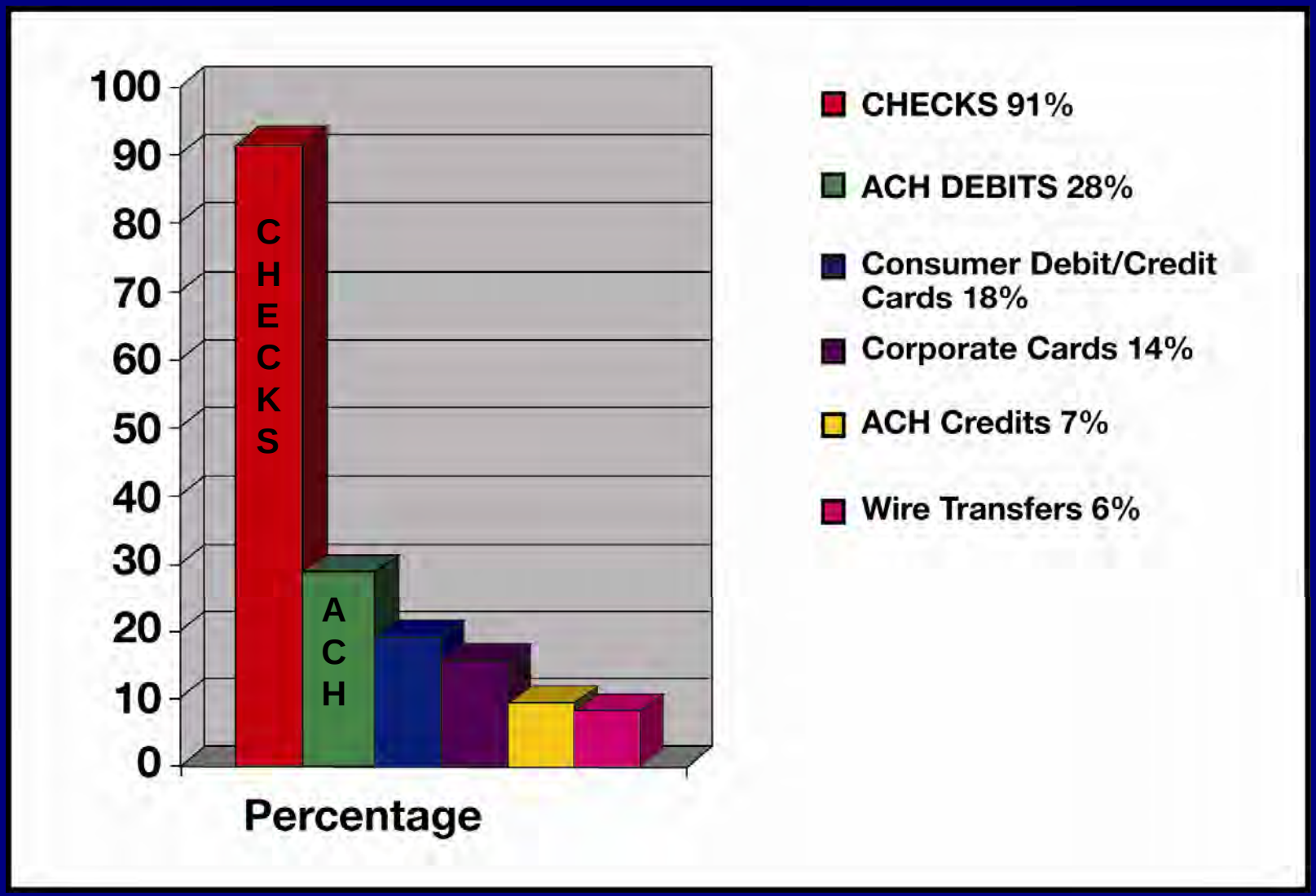
Check Fraud produces more losses than all other payment fraud COMBINED!

Total Non-Cash Payments by Method
(Transactions)

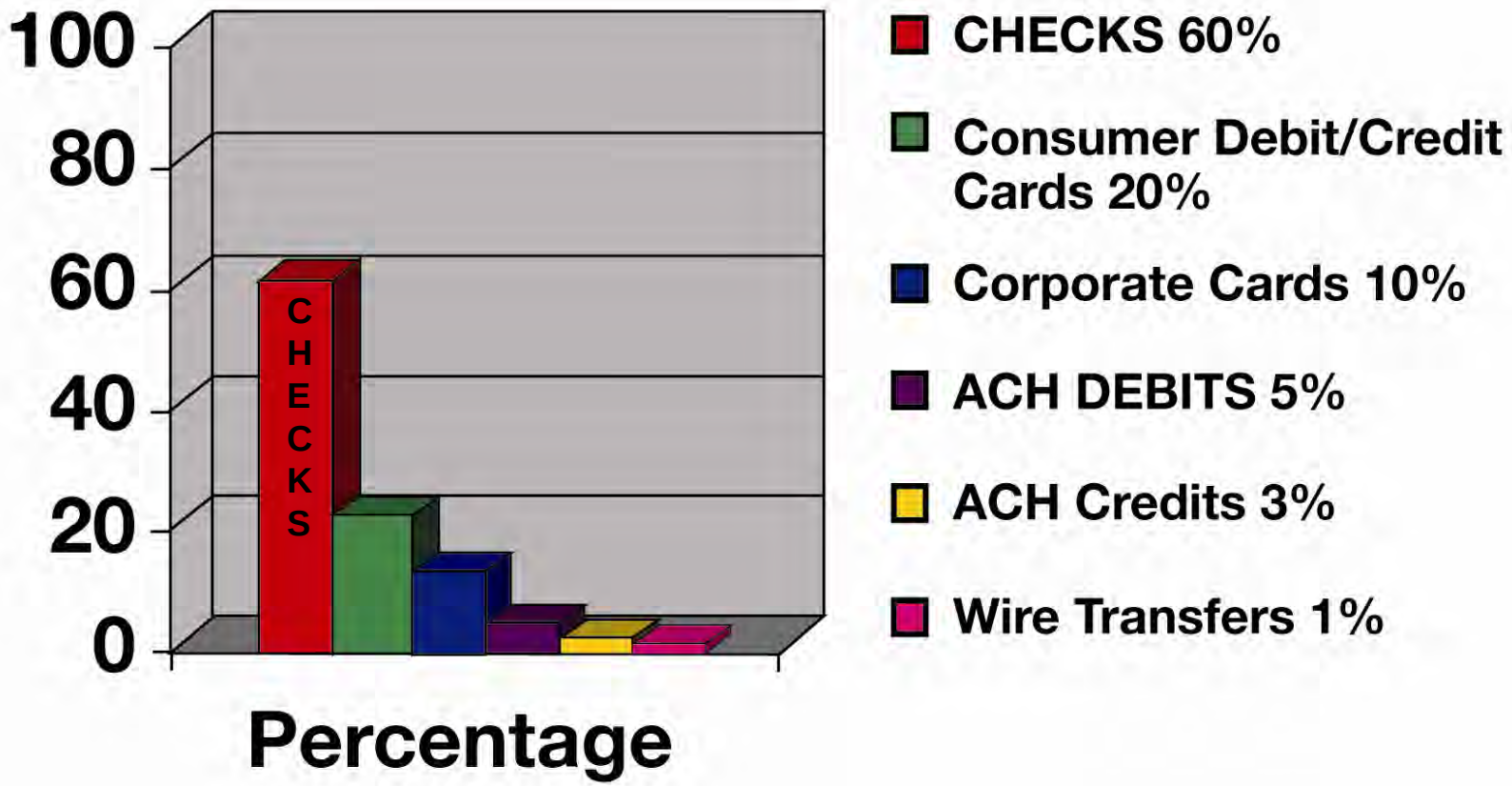


Fraudulent Payments by Method

(Some Respondents were hit multiple ways; total > 100%)



Fraud Losses by Method
(How Dollars were actually lost)



Check Writing Software

VERSACHECK® Gold 2007

Create Checks and Manage Finances - For Home and Business!

Only

$20

Checksoft™ Premier

Create checks and manage your business finances

$69.95!

Buy Now

Solutions

#1. High Security Checks

High Security Checks

1. Help deter forgers' attempts

2. Thwart some Holder in Due Course claims

3. Establish the basis for an indemnity claim

What makes a check secure?

10+ safety features

Abagnale SuperBusinessCheck
16 Safety Features

- Controlled Check Stock
- True Watermark
- Thermochromatic Ink (Heat)
- UV Ink + UV Fibers
- Copy Void Pantograph
- Chemical-reactive Ink + Paper
- Microprinting
- Inventory Control Number on Back (laser)
- Toner Grip™ Toner Anchorage
- Warning Banner

#2. Payee Positive Pay

#3. Timely Account Reconciliation

#4. Tight Internal Controls

Tighter Internal Controls

- Secure all check stock (lock and key)
- Restrict employee access to check supply
- Physical inventory of check supply regularly
- Reconcile accounts immediately (UCC: 30 days)
- Secure facsimile signature plate (lock and key)
- Never sign a check with a rubber stamp
- Use a cloth ribbon when typing manual checks
- Embezzlement
  - Separate financial duties

Separate Financial Duties

- "Reasonable Employee Rule"
- Responsible for acts of employees
  - Hiring Procedures
  - Background Investigations

“Reasonable Employee Rule”

Section 3-405 adopts the principle that the risk of loss for fraudulent endorsements by employees who are entrusted with the responsibility with respect to checks should fall on the employer rather than on the bank that takes the check or pays it, if the bank was not negligent in the transaction.

“Reasonable Employee Rule”

Section 3-405 is based on the belief that the employer is in a far better position to avoid the loss by care and choosing employees, in supervising them, and in adopting other measures to prevent forged endorsements on instruments payable to the employer.

Source: Clark’s Bank Deposits and Payments Monthly
January 1995: Volume 3 #7

Positive Pay…

Web: PositivePay.net

Positive Pay...

...a powerful tool!

...one big issue

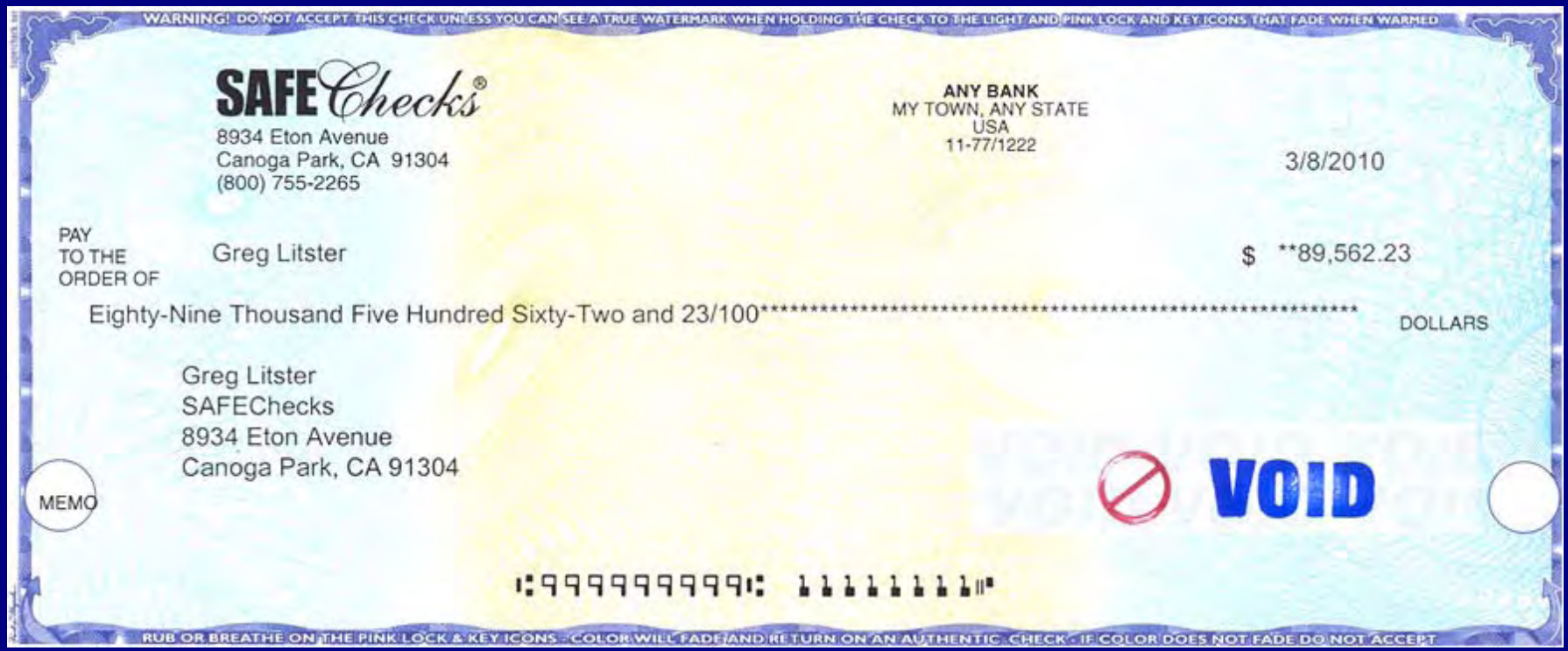
the Payee Name ...

Altered or Added Payee Names

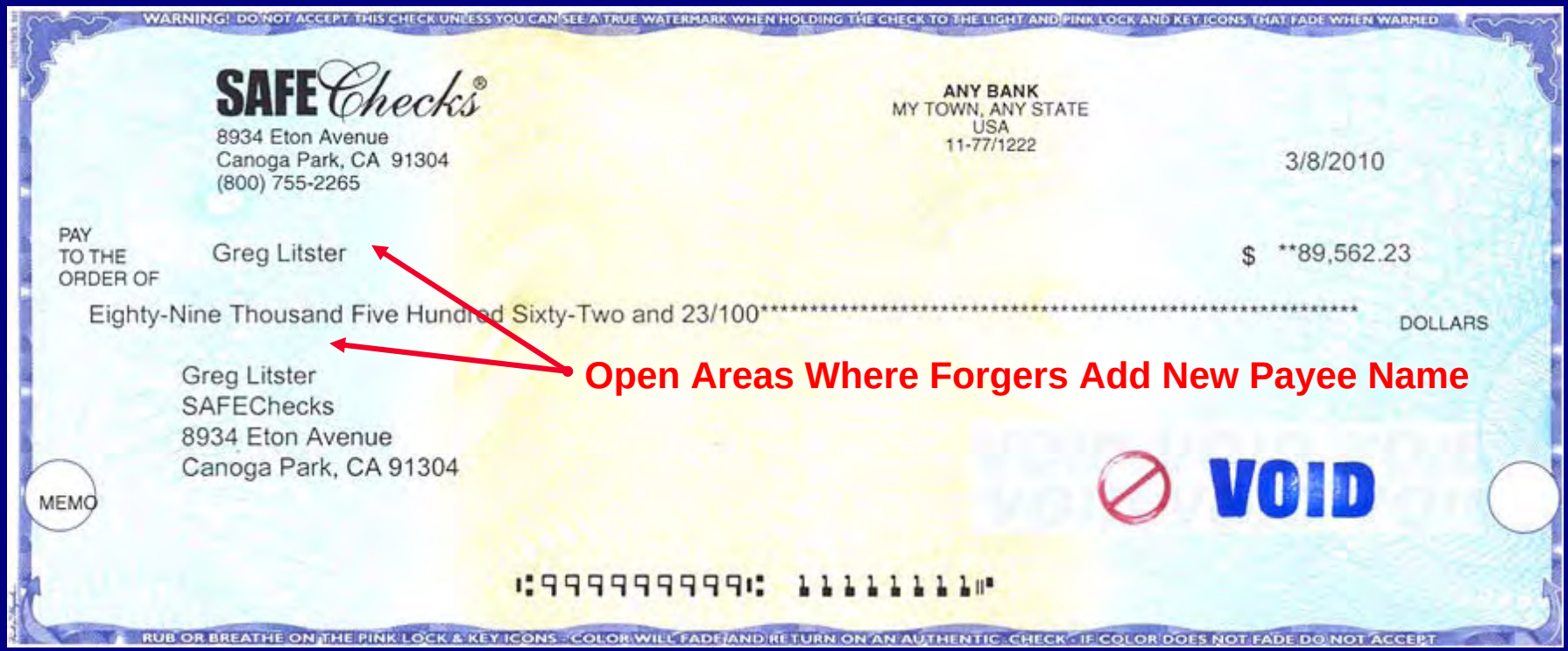
Preventing Altered Payees

- High-security checks
  - Requires Toner Anchorage
- Use 14 point font for Payee Name
- Positive Pay with Payee Name Recognition
- High-quality laser toner
- Hot laser printer
  - Highest temperature setting available
  - Replace fuser element every 2-3 years

Typical Check Layout



Typical Check Layout



The identical check printed thru the secure Printer Driver

The “secure seal” barcode is created by a Printer Driver

Preventing Altered Payees

- Frank Abagnale Fraud Bulletin

Page 7: A Primer on Laser Printing

Altered Payee Names

and

“Secure Seal” Technology

Secure Seal

is an

image-survivable

encrypted barcode

Secure Seal barcode

Barcode is created by a Printer Driver

For more details, call Greg Litster (800) 949-2265

or email greg@safechecks.com

Secure Seal barcode

14 point font

Secure Seal barcode

Secure Name Font 18 point

14 point font

Secure Seal barcode

Secure Number Font

Secure Name Font 18 point

14 point font


Secure Seal barcode
"Forger-Deterrent" Text
"Forger-Deterrent" Text
WARNING! DO NOT ACCEPT THIS CHECK UNLESS YOU CAN SEE A TRUE WATERMARK WHEN HOLDING THE CHECK TO THE LIGHT AND PINK LOCK AND KEY ICONS THAT FADE WHEN WARMED
SAFE Checks
8934 Eton Avenue
Canoga Park, CA 91304
(800) 755-2265 • Fax (800) 615-2265
safechecks.com • supercheck.NET
Any Bank
My Town, Any State
11-777/1222
This Check is Protected By
Cheque Guard
Check Number
300257
CHECK DATE
3/8/2010
CHECK AMOUNT
$89,562.23
$89,562.23
PAY
EIGHTY NINE THOUSAND FIVE HUNDRED SIXTY TWO DOLLARS AND 23/100 CENTS
Payee GREG LITSTER
TO THE ORDER OF
GREG LITSTER
SAFEChecks
8934 Eton Avenue
Canoga Park, CA 91304
THIS CHECK EXPIRES AND IS VOID 25 DAYS FROM ISSUE DATE
Holder in Due Course Text
PAYEE NAME ON FILE AT THE BANK
THIS CHECK CLEARS THROUGH POSITIVE PAY
Secure Number Font
Secure Name Font 18 point
14 point font

Print driver can also:

1. Accumulate check data for Positive Pay
2. Add Barcode, Secure Name & Number fonts
3. Reposition Check Placement
4. Change Font size

SAFE Checks 8934 Eton Avenue, Canoga Park, CA 91304
Greg Litster 3/8/2010 89,562.23

Typical Check Layout

Printer Driver can Reposition the Check

Any Bank 89,562.23

SAFE Checks 8934 Eton Avenue, Canoga Park, CA 91304
Greg Litster 3/8/2010 89,562.23

Any Bank 89,562.23

GREG LITSTER
SAFEChecks
8934 Eton Avenue
Canoga Park, CA 91304

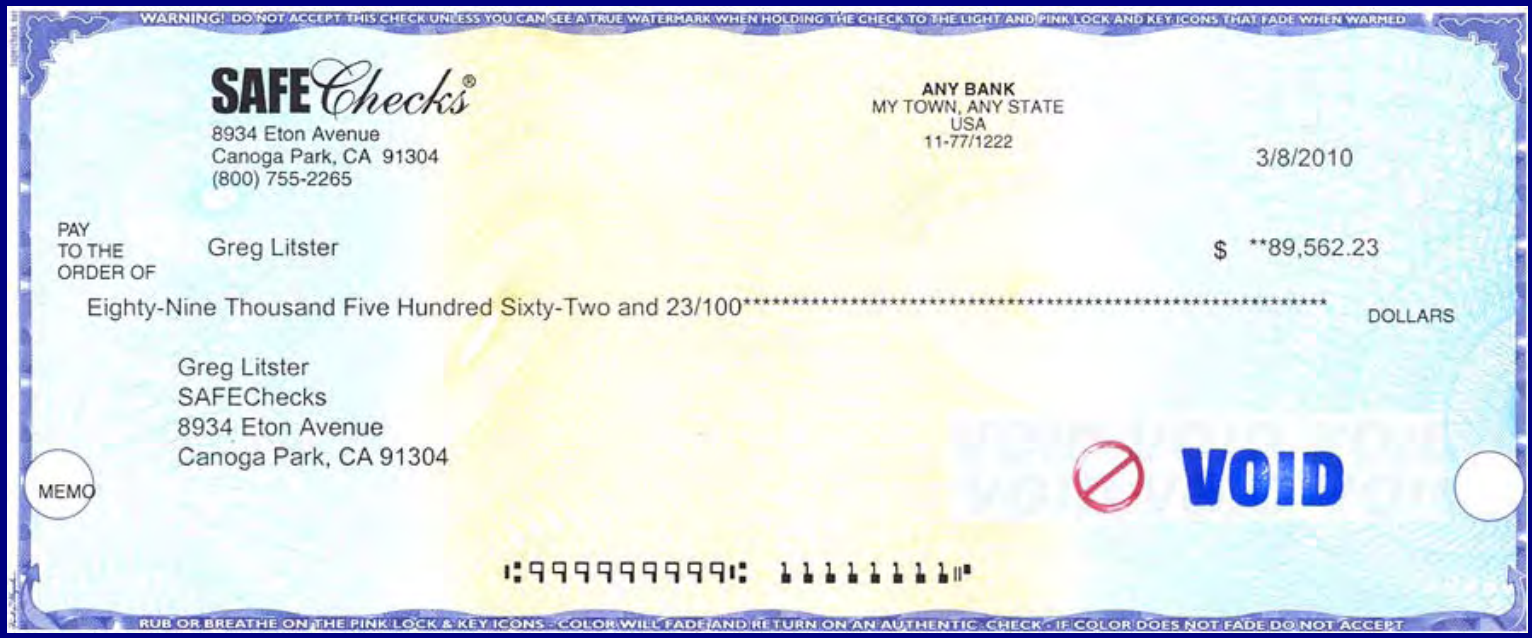
Check Number: 300257
Check Date: 3/8/2010

Invoice Date	Type	Reference	Gross Amount	Amount Due	Disc. Amount	Amount Paid
						89,562.23

Payee Name, Address is printed in top white panel for mailing. It isn't evident the envelope contains a check.

Check is repositioned to the bottom

Which check would forgers prefer to attack?
Identical data is printed on both checks.



WARNING! DO NOT ACCEPT THIS CHECK UNLESS YOU CAN SEE A TRUE WATERMARK WHEN HOLDING THE CHECK TO THE LIGHT AND PINK LOCK AND KEY ICONS THAT FADE WHEN WARMED

SAFE Checks®
8934 Eton Avenue
Canoga Park, CA 91304
(800) 755-2265

ANY BANK
MY TOWN, ANY STATE
USA
11-77/1222

3/8/2010

PAY TO THE ORDER OF Greg Litster

$ **89,562.23

Eighty-Nine Thousand Five Hundred Sixty-Two and 23/100********** DOLLARS

Greg Litster
SAFEChecks
8934 Eton Avenue
Canoga Park, CA 91304

MEMO

VOID

⑆999999999⑆ 111111111⑈

RUB OR BREATHE ON THE PINK LOCK & KEY ICONS - COLOR WILL FADE AND RETURN ON AN AUTHENTIC CHECK - IF COLOR DOES NOT FADE DO NOT ACCEPT

WARNING! DO NOT ACCEPT THIS CHECK UNLESS YOU CAN SEE A TRUE WATERMARK WHEN HOLDING THE CHECK TO THE LIGHT AND PINK LOCK AND KEY ICONS THAT FADE WHEN WARMED

SAFE Checks®
8934 Eton Avenue
Canoga Park, CA 91304
(800) 755-2265 • Fax (800) 615-2265
safechecks.com • supercheck.NET

Any Bank
My Town, Any State

11-777/1222

This Check is Protected By™ ChequeGuard

Check Number
300257

CHECK DATE	CHECK AMOUNT
3/8/2010	$89,562.23

$89,562.23

PAY EIGHTY NINE THOUSAND FIVE HUNDRED SIXTY TWO DOLLARS AND 23/100 CENTS

Payee GREG LITSTER

TO THE ORDER OF
GREG LITSTER
SAFEChecks
8934 Eton Avenue
Canoga Park, CA 91304

THIS CHECK EXPIRES AND IS VOID 25 DAYS FROM ISSUE DATE

NON-NEGOTIABLE

⑈300257⑈ ⑆999999999⑆ 111111111⑈

PAYEE NAME ON FILE AT THE BANK

THIS CHECK CLEARS THROUGH POSITIVE PAY

Holder in Due Course

Web: FraudTips.net

Holder in Due Course

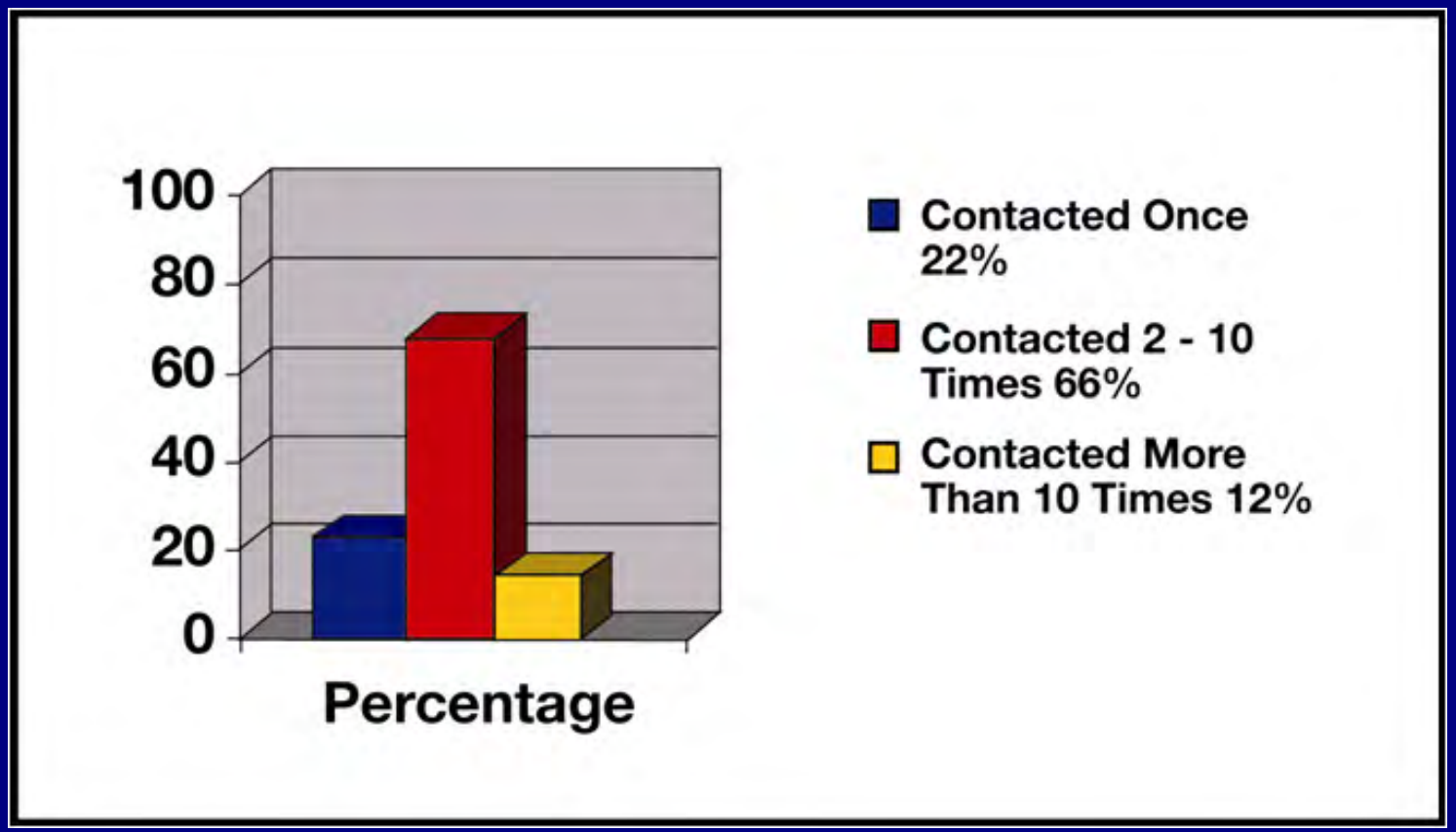
- An innocent party who accepts a check for goods or services
- No evidence of alteration or forgery, or knowledge of fraud by recipient
- Statute of Limitations
  - 10 years from date of issue
  - Three (3) years from date of return
- A Holder in Due Course can sell his/her rights

Holder in Due Course

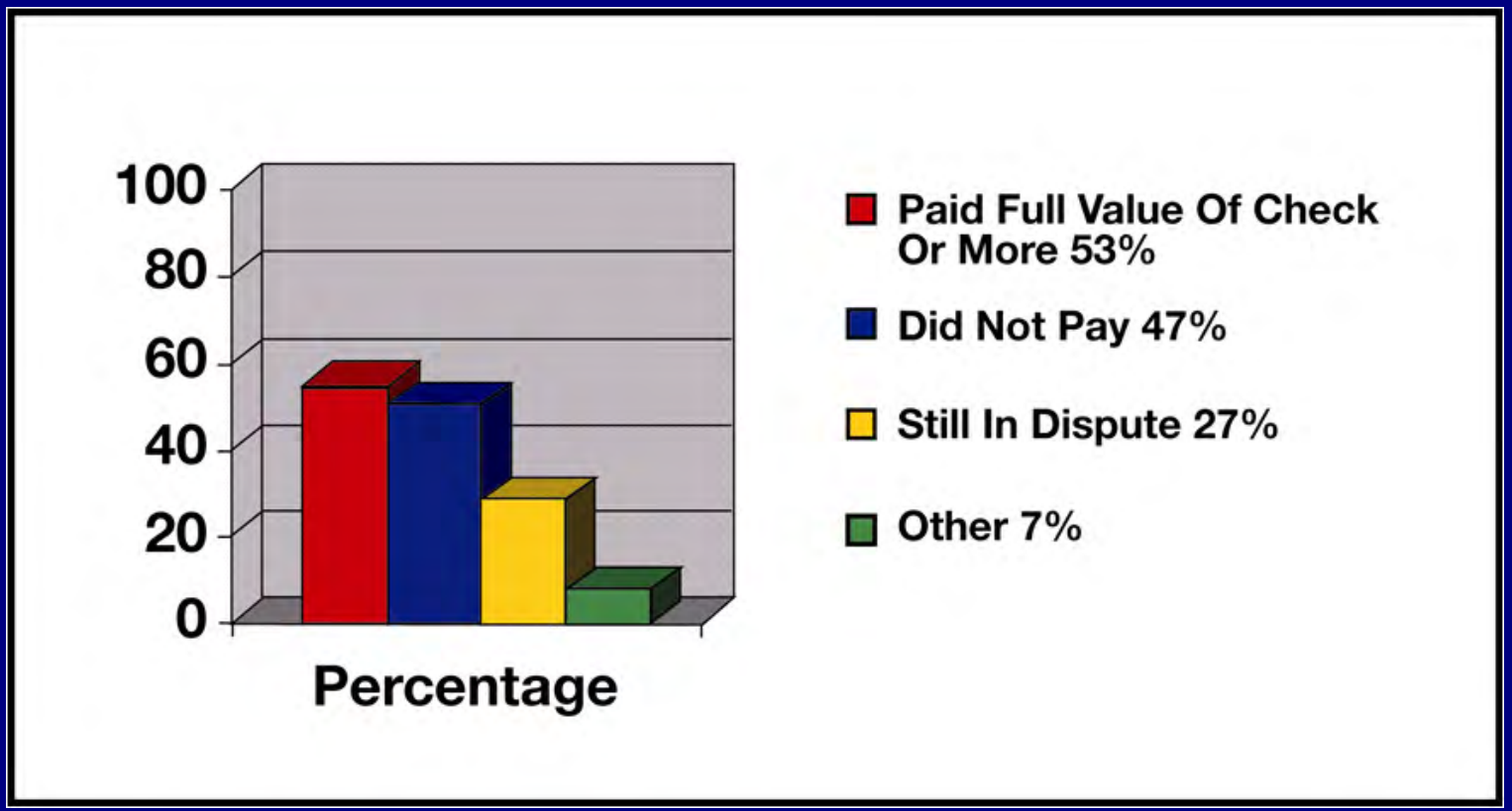
- Trumps Stop Payments
- Trumps Positive Pay

Trump (n.) To get the better of an adversary or competitor by using a crucial, often hidden resource.

Holder in Due Course



Holder in Due Course



Holder in Due Course

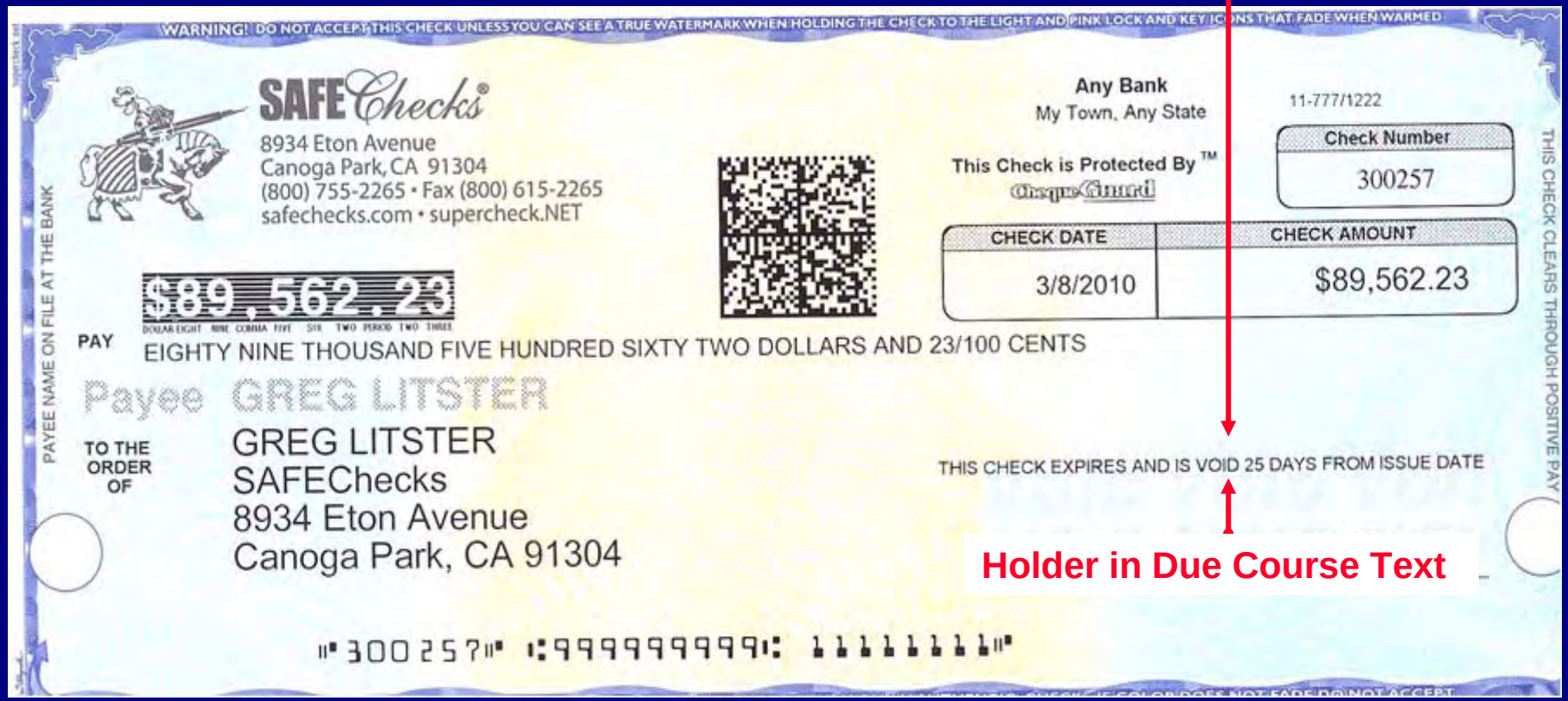
Federal Appellate Court

Lawsuits

Holder in Due Course #1

- Robert Triffin v. Cigna Insurance
  - Two year old check, payment stopped
  - No "expiration date" printed on check
    - UCC rules apply: 3 years or 10 years
  - Print on checks: "This check expires and is void 25 days from issue date"
    - Don't re-issue check until first check expires

Holder in Due Course Text



Holder in Due Course #2

- Robert Triffin v. Somerset Valley Bank and Hauser Contracting Company
  - 80 counterfeit checks on authentic-looking check stock (ADP payroll checks)
  - $25,000
  - Hauser Contracting held liable in both Courts because checks looked authentic
  - Solution: Use controlled, high security check stock that cannot be purchased blank

Who Sells Blank, Uncontrolled Checks?

- Software Companies
  - Bottom Line, Acom, Payformance, Create-a-Check, et. al.
- Deluxe
- John Harland/Clarke American
- SafeGuard
- Superior Press
- Standard Register
- Moore Wallace
- American Solutions for Business
- Office Depot
- Small Print Brokers / Distributors

Who Sells Controlled Checks?

- SAFEChecks

Holder in Due Course #3

- Robert Triffin v. Pomerantz Staffing Services
  - Pomerantz used high security checks with
  - heat-sensitive ink on back, and
  - specific warning banner about authenticating
  - Positive Pay (all 18 checks < $400)

Counterfeits looked authentic on face, but lacked heat-sensitive ink on back

- Triffin LOST; check security features won!

Check 21

"Check Clearing for the 21st Century Act"

Check 21

Allows banks to:

- Convert original paper checks into electronic images
- Truncate the original check
- Process the image electronically
- Create “substitute checks” (paper)

Check 21

Does NOT require banks to:

- Create an electronic check image
- Accept an electronic check image

Does NOT:

- Give an electronic image the legal equivalence of a paper check

Check 21

Does give legal equivalence to:

- a properly prepared “substitute check”

  (aka “image replacement document” (IRD)

Does require banks to:

- Accept substitute checks

Substitute Checks

A Substitute Check MUST:

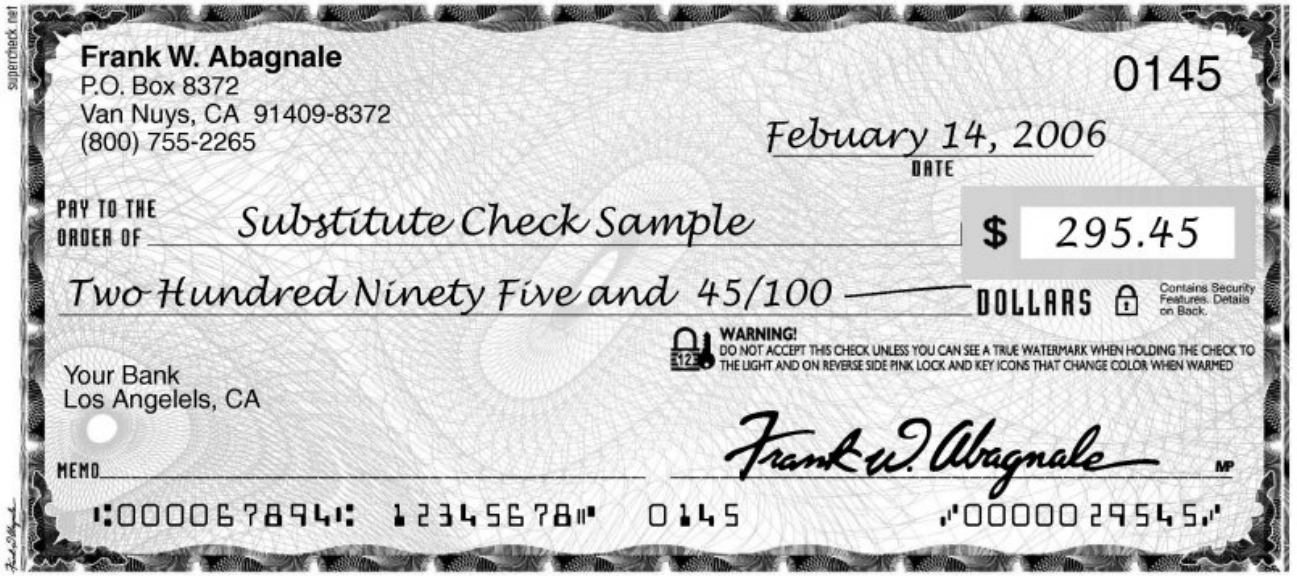
- Contain an image of the front and back of original check
- Bear a MICR line consistent with the original MICR line
- Conform to established standards for substitute checks
- Be suitable for automated processing

Substitute Check Sample

098765187
02/14/2006
3115035506183728

This is a legal copy of your check. You may use it the same way you would use the original check.

[121000374] 02/14/2006
090804712809781



⑆000067894⑆ 123456781 0145 ⑈00000295450⑈

www.FraudTips.net

Check 21

Two Warranties:

- Substitute check is properly prepared
- No “double debit”

Indemnity:

- Converting bank is liable for any loss that is directly related to the paying bank receiving a substitute check

Federal Reserve Board “Final Rule”

A bank “that transfers, presents, or returns a substitute check...shall indemnify the recipient and any subsequent recipient...for any loss incurred by any recipient of a substitute check if that loss occurred due to the receipt of a substitute check instead of the original check.”

Federal Reserve Board example:

"A paying bank makes payment based on a substitute check that was derived from a fraudulent original cashier's check. The amount and other characteristics of the original cashier's check are such that, had the original check been presented instead, the paying bank would have inspected the original check for security features and likely would have detected the fraud and returned the original check before its midnight deadline. The security features that the bank would have inspected were security features that did not survive the imaging process. Under these circumstances, the paying bank could assert an indemnity claim against the bank that presented the substitute check."

Indemnity Claims = Two Conditions

1. Non-image survivable security features
   a. Add features that DO NOT survive the imaging process
2. Dollar Threshold: Bank would have PHYSICALLY INSPECTED the check

   (Banks should lower Sight Review limits)

Indemnity Timeframe

Indemnity claims can be filed One Year from the Cause of Action

1. Cause of action accrues as of the date the injured party first learns of the loss

2. Claims must be made within 30 days after the person has reason to know

3. "Comparative negligence"

Remote Deposit Capture

- New technology streamlines deposit process
- Company scans checks it normally deposits
- Transmits the file of check images to bank
- Bank processes file, sends images for collection to their respective banks
- Images presented for payment electronically or as substitute checks

Remote Deposit Benefits

- Eliminates Paper
- Lower Banking Costs
- Faster Funds Availability
- Higher Acct Analysis & Investment Income
- Quicker notification of a Returned Item
- Geography-independent

Remote Deposit Risks

- Company that converts the check issues the warranties and indemnity
- Company can be held liable for converting a counterfeit or altered check

Consumer Remote Deposit

- Consumer remote deposit capture is VERY hazardous to banks because...
- Dishonest customers can make “remotely created checks,” deposit remotely, pull out cash, and abandon the account.
- The depositing bank is liable, not the paying bank.

Remote Deposit Capture

Q: How long should paper checks be stored?
A: At least 60 days

- Scenario: Counterfeit or altered check is truncated on 2nd day of a month
- Bank sends customer (injured party) its bank stmt by 5th day of following month-33+ days
- Under the UCC, Injured Party has 30 days to reconcile after bank statement is sent

How to turn $12.00 into $90,000

Turn $12 → $90,000

1. Company issued $12 check; check was stolen
   - Company NOT on Positive Pay
2. $12 check became $90,000; was deposited
3. Bank converted $90,000 check into an image
4. Check image paid, but not discovered for 11 days
5. Who is liable for the loss?
6. Depends on security features in the original check!

ATM Fraud

Card & PIN Thefts

Stealing PINS is now a major activity of cyber criminals.

This person lookd like he is using a bank ATM...

But, he’s not. He is a thief.

What is he really doing?

Setting a trap in the ATM machine to “capture” the next user’s card.

Altering ATMs is very risky business.

Thieves work in teams.

The “lookout” warns of possible witnesses and of the next potential victim.

The trap has been set.

The next client uses the ATM.

He inserts his card and begins his transaction.

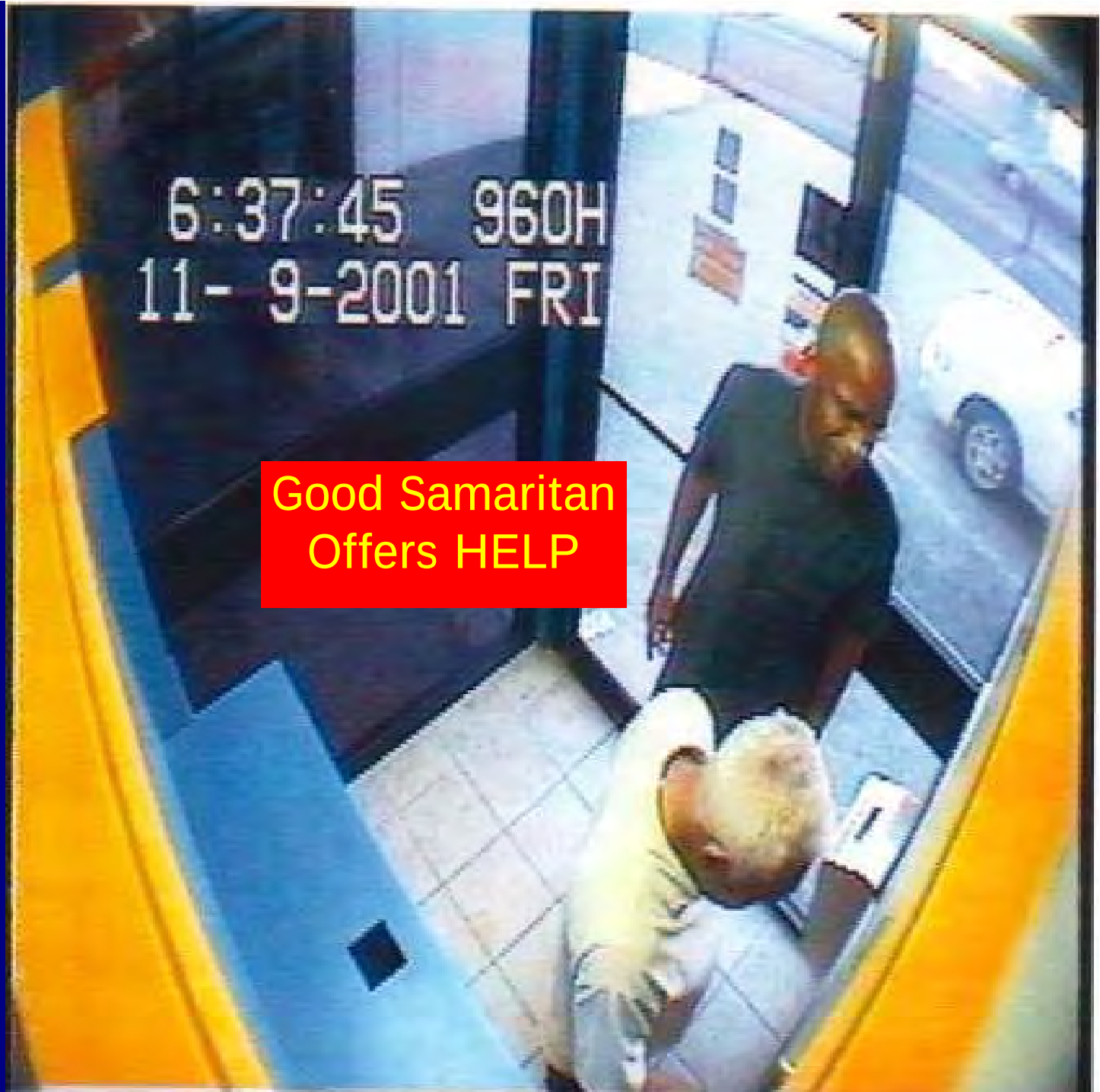
The ATM card is confiscated. The customer is confused.

“Why has my card been confiscated?”

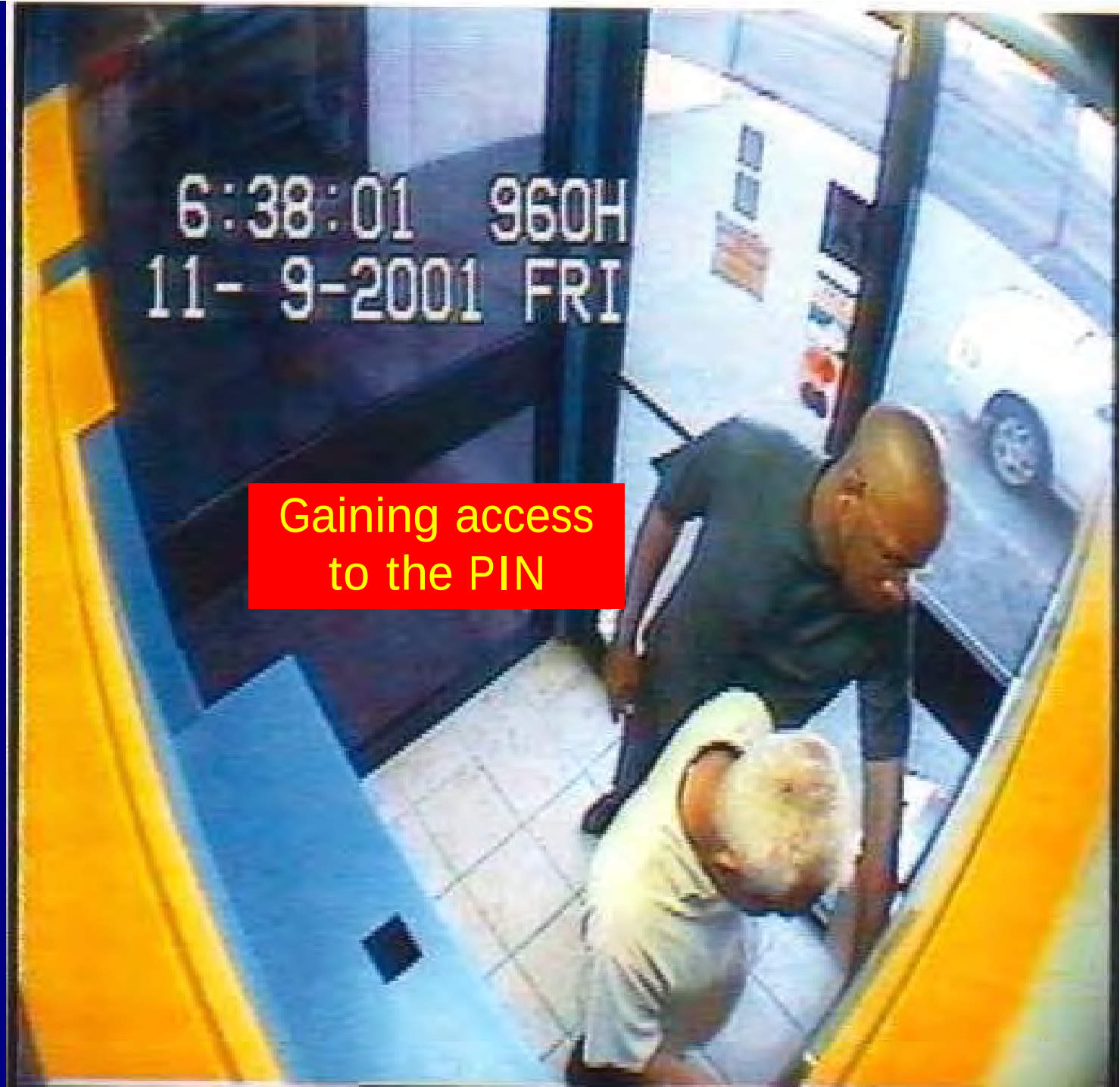
But wait!
A “Good Samaritan” is about to help !!!

The Good Samaritan pretends to help. His trap has the ATM card.

Now he tries to obtain the customer's PIN.

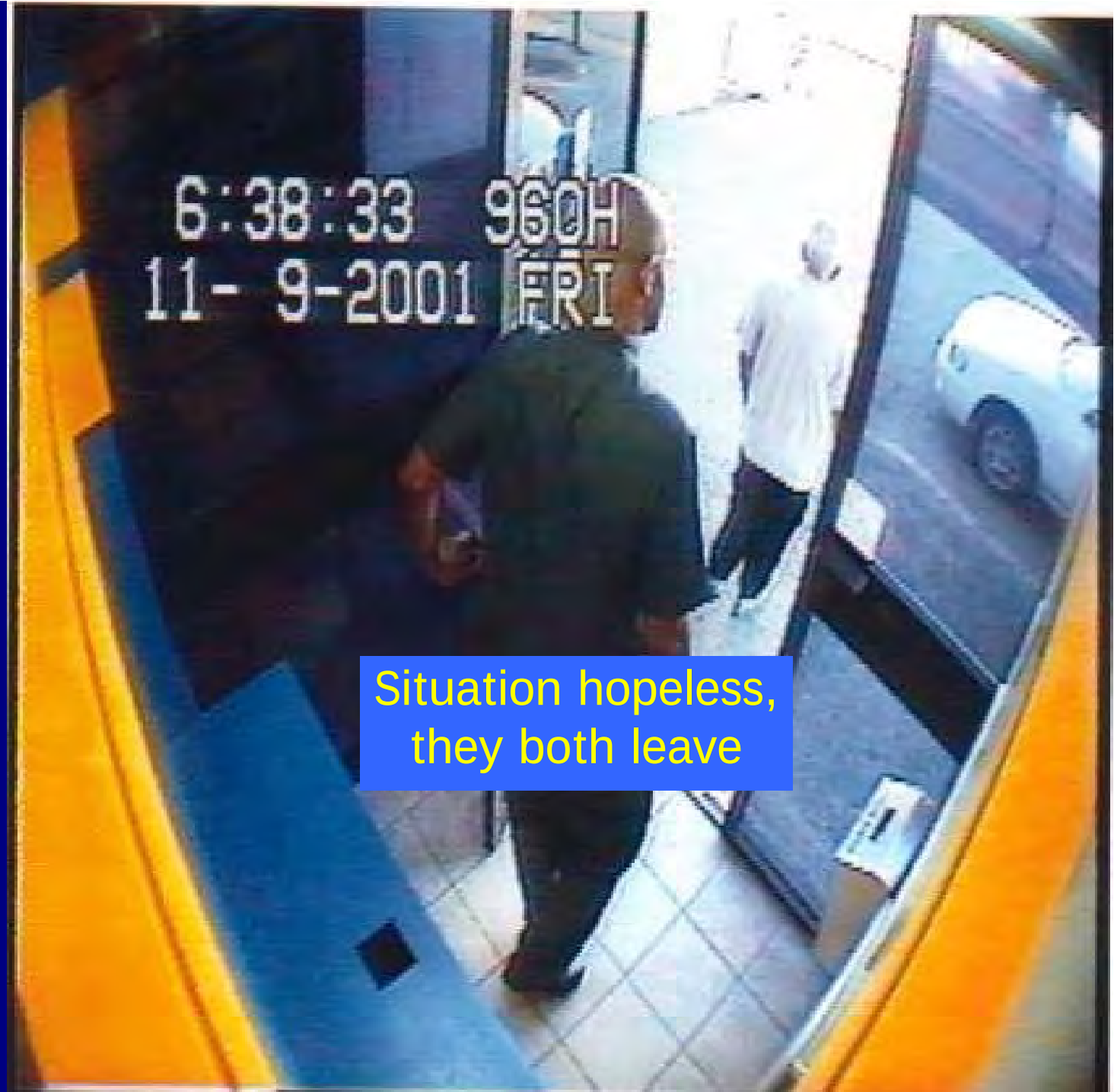


The Good Samaritan convinces the customer he can recover the card if he enters his PIN while the Good Samaritan presses “Cancel” and “Enter.”



After several failed attempts, the customer is convinced his card has been confiscated.

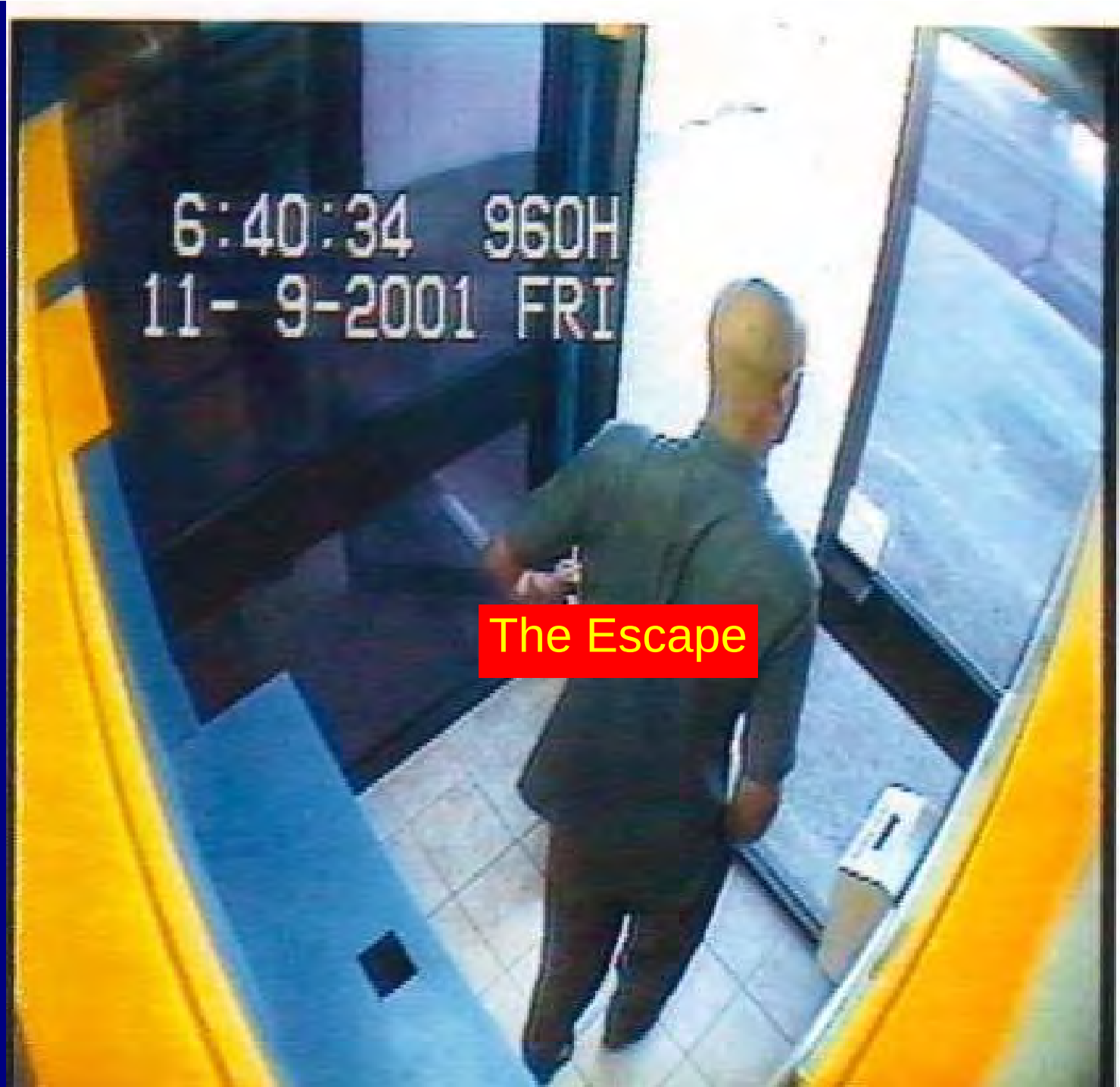
Customer and Good Samaritan leave the ATM.



Satisfied the coast is clear, the thief returns to recover the confiscated card from his trap.

He has the card AND the PIN.

In possession of the card and the PIN, he leaves the ATM with money withdrawn from the Customer's account.



The trap is made up of XRAY film.

XRAY film is the material preferred by thieves because of the black color that looks similar to the slot on the card reader.

The trap is carefully inserted into the ATM slot.

The ends are folded and have glue strips that adhere to the inner and outer surface of the slots.

When the ends are firmly glued to the card slot, it is almost impossible to detect by unsuspecting ATM clients

How your card is confiscated

Slits are cut into both sides of the trap.

This prevents the card from being ejected prior to completing your transaction.

When the customer has left, the thief removes the glued trap by grasping the folded tips and pulling the trap and retained card out.

They have your PIN!

If your card is confiscated, check the ATM slot for tampering.

If you see film tips glued to the slot, pull the trap out to recover your card.

Report to the bank ASAP!

Contact Us!

www.safechecks.com

greg@safechecks.com

(800) 949-2265