The New Faces of Fraud

and

How to Thwart Them

Presented at

SoCal EXPO

By Greg Litster, SAFEChecks

Mobile Banking/Deposit Fraud:

Slides #3 – 6

Check Fraud and Payment Fraud:

Slides #7 – 91

Cyber Crime:

Slides #92 – end

Mobile Banking
and
Deposit Fraud

Mobile Banking and Deposit Fraud

Scenario: A title insurance company gives John Doe a check at closing. John Doe steps outside, deposits the check via a mobile app, then comes back in and returns the check, asking that it be made payable to John Doe and Jane Doe.

Mobile Banking and Deposit Fraud

The company does not think to put a Stop Payment on the first check, because they have the physical check in hand.

---

1. If a physical check is returned for a replacement, place a stop payment on the returned check. It may have been deposited remotely.

2. Recipient MUST sign an affidavit stating the check was not "deposited."

3. An Affidavit does not provide protection, only a right to sue and collect legal fees.

Check Fraud...

Why talk about Check Fraud?

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

Association for Financial Professionals (AFP)

2013 Payments Fraud Survey:

"Checks remain the most popular vehicles for criminals committing payments fraud, even though the corporate use of checks has declined."
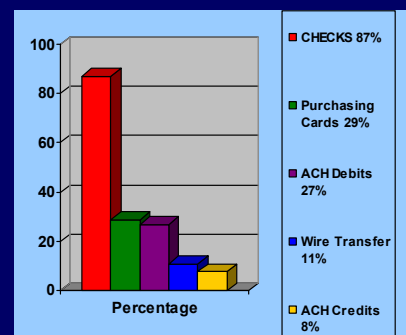

Association for Financial Professionals (AFP)

2011 Payments Fraud Survey:

"Checks continue to be widely used and abused, and fraud via check payments remains the overwhelming threat faced by companies."
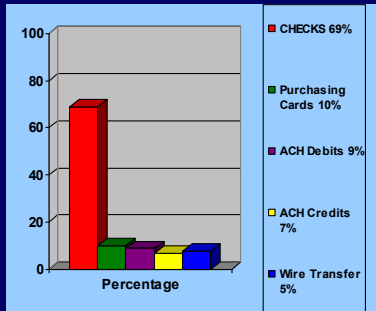

Total Non-Cash Payments by Method
(Transactions)
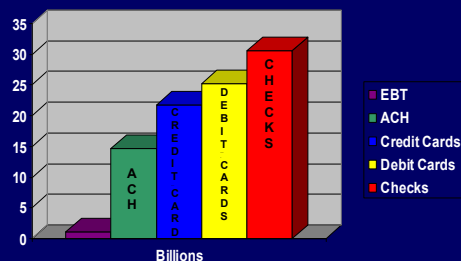
Fraudulent Payments by Method
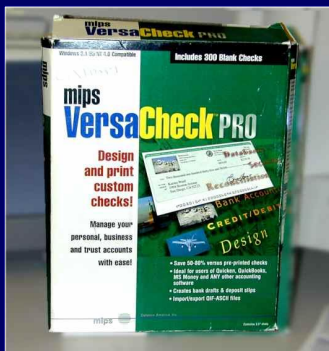### (Some Respondents were hit multiple ways; total > 100%)

Fraud <u>Losses</u> by Method
(How Dollars were actually lost)

- CHECKS 69%
- Purchasing Cards 10%
- ACH Debits 9%
- ACH Credits 7%
- Wire Transfer 5%

Frank Abagnale

Catch Me If You Can

<u>Technology</u> is making Frank Abagnale's "gift" achievable by mere mortals

---

The Evolution

of

Check Fraud

and

Banker Solutions

Counterfeit Checks

...Banks developed Positive Pay

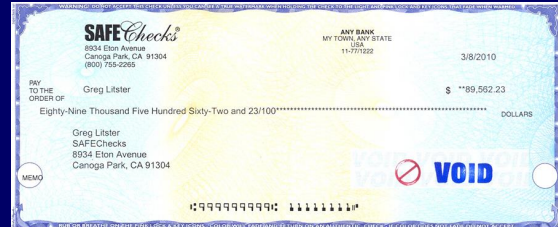
Altered Payees

...Banks developed <u>Payee</u> Positive Pay

Added Payee Names

Checks pass right through Payee Pos Pay!

How?

Typical Check Layout

Typical Check Layout

Open Areas Where Forgers Add A New Payee Name

Added Payee printed 2 lines above the original Name

Added Payee Names

No Banker Solution!

(There is a software solution....)

Strategies to Prevent Check Fraud

Don't Write Checks!

- **Use Commercial Purchase Cards**
- **Pay electronically (ACH)**

Commercial Purchase Card Benefits

1. Reduces check writing and check fraud risk
2. Does not expose the checking account number
3. Terminating a card is easier than closing a checking account.
4. Reduces bank per-item fees
5. Increases payment float by 40+ days
6. Reduces interest expense
7. Potential for Rebates or Rewards

ACH Payment Benefits

1. Reduces check writing and check fraud risk
2. Does not expose the checking account number
3. Reduces late fees
4. Reduces mailing expense and bank fees
5. Pay 1 invoice at a time, or
6. Pay multiple invoices and email remittance detail

If you're going to write checks...

#1. High Security Checks

Effective check fraud prevention strategies begin with a
<u>high security check</u>

High Security Checks

1. Deter the forger (psychological warfare)
2. Thwart attempts to replicate or alter the check
3. May help protect you legally from some Holder in Due Course claims

What makes a check secure?

10+ safety features

Important Security Features

- **Controlled** Check Stock
- Dual-tone True Watermark
- Thermochromatic Ink (reacts to heat)
- Correctly Worded Warning Banner
- Toner Anchorage
- Copy Void Pantograph
- Chemical-reactive Ink + Paper
- Inventory Control Number on Back (laser)
- UV Ink + UV Fibers
- Microprinting
- Laid Lines

"Controlled" Check Stock is the most critical security feature

"Controlled" check stock is check stock that is unique to each company

Uncontrolled check stock is check stock that is sometimes sold entirely blank to anyone (including fraudsters)

Uncontrolled check stock

is a major contributor to check fraud.

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

How to Obtain Controlled Checks?

- Custom Manufacture with an ORIGINAL design and include at least 10 security features

  or

- Abagnale's SuperBusinessCheck (16 features)
- SAFEChecks (12 features)

6

#2. Payee Positive Pay

Web: PositivePay.net

Positive Pay...

...a powerful tool!

Added or Altered

Payee Names

Lawsuit

Cincinnati Insurance Company

v.

Wachovia Bank

$154,000 Loss from an Altered Payee

Preceding Events

Schultz Foods had 4 check fraud attempts against their account.

Wachovia repeatedly encouraged Schultz Foods to use Positive Pay.

Schultz Foods does NOT use Positive Pay, but it buys check fraud insurance.

Facts

Dec. 1, 2005: Schultz Foods issues $154,000 check payable to Amerada Hess Corporation.

Facts

$154,000 check is intercepted and stolen.

Payee Name changed to "Kenneth Payton."

Kenneth Payton, an unwitting participant, deposits $154,000 check into TCF Bank.

Wachovia pays the altered check.

Facts

Per instructions, Kenneth Payton keeps $3,500 and wires $150K to Singapore to "...help a refugee South African family."

The money disappears.

Facts

January 2006: Schultz Foods notifies Wachovia Bank of Altered Payee and demands repayment.

Wachovia demands repayment from TCF Bank (bank of first deposit).

Facts

Wachovia Bank pursues TCF Bank for $154,000; does not pay Schultz Foods.

Schultz Foods makes a claim under its policy; Cincinnati Insurance Co. pays Schultz Foods $154,000.

Cincinnati Insurance Co. sues Wachovia Bank for $154,000.

Facts

Wachovia had a "defense" against Schultz Foods and its insurance company: A Signed Deposit Agreement

Under UCC § 3-119, TCF Bank's attorneys, acting for Wachovia Bank, use Wachovia's "deposit agreement defense" against Cincinnati Insurance Co.

Resolution:

Wachovia Bank Wins!

This case demonstrates you can have a great relationship with your bank and still lose a lawsuit!

8

If…

Schultz Food's <u>had used Positive Pay</u>,

the check <u>may not</u> have paid, and

there <u>may not</u> have been a loss!

(Exception: Added Payees)

Preventing

<u>Altered</u> Payee Names


Preventing <u>Altered</u> Payees

➢ **High-security checks**
  ˜ Includes "toner anchorage"

➢ **Use 14 point font for Payee Name**

➢ **High-quality toner**

➢ **Hot laser printer**
  ˜ Highest temperature setting available
  ˜ Replace fuser element every 2-3 years

➢ **Positive Pay with Payee Name Recognition**

Frank Abagnale Fraud Bulletin, Page 7:
A Primer on Laser Printing

Preventing

<u>Added</u> Payee Names

Typical Check Layout

Open Areas Where Forgers Add A New Payee Name
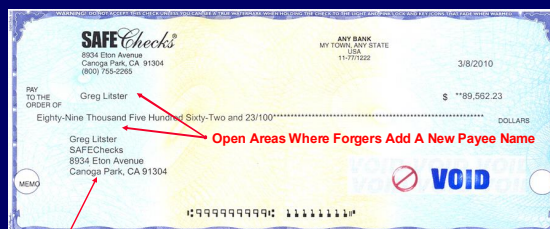
10 point font

<u>Identical</u> check data strengthened by software

There is no room for an Added Payee

"Secure Seal"

is an
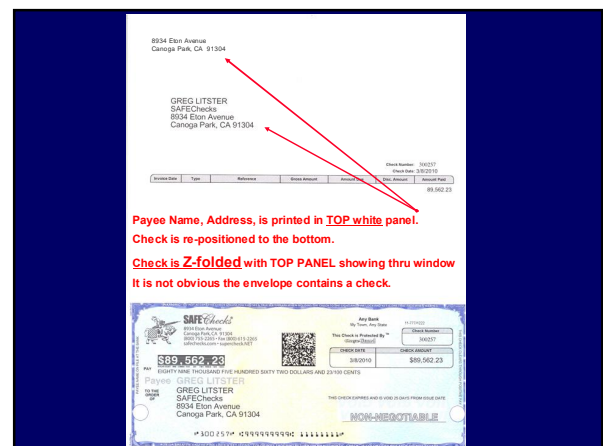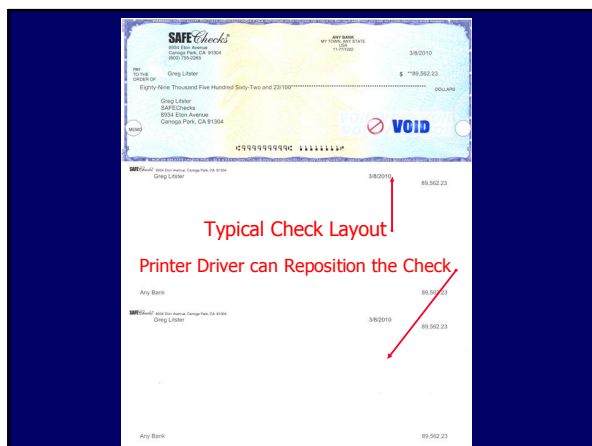
image-survivable
encrypted barcode
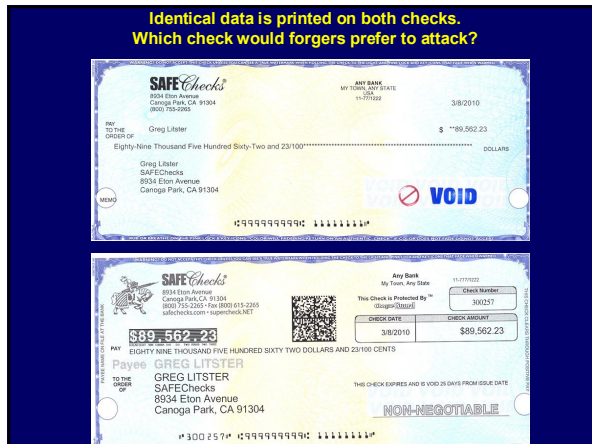
Barcode contains:

1. Drawer
2. Payee Name
3. Dollar Amount
4. Issue Date
5. Check Number
6. Account Number
7. Routing/Transit Number
8. X,Y coordinates on the check face of each data piece
9. Date and Time Check was printed
10. Laser Printer used
11. The employee that printed the check

Barcode is created

by a
Printer Driver

Printer driver can:

1. Accumulate check data for Positive Pay
2. Change Font size
3. Add Barcode, Secure Name & Number fonts
4. Be configured to send Pos Pay files to the bank automatically
5. Reposition Check Placement

Typical Check Layout

Printer Driver can Reposition the Check

Payee Name, Address, is printed in TOP white panel.
Check is re-positioned to the bottom.

Check is Z-folded with TOP PANEL showing thru window
It is not obvious the envelope contains a check.

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

#3. Timely Account Reconciliation

#4. Tight Internal Controls

Tight 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

Uniform Commercial Code (UCC)

Uniform Commercial Code

"**Ordinary Care**"

and

"**Contributory Negligence**"

determine Bank's and Customer's degree of liability for fraud.

Ordinary Care (Bank)

➢ **Electronic Check Presentment**

➢ **Check Truncation (Imaging)**

➢ **Selective Check Inspection**

Uniform Commercial Code

‰reasonable commercial standards <u>do not require the bank to examine the instrument</u> if the failure to examine does not violate the bank's prescribed procedures and the bank's procedures do not vary unreasonably from general banking usage...+

Ordinary Care (Drawer)

‰.in the case of a person engaged in business means <u>observance of reasonable commercial standards</u>, prevailing in the area in which the person is located, and with respect to the business in which the person is engaged...+

Contributory Negligence

➢ **Bank acts with ORDINARY CARE**

➢ **DRAWER fails to act with ORDINARY CARE (i.e. Drawer is negligent)**

➢ **If that negligence contributes substantially to the forgery…**

BANK HAS NO LIABILITY!

Holder in Due Course

Web: FraudTips.net

Holder in Due Course

➢ An innocent party who accepts a check as payment for goods or services

➢ No evidence of alteration or forgery on face of the check, or knowledge of fraud by recipient

➢ **Statute of Limitations**

˝ 10 years from date of issue

˝ Three (3) years from date of return

➢ <u>A Holder in Due Course can sell his/her rights</u>

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

Federal Appellate Court

Lawsuits

Holder in Due Course #1

➢ <u>Robert Triffin</u> v. Cigna Insurance

″ Two year old check, payment stopped

″ No "expiration date" printed on check
  ◼ UCC rules: <u>3 years or 10 years</u>

″ Print on check face: "This check expires and is void 25 days from issue date"
  ✓<u>Don't re-issue check until first check expires</u>

Holder in Due Course Text

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 ™   Check Number 300257

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

$89,562.23

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⑈ ⑈⑈⑈⑈⑈⑈

Someone who accepts an

<u>expired instrument</u>

Has No Legal Standing!

as a Holder in Due Course

Holder in Due Course #2

➢ <u>Robert Triffin</u> 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 <u>controlled</u>, high security check stock that cannot be purchased blank

Who Sells Blank, <u>Uncontrolled</u> 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

How to Obtain <u>Controlled Checks</u>?

- Custom Manufacture with an ORIGINAL design and include at least 10 security features

  or

- Abagnale's SuperBusinessCheck (16 features)
- SAFEChecks (12 features)

Holder in Due Course #3

- <u>Robert Triffin</u> 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 Fraud Scams

Check Fraud Scams

- "...you have won a large award...taxes must be prepaid on the award, but a check for a portion of the award will be mailed to you...."

- Someone buys something from you and pays with a check that exceeds the purchase price. You are instructed to deposit the check, keep what you are owed, plus $100 "for your trouble," and to wire the purchaser the rest of the money. Of course, the check is bad.
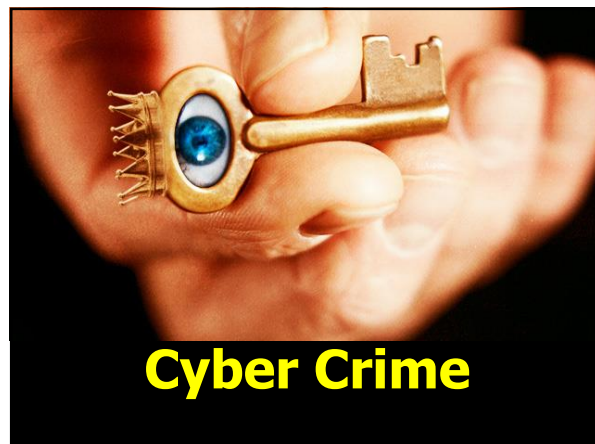
Check Fraud Scams

- Altered Names / Dollar Amounts
- Added Payees Names (beats Payee Positive Pay)
- Check Counterfeiting
- Check Washing
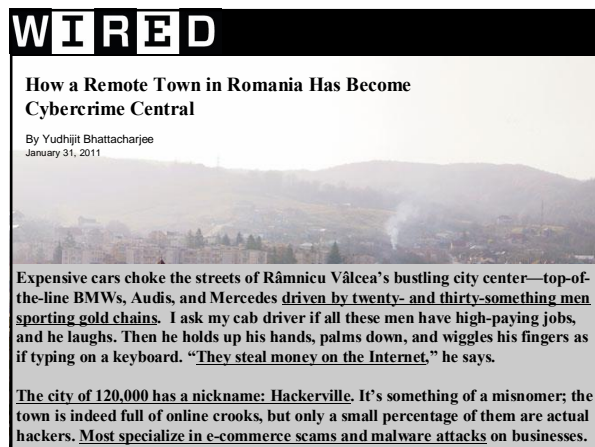- Online Lottery Winners (Holder in Due Course)
- Bogus Cashier's Checks

15

ACH Fraud

˝ Utilize ACH Filter or Block

˝ Select "Return All" as your default choice for
    ACH Debit Filter

˝ Set maximum debit limit for all Approved Vendors

˝ Be alert for small dollar ($1) ACH debits/credits

Cyber Crime

WIRED

How a Remote Town in Romania Has Become Cybercrime Central

By Yudhijit Bhattacharjee
January 31, 2011

WIRED

How a Remote Town in Romania Has Become Cybercrime Central

By Yudhijit Bhattacharjee
January 31, 2011

Expensive cars choke the streets of Râmnicu Vâlcea's bustling city center—top-of-the-line BMWs, Audis, and Mercedes driven by twenty- and thirty-something men sporting gold chains. I ask my cab driver if all these men have high-paying jobs, and he laughs. Then he holds up his hands, palms down, and wiggles his fingers as if typing on a keyboard. "**They steal money on the Internet,**" he says.

The city of 120,000 has a nickname: Hackerville. It's something of a misnomer; the town is indeed full of online crooks, but only a small percentage of them are actual hackers. **Most specialize in e-commerce scams and malware attacks** on businesses.

Video
Rock Center – Brian Williams

Keystroke Logger Virus

Tracks every keystroke; sends hourly reports to hacker
Spreads by:
     - Internet (email, Web sites)
     - Infected files on network
     - USB drive or CD

Pharming

Hacker's attack to <u>redirect a legitimate website's traffic</u> to a fraudulent website.
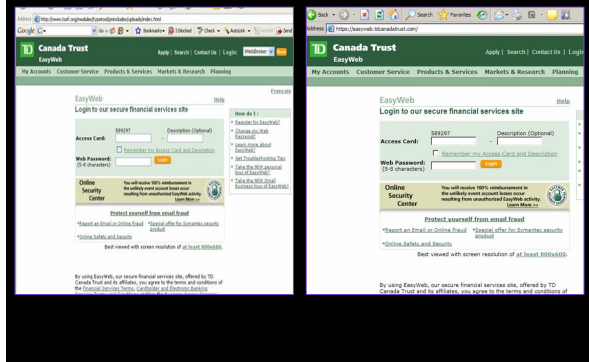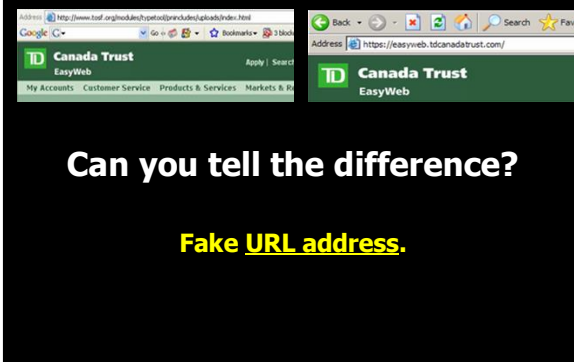
Hacker is paid by the click.

Phishing

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

<u>Purpose</u>: Steal user names, passwords, personal info, introduce a virus attack
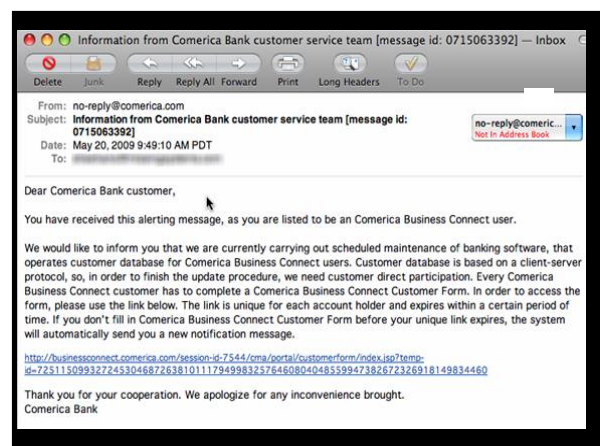
Phishing Hosts

Phishing Hosts

Can you tell the difference?

Fake <u>URL address</u>.

Phishing Bogus Emails

"Dear clients,

Your account **ACH and Wire transactions** have been **temporarily suspended** for your Security, due to the expiration of your security version. To download and install the **newest Updates**, follow this <u>link</u>. As soon as it is set up, your transaction abilities will be fully restored. Best regards, Online security department, Federal Deposit Insurance Corporation."

Can lead to "account takeovers"

Information from Comerica Bank customer service team [message id: 0715063392] — Inbox

Delete   Junk   Reply   Reply All   Forward   Print   Long Headers   To Do

From: no-reply@comerica.com
Subject: Information from Comerica Bank customer service team [message id: 0715063392]
Date: May 20, 2009 9:49:10 AM PDT
To:

no-reply@comeric...
Not In Address Book

Dear Comerica Bank customer,

You have received this alerting message, as you are listed to be an Comerica Business Connect user.

We would like to inform you that we are currently carrying out scheduled maintenance of banking software, that operates customer database for Comerica Business Connect users. Customer database is based on a client-server protocol, so, in order to finish the update procedure, we need customer direct participation. Every Comerica Business Connect customer has to complete a Comerica Business Connect Customer Form. In order to access the form, please use the link below. The link is unique for each account holder and expires within a certain period of time. If you don't fill in Comerica Business Connect Customer Form before your unique link expires, the system will automatically send you a new notification message.

http://businessconnect.comerica.com/session-id-7544/cma/portal/customerform/index.jsp?temp-id=72511509932724530468726381011179499832576460804048559947382672326918149834460

Thank you for your cooperation. We apologize for any inconvenience brought.
Comerica Bank

Lawsuit

Experi-Metal, Inc.

v.

Comerica Bank

"Phishing" Attack:

CFO responds with to email with his login

Lawsuit

Experi-Metal, Inc.

82 Wires, $5,200,000

$560,000 Loss

Company sued the bank.

Company sued the bank.

**Who won the lawsuit?**

Company sued the bank.

Who won the lawsuit?

The Customer!

WHY did the Bank lose?

1. **Bank wired out funds <u>exceeding</u> Customer's Actual Account Balance (OD = $5MM)**
   (This programming error has been remedied!)

2. **Five (5) other companies were hit that day**

3. **Company "won" lawsuit against Comerica, <u>but</u>**

4. **Was <u>not</u> awarded attorney fees   (> $250K)**

Facebook

1 Billion Users

Hi Jeff,

FAKE URL

Here
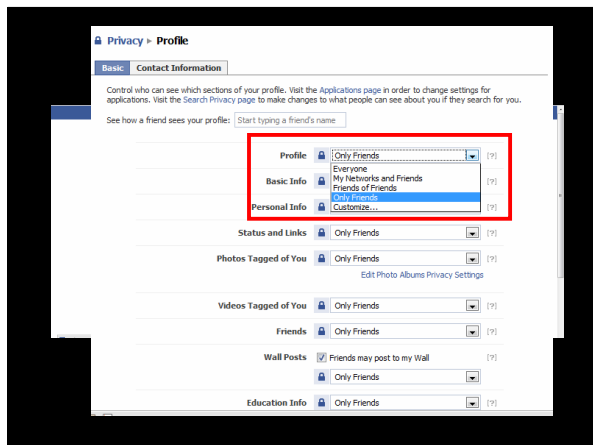
"Physical" Attacks –

"Skimmers" in credit/debit card devices

Infected flash/thumb drives

"Vishing" –
Using the telephone to get
personal information, using real
names known to the victim.

New Types of
Cyber Attacks

Criminals are targeting
smartphones and tablets

"Smishing" –
Using a text message to get
personal information.

Industry experts expect mobile
threats to eventually surpass
threats to PCs.

10% of mobile applications leak
logins and passwords, 25%
expose personally identifiable
information (PII) and 40%
communicate with third parties.

%Cybercrime: This Is War+ Report by JPMorganChase 3/2013

- Many downloadable applications lack any
encryption, and many insecurely share
information.

- 30 percent of apps have the ability to
obtain a device $ location without the user's
consent.

- 14.7 percent of apps request permissions
that could lead to the initiation of phone
calls without user knowledge.

Juniper Networks, 2011 Mobile Threats Report

Mobile web browsers also present
threats. Browser-based attacks can
be launched by simply visiting an
infected site.

Juniper Networks, 2011 Mobile Threats Report

Solutions

Smartphone & Tablet Security

http://mobile-security-software-review.toptenreviews.com/

http://www.pcmag.com   *15 Mobile Security Tools*

Use a properly configured FIREWALL,
which helps make your computer
invisible on the Internet.

Anti-Virus, Anti-Spyware Software

Software to identify, neutralize or eliminate malicious code

 - Monitors behavior of all programs.

Online Banking

Require 2 different computers
to move money.

1. Computers #1-99 to "originate"

2. Computer #100 to "release"

Use a Layered Approach for Wires & ACH

˝ Dual Factor Authorization
   ˝ (*"something you have (token), and something you know"*)

˝ %Out of Band+Authentication
   ˝ (text msg from bank with password for that specific wire)

˝ Tokens

˝ Transactional Alerts via
   ˝ Text
   ˝ E-mail
   ˝ Voice call back (human confirmation)

Email Server Protection

(Better protection with more users)

Protect Passwords

	10 Most Popular Passwords
1	123456
2	12345
3	123456789
4	Password
5	qwerty

	10 Most Popular Passwords
6	trustno1
7	abc123
8	monkey
9	letmein
10	dragon

Cracking Passwords

The most important single contribution to cracking came in 2009, when an attack against online games service RockYou.com exposed 32 million plaintext passwords used by its members to log in to their accounts. The passcodes were posted online. **Overnight, the way hackers cracked passwords changed.**

The RockYou.com list confirmed nearly all CAPITAL LETTERS come at the beginning of a password. Almost all NUMBERS and PUNCTUATION show up at the end.

It also revealed a strong tendency to use first names followed by years, such as Julia1984 or Christopher1965.

Passwords Posted on the Web

Last Year

100,000,000+

---

5 Years Ago

**The Time it Took a Hacker
to Randomly Guess Your Password**

Length	lowercase	+ Uppercase	+ numbers and symbols
6 Characters	10 Minutes	10 Hours	18 Days
7 Characters	4 Hours	23 Days	4 Years
8 Characters	4 Days	3 Years	463 Years
9 Characters	4 Months	178 Years	44,530 Years

Today:

**It Takes a Hacker 12 Hours
to Randomly Guess Your Password**

Length		Upper + Lower + Numbers + symbols
8 Characters		12 Hours

This $12,000 computer containing 8 AMD Radeon GPU cards can brute force the entire keyspace for any eight-character password in 12 hours.
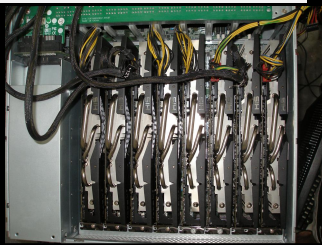
Asd09871234zxcvvconradfcvg crp3adm3
xzlkjhyuiogrdswaglitsxcvfdtermnbvFESS
Muniondesxcbswanhkmnb.com

Asd2071300042 zxcv0713vcxz lkKatieJean jhyuiogreglitster
Mnbv greg@safechecks.com
unionbank.com

zxcvbnmjklacapulco

www.logmein.com

qaswdc096524rfvfraves ginaRobinJohnson

fultonhjlk8934etonavecanogaparkca91304xcvcb
info_SSAFEVVFGSsjkrobinzxcvbnmalisaelainesjklrobin_sklejk

_SSAFE
214598fdseaced02_101285xcvnm,4037nm,.8400uipohkl185
hjklj5449jkl;0114bnm,779 zxcvcrp3adm3usbank

Asd09871234zxcvvconradfcvg crp3adm3
xzlkjhyuiogrdswaglitsxcvfdtermnbvFESS
Muniondesxcbswanhkmnb.com

Asd2071300042 zxcv0713vcxz lkKatieJean jhyuiogreglitster
Mnbv greg@safechecks.com
unionbank.com

zxcvbnmjklacapulco

www.logmein.com

qaswdc096524rfvfraves ginaRobinJohnson

fultonhjlk8934etonavecanogaparkca91304xcvcb
info_SSAFEVVFGSsjkrobinzxcvbnmalisaelainesjklrobin_sklejk

_SSAFE
214598fdseaced02_101285xcvnm,4037nm,.8400uipohkl185
hjklj5449jkl;0114bnm,779 zxcvcrp3adm3usbank

Wall Street Journal
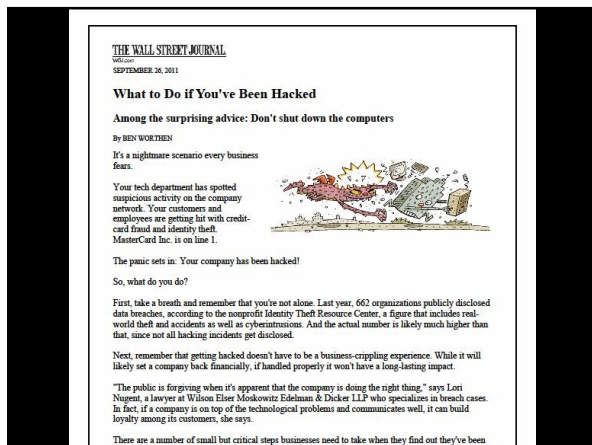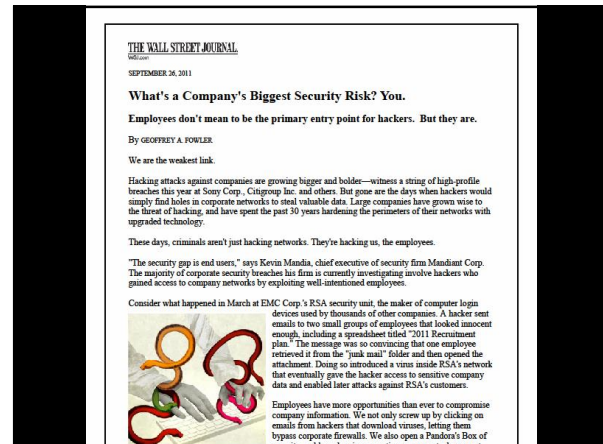
Track Your Kids Keystrokes

Kids keep 2 Facebook Accounts
(Mom only sees one)

Track Your Kids' Keystrokes

Track Your Kids' Keystrokes

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

eBlaster forwards incoming and outgoing emails to your email address.

Spectorsoft.com/mobile

Spectorsoft.com/mobile

Track Your Employees

www.NoSlang.com

Internet Slang Dictionary & Translator

www.NoSlang.com
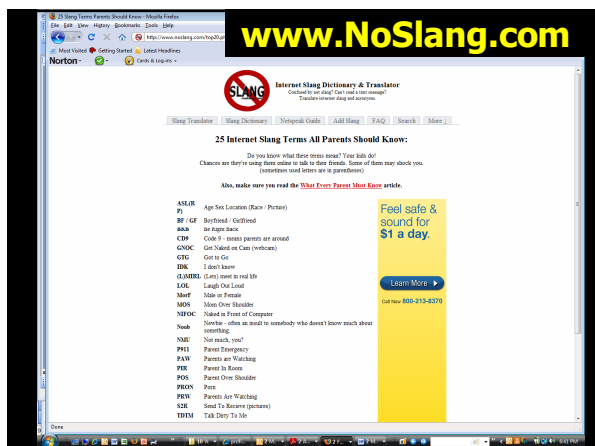
Please review **Resources**

in Abagnale Fraud Bulletin

Page 11

Greg Litster
President
SAFEChecks
(800) 949-2265 direct
(818) 383-5996 cell
greg@safechecks.com