Cybercrime, Mobile Banking Fraud, Check Fraud, Embezzlement

Greg Litster
SAFEChecks
(800) 949-2265
GLITSTER@aol.com
greg@safechecks.com

Smartphones and Tablets

Criminals are targeting smartphones and tablets

Mobile malware grew 155% in 2011

and

614% from March 2012 to March 2013

Juniper Networks, 2013 Mobile Threat Report

"There are several indicators of a shift in mobile malware, from being a cottage industry to a more developed market…"

Juniper Networks, 2013 Mobile Threat Report

Targeting Markets with Greatest ROI

Shortened Supply Chains and Distribution

Multiple Paths to Market

Juniper Networks, 2013 Mobile Threat Report

Industry experts expect mobile threats to surpass PC threats.

- 10% of mobile apps leak logins or passwords
- 25% expose personally identifiable info (PII)
- 40% communicate with third parties.

"Cybercrime: This Is War" Report by JPMorganChase 2013

An emerging trend:

“Spear Phishing” attacks (Trojans) on Android device apps that allow users to download Gmail attachments.

It can compromise the mobile devices and the PCs or Macs to which these devices connect….

Kaspersky Lab - research April 2013

Spear Phishing is based on social engineering…. Fraudsters gather information about mobile users through groups with which they are affiliated, as well as social media channels.

Kaspersky Lab - research April 2013

App Security

Product Reviews: CNET.com, PCmag.com

MyLookOut, Bullguard, etc.)

Mobile Banking and Deposit Fraud:

Double Debits

Mobile Banking Deposit Fraud

Scenario: A check is mailed to Dishonest Dan

- Dan deposits the check using smart phone app
  - Digitized check is paid at drawer's bank
- 10 days later, Dan cashes the same check at a check cashing store
  - 2nd check hits the drawer's bank account (check is presented for payment twice)
- **WHO TAKES THE LOSS??**

The answer is found in the Rules governing Check 21

Mobile Banking & Check 21

1. "Mobile Banking" is another form of Remote Deposit Capture
2. Remote Deposit Capture is part of Check 21
3. Check 21 has specific rules that govern Remote Deposit Capture, which includes Mobile Banking
4. Rules determine who takes the loss, and why

Check Clearing for the 21st Century Act

- Check 21 law enacted on October 28, 2003; became effective on October 28, 2004
- Allows the recipient of an original paper to create a digital version of the original check, and deposit the digital image electronically.
- Under Check 21's "warranty" provision, the converting party warrants that it will not present the check for payment twice.

Check 21 Rules

§ 229.52 Substitute check warranties

- A bank that transfers, presents, or returns a substitute check (or a paper or electronic representation of a substitute check)… warrants… that—

§ 229.52 Substitute check warranties

- (2) No depositary bank, drawee, drawer, or indorser will receive presentment or return of, or otherwise be charged for, the substitute check, the original check, or a paper or electronic representation of the substitute check or original check such that that person will be asked to make a payment based on a check that it already has paid.

§ 229.52 Substitute check warranties

(b) Warranty recipients. A bank makes the warranties… to the person to which the bank transfers, presents, or returns the substitute check or a paper or electronic representation of such substitute check and to any subsequent recipient, which could include a collecting or returning bank, the depositary bank, the drawer, the drawee, the payee, the depositor, and any indorser. These parties receive the warranties regardless of whether they received the substitute check or a paper or electronic representation of a substitute check.

§ 229.56 Liability

(c) Jurisdiction. A person may bring an action to enforce a claim... in any United States district court or in any other court of competent jurisdiction. Such claim shall be brought within one year of the date on which the person's cause of action accrues... a cause of action accrues as of the date on which the injured person first learns...of the facts and circumstances giving rise to the cause of action, including the identity of the warranting or indemnifying bank against which the action is brought.

Under the § 229.56 Warranty…

Liability for the loss falls to the bank that allowed its customer to use its smart phone app.

Bank can charge the loss against its customer (assuming $$ is still there)

Mobile Banking and Deposit Fraud:

Holder in Due Course

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

The company doesn't think to place a Stop Payment on the first check because they have the 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.

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.

Cyber crime is a mature, underground international business with well-organized syndicates attacking companies, municipalities, non-profits, and even power grids.

These syndicates also sell customized malware and instant hacking tools to novice cyber criminals, allowing them to quickly join the criminal community.

Malware and Hacking are the primary methods used to get inside an organization’s computer system.

There are two primary types of malware:

auto-executable code

(a "drive-by" download)

that can happen merely by visiting an infected website….

…and code that requires

interaction by users:

opening an email attachment or

clicking on an imbedded link

Keystroke Logger Viruses

Tracks every keystroke; sends hourly reports

Spreads by:

- Email, Web sites
- Infected files on network
- USB drive or CD

Trojan Horse

A malicious program concealed in something innocuous.

Contains keystroke logger virus

- Pictures, Video on Facebook and MySpace
- Free music downloads
- Email attachments

Corporate Identity Theft

Corporate Identity Theft

- ✓ Hackers target Accounts Receivable List

Corporate Identity Theft

- ✓ Hackers target Accounts Receivable List
- ✓ Send bogus change-of-bank notifications to customers

Corporate Identity Theft

- ✓ Hackers target Accounts Receivable List
- ✓ Send bogus change-of-bank notifications to customers
- ✓ New PO Box

Corporate Identity Theft

- ✓ Hackers target Accounts Receivable List
- ✓ Send bogus change-of-bank notifications to customers
- ✓ New PO Box
- ✓ New Bank R/T and account

Corporate Hacking

Corporate Hacking

- ✓ Banks: Monitor bank changes on outgoing repetitive wires

Corporate Hacking

- ✓ Banks: Monitor bank changes on outgoing repetitive wires
- ✓ Companies: Confirm ALL bank change notifications from vendors

Corporate Hacking

- ✓ Banks: Monitor bank changes on outgoing repetitive wires
- ✓ Companies: Confirm ALL bank change notifications from vendors
- ✓ Buy cyber crime and check fraud insurance

Corporate Hacking

- ✓ Banks: Monitor bank changes on outgoing repetitive wires
- ✓ Companies: Confirm ALL bank change notifications from vendors
- ✓ Buy cyber crime and check fraud insurance
- ✓ Use payee positive pay and high security checks

Phishing Emails

Can look legitimate

"**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 **link**. As soon as it is set up, your transaction abilities will be fully restored. Best regards, Online security department, Federal Deposit Insurance Corporation."

Lead to account takeovers

Cyber Crime "Phishing" Attack:

V.

$560,000 Loss

CFO responded to phishing email with his bank login

Lawsuit

eXperi-METAL INC.

Computer was taken over.
93 Wires, $1,900,000 left the bank

$560,000 Unrecovered

Company sued the bank.

Who won the lawsuit?

http://www.lerchearly.com/publications/499-commercial-lending-bulletin-september-october

http://www.alstonprivacy.com/blog.aspx?entry=4353

WHY did the bank lose?

1. **Programming error (immediately remedied) allowed funds exceeding Customer's actual account balance to be wired out of a ZBA acct, creating a $2 million overdraft in the concentration acct.**

2. **Five other companies were hit same day, same way**

3. **Company was liable for CFO clicking on fake email**

4. **Company "won" lawsuit against Comerica, but**

5. **Company was not awarded attorney fees (> $250K)**

eXperi-METAL INC.

Important Links

Summaries:

(This article is really good.)
http://www.lerchearly.com/publications/499-commercial-lending-bulletin-september-october

http://www.bankinfosecurity.com/court-favors-emi-in-fraud-suit-a-3750
http://www.pcworld.com/article/230392/article.html
http://www.alstonprivacy.com/blog.aspx?entry=4353

Bench Opinion: http://zra.com/attachments/article/43/ExperiMetal.pdf

Choice Escrow and Land Title

vs.

BancorpSouth Bank

Important Link

http://courtweb.pamd.uscourts.gov/courtwebsearch/mowd/qmC2dt555T.pdf

Choice Escrow and Land Title
vs.
BancorpSouth Bank

- ✓ March 17, 2010: Bank received an internet-based request to wire **$440,000** out of Choice Escrow's Trust Account
- ✓ Request not legitimate – Choice Escrow employee's computer was hacked, taken over by fraudsters
- ✓ NO "Dual Authentication" in place at Company
- ✓ Wire transfer request to send $440K to **Republic of Cypress**

http://courtweb.pamd.uscourts.gov/courtwebsearch/mowd/qmC2dt555T.pdf

Computer Takeover: NO "Dual Control"

- ✓ Wire to Cypress was initiated using the User ID and password of a Choice Escrow employee
- ✓ Wire was initiated from IP address registered to Choice
- ✓ Bank authenticated employee's computer by detecting the secure device ID token that Bank previously installed
- ✓ Immediately after wiring funds, Bank auto-generated a Transaction Receipt that was faxed to and received by Choice Escrow. Fax placed on a desk, without review.

Bank: Customer Failed to Implement "Dual Control"

- ✓ Bank required online banking customers sending wires to utilize "Dual Control"
- ✓ Dual Control = **2 computers, 2 logins, 2 passwords**
- ✓ Wire transfer could only be effectuated by two individuals using separate User IDs and passwords
- ✓ Choice declined in writing, **TWICE**, to use Dual Control

Feeble Argument about Dual Control

- ✓ Choice contended "Dual Control" was not "commercially reasonable" because…
- ✓ "…at times, one or both of the two individuals authorized to perform wire transfers through the [bank] system were out of the office due to various reasons."
- ✓ Court disagreed.
- ✓ Choice Escrow held liable for loss.

Official Comments to the Funds Transfers provisions of the UCC:

The purpose of having a security procedure deemed to be commercially reasonable is to encourage banks to institute **reasonable safeguards** against fraud **but not to make them insurers against fraud**.

A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. **The standard is not whether the security procedure is the best available**.

Official Comments to the Funds Transfers provisions of the UCC:

Sometimes an informed customer refuses a security procedure that is commercially reasonable and suitable for that customer and insists on using a higher-risk procedure because it is more convenient or cheaper. In that case, under the last sentence of subsection (c), the customer has voluntarily assumed the risk of failure of the procedure and cannot shift the loss to the bank.

Court Order, March 18, 2013

"For the foregoing reasons, the Court **GRANTS** the MOTION OF DEFENDANT BANCORPSOUTH FOR SUMMARY JUDGMENT. All other pending motions, including all other motions for summary judgment (including motions for partial summary judgment), are **DENIED** as moot. Accordingly, it is **ORDERED** that summary judgment is entered in favor or defendant BancorpSouth Bank."

Prevent Online Banking Fraud

Require 2 different computers to move $$

1. Computers #1-99 can "originate" wires

2. Dedicated "banking-only" computer to "release" the wire / ACH

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)

"Physical" Attacks –

"Skimmers" in credit/debit card devices

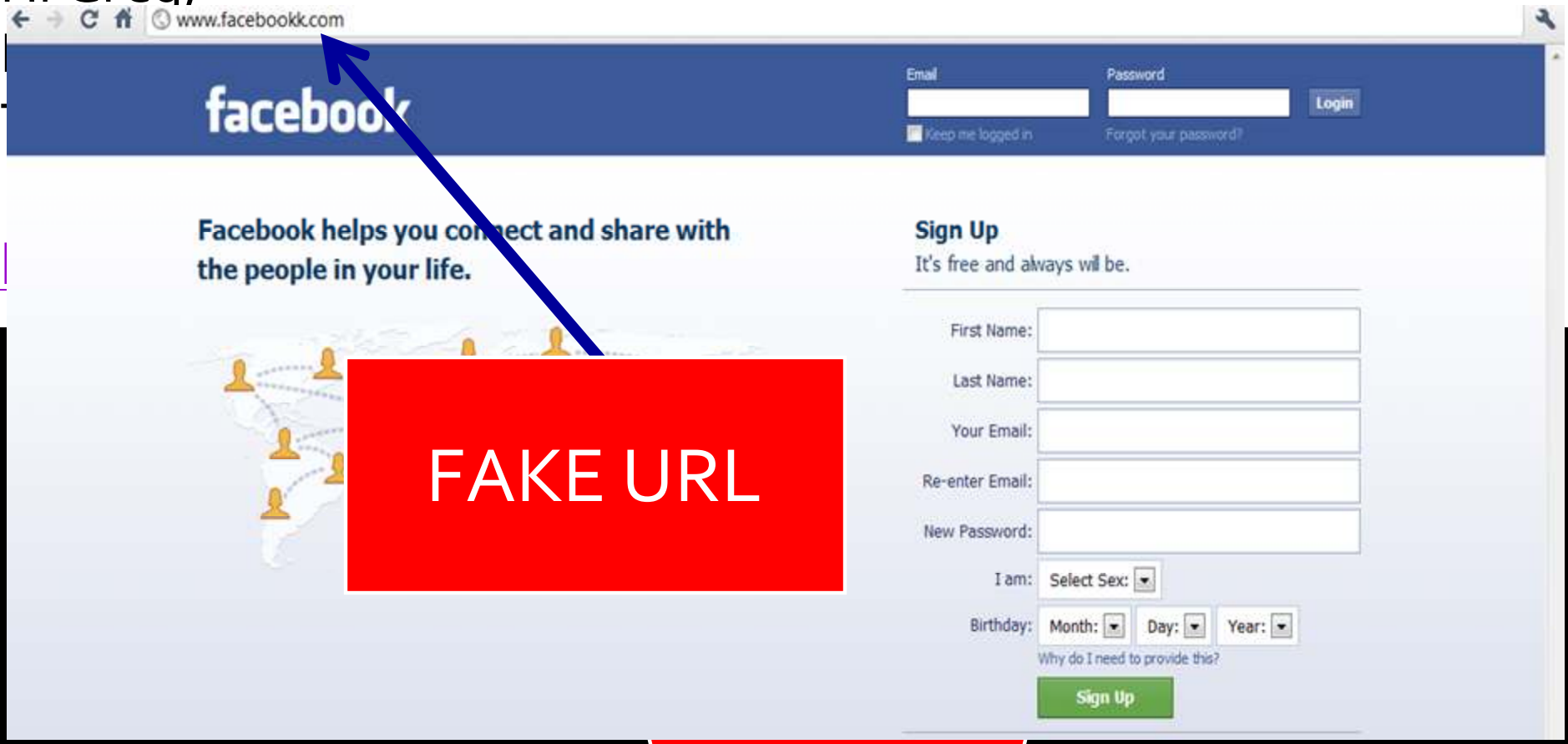
Infected flash/thumb drives

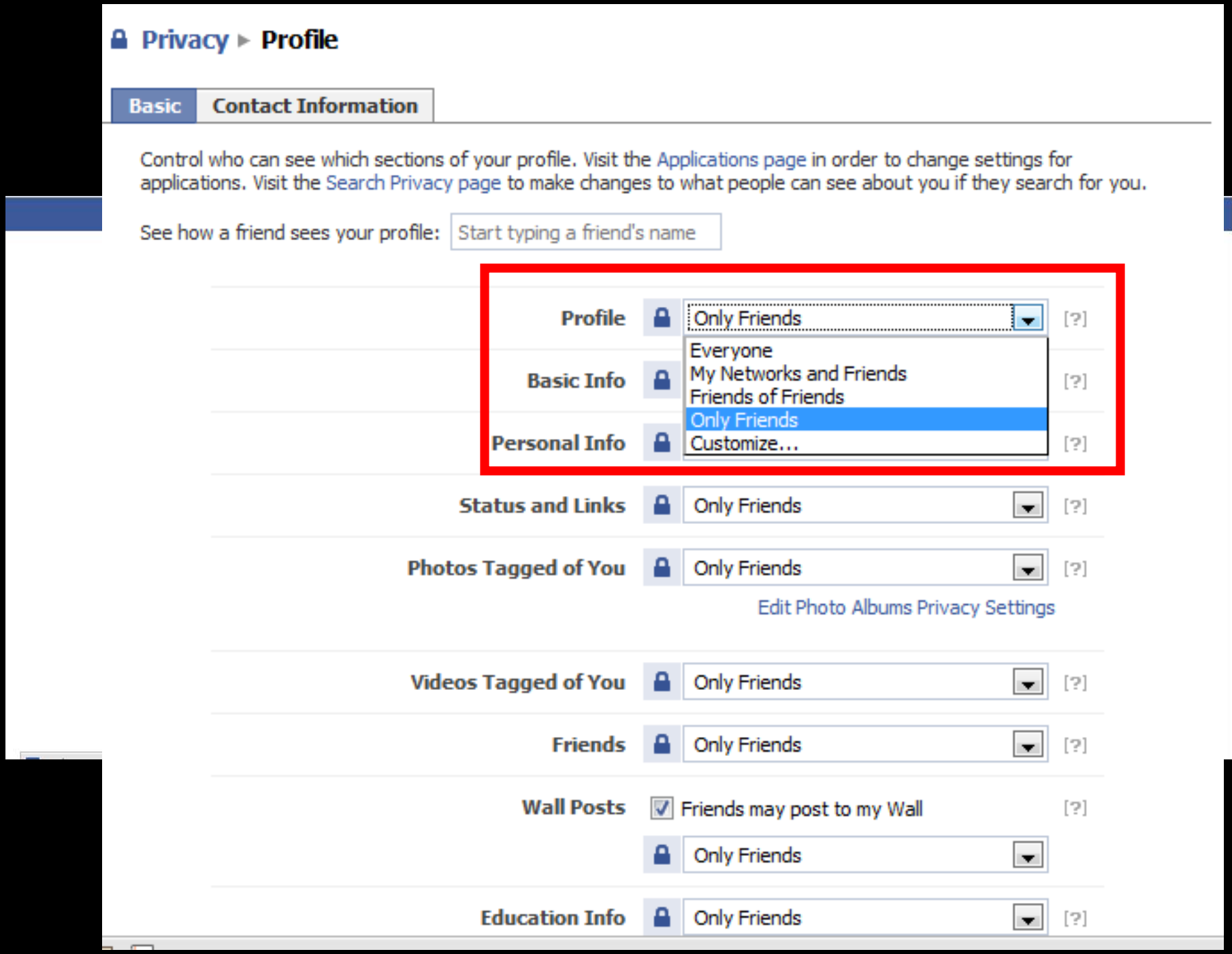
Fraudsters Targeting Banks

Facebook

1 Billion Users

Hi Greg,


www.facebookk.com
facebook
Email
Password
Login
Keep me logged in
Forgot your password?
Facebook helps you connect and share with the people in your life.
Sign Up
It's free and always will be.
First Name:
Last Name:
Your Email:
Re-enter Email:
New Password:
I am:
Select Sex:
Birthday:
Month:
Day:
Year:
Why do I need to provide this?
Sign Up
FAKE URL
Here


Privacy ▸ Profile
Basic
Contact Information
Control who can see which sections of your profile. Visit the Applications page in order to change settings for applications. Visit the Search Privacy page to make changes to what people can see about you if they search for you.
See how a friend sees your profile:
Start typing a friend's name
Profile
Only Friends
[?]
Everyone
My Networks and Friends
Friends of Friends
Only Friends
Customize...
Basic Info
Personal Info
Status and Links
Only Friends
Photos Tagged of You
Only Friends
Edit Photo Albums Privacy Settings
Videos Tagged of You
Only Friends
Friends
Only Friends
Wall Posts
Friends may post to my Wall
Only Friends
Education Info
Only Friends

Ramnit Worm Threatens Online Account

Facebook Targeted by Fraudsters Seeking Log-in Credentials

THE JOURNAL REPORT

What's a Company's Biggest Security Risk? YOU.

THE WALL STREET JOURNAL.
WSJ.com

SEPTEMBER 26, 2011

What's a Company's Biggest Security Risk? You.

Employees don't mean to be the primary entry point for hackers. But they are.

By GEOFFREY A. FOWLER

We are the weakest link.

Hacking attacks against companies are growing bigger and bolder—witness a string of high-profile breaches this year at Sony Corp., Citigroup Inc. and others. But gone are the days when hackers would simply find holes in corporate networks to steal valuable data. Large companies have grown wise to the threat of hacking, and have spent the past 30 years hardening the perimeters of their networks with upgraded technology.

These days, criminals aren't just hacking networks. They're hacking us, the employees.

"The security gap is end users," says Kevin Mandia, chief executive of security firm Mandiant Corp. The majority of corporate security breaches his firm is currently investigating involve hackers who gained access to company networks by exploiting well-intentioned employees.

Consider what happened in March at EMC Corp.'s RSA security unit, the maker of computer login devices used by thousands of other companies. A hacker sent emails to two small groups of employees that looked innocent enough, including a spreadsheet titled "2011 Recruitment plan." The message was so convincing that one employee retrieved it from the "junk mail" folder and then opened the attachment. Doing so introduced a virus inside RSA's network that eventually gave the hacker access to sensitive company data and enabled later attacks against RSA's customers.

Employees have more opportunities than ever to compromise company information. We not only screw up by clicking on emails from hackers that download viruses, letting them bypass corporate firewalls. We also open a Pandora's Box of security problems by circumventing company tech-support

THE WALL STREET JOURNAL.
WSJ.com
SEPTEMBER 26, 2011

What to Do if You've Been Hacked

Among the surprising advice: Don't shut down the computers

By BEN WORTHEN

It's a nightmare scenario every business fears.

Your tech department has spotted suspicious activity on the company network. Your customers and employees are getting hit with credit-card fraud and identity theft. MasterCard Inc. is on line 1.

The panic sets in: Your company has been hacked!

So, what do you do?

First, take a breath and remember that you're not alone. Last year, 662 organizations publicly disclosed data breaches, according to the nonprofit Identity Theft Resource Center, a figure that includes real-world theft and accidents as well as cyberintrusions. And the actual number is likely much higher than that, since not all hacking incidents get disclosed.

Next, remember that getting hacked doesn't have to be a business-crippling experience. While it will likely set a company back financially, if handled properly it won't have a long-lasting impact.

"The public is forgiving when it's apparent that the company is doing the right thing," says Lori Nugent, a lawyer at Wilson Elser Moskowitz Edelman & Dicker LLP who specializes in breach cases. In fact, if a company is on top of the technological problems and communicates well, it can build loyalty among its customers, she says.

There are a number of small but critical steps businesses need to take when they find out they've been

THE WALL STREET JOURNAL.
WSJ.com
SEPTEMBER 26, 2011

You May Be Fighting the Wrong Security Battles

How IT executives can determine the right amount to spend—and where to spend it

By LAWRENCE A. GORDON AND MARTIN P. LOEB

A recent wave of information-security breaches at high-profile companies has many executives on heightened alert. They're trying to figure out everything they can do to prevent breaches, limit the damage if one occurs, and be prepared to rebound quickly from whatever harm is done.

As they consider their options, two questions loom large: How much should they spend to protect their companies' information? And how can they get the most for their money?

Our research suggests they should spend substantially less than the expected loss from a breach, and perhaps spend it differently than many might think.

The One-Third Mark

We developed a model to help executives determine the optimal level of investment to protect a given set of information—whether it's customers' personal information, company financial data, strategic-planning documents or something else. The model weighs the potential loss from a security breach, the probability that a loss will occur, and the effectiveness of additional investments in security.

One key finding from the model: The amount a firm should spend to protect information is generally no more than one-third or so of the projected loss from a breach. Above that level, in most cases, each dollar spent will reduce the anticipated loss by less than a dollar.

A second key finding: It doesn't always pay to spend the biggest share of the security budget to protect the information that is most vulnerable to attack, as many companies do. For some highly vulnerable

10 Tips to Fight Insider Fraud

http://www.bankinfosecurity.com/10-tips-to-fight-insider-fraud-a-4550

BANK INFO SECURITY

10 Tips to Fight Insider Fraud

Organizations Often Fail to Fend Off the Obvious Risks

Tracy Kitten, March 2, 2012

Regardless of industry, insiders always pose the greatest threat to an organization's security. Insiders are risky, especially ones with axes to grind.

Researchers within CERT's Software Engineering Institute at Carnegie Mellon have reviewed internal threats for the last decade, examining the threats posed by so-called malicious insiders. Now CERT offers some new insights, about the threats posed by unintentional breaches - those that happen by accident.

This week, during RSA Conference 2012 in San Francisco, Dawn Capelli of the Software Engineering Institute at CERT, said most organizations continually fail to adequately address internal threats, though most agree insider fraud is a growing area of concern. from RSA.]


Dawn Capelli

"About 50 percent of all companies experience at least one malicious insider attack," said Capelli, who co-authored *The Search Guide to Insider Threats* with two other CERT researchers. "And an internal attack has more of an impact than an external attack."

When companies break down breaches, about one-third are directly linked to insiders, and more probably have some link to an insider that the organization simply has not identified. "A lot of the attacks we've seen this year, with cyber attacks, were unintentional," Capelli says.

http://www.bankinfosecurity.com/10-tips-to-fight-insider-fraud-a-4550

Top 10 Tips

Here are Capelli's top 10 tips for fighting the insider threat:

1. **Repeat Offenders and Offenses.** Learn from past incidents. Most organizations get hit

Protect Passwords

1	123456
2	12345
3	123456789
4	Password
5	qwerty

FBI:
10 Most Popular Passwords

6	trustno1
7	abc123
8	monkey
9	letmein
10	**dragon**

FBI:
10 Most
Popular
Passwords

Cracking Passwords

2009

- Online games service **RockYou.com** hacked
- **32 Million** plain-text passwords stolen
- **14 Million** unique passcodes were posted

✓ **Overnight, the way hackers cracked passwords changed!**

RockYou.com list confirmed nearly all **CAPITAL LETTERS** come at the beginning of a password. Nearly all **PUNCTUATION** and **NUMBERS** are at the end.

RockYou list revealed a strong tendency to use first names followed by years:

Christopher1965 or **Julia1984**

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

Five years ago: 8 Characters, all lower case = 4 days

Today: 8 Characters, all lower case = 12 hours

Today

It Takes a Hacker 12 Hours to Randomly Guess Your 8-Character Password

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

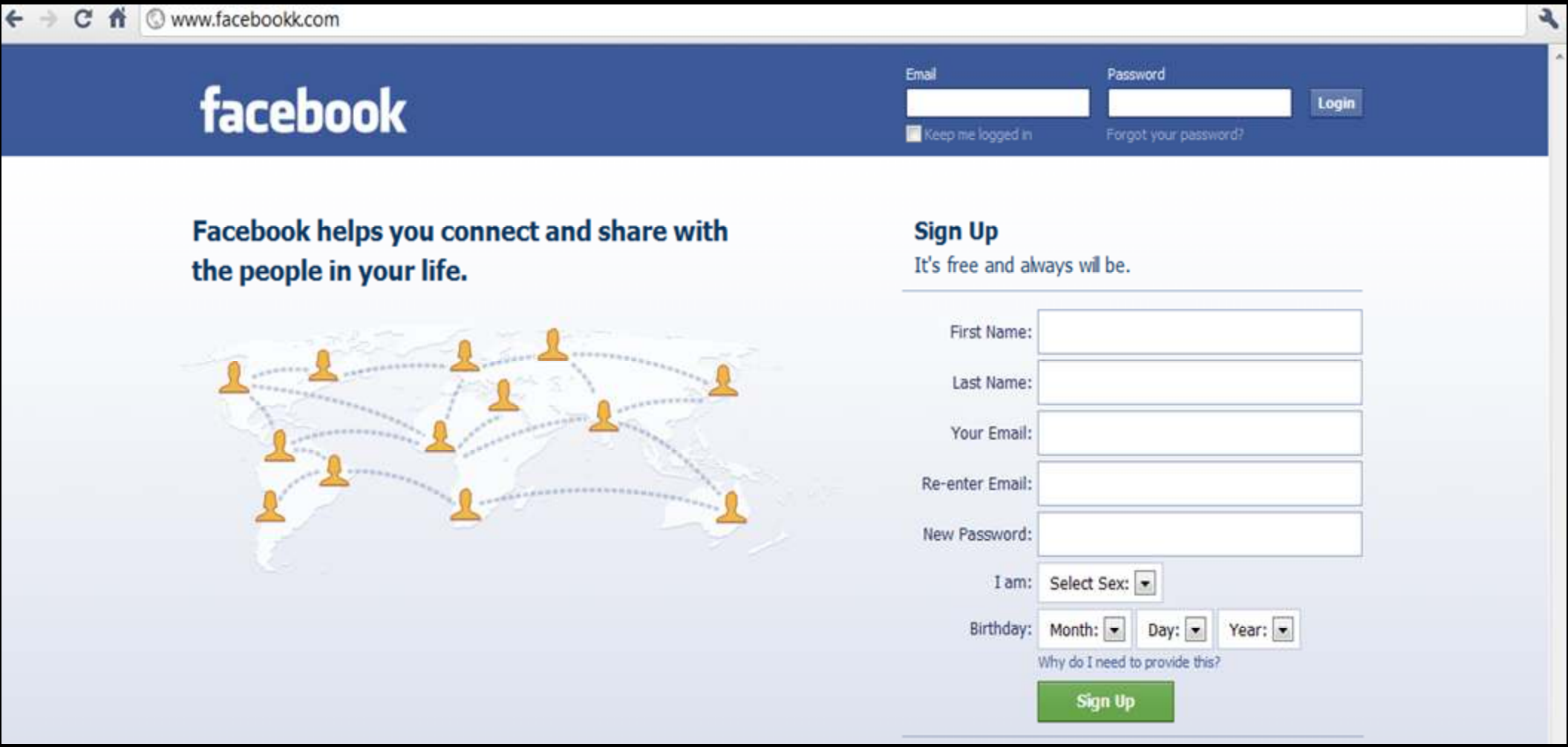
Track Your Kids

Track Your Kids Keystrokes

(without them knowing, ever.)

Kids keep 2 Facebook Accounts

(Mom only sees one)



Track Your Kids' Keystrokes

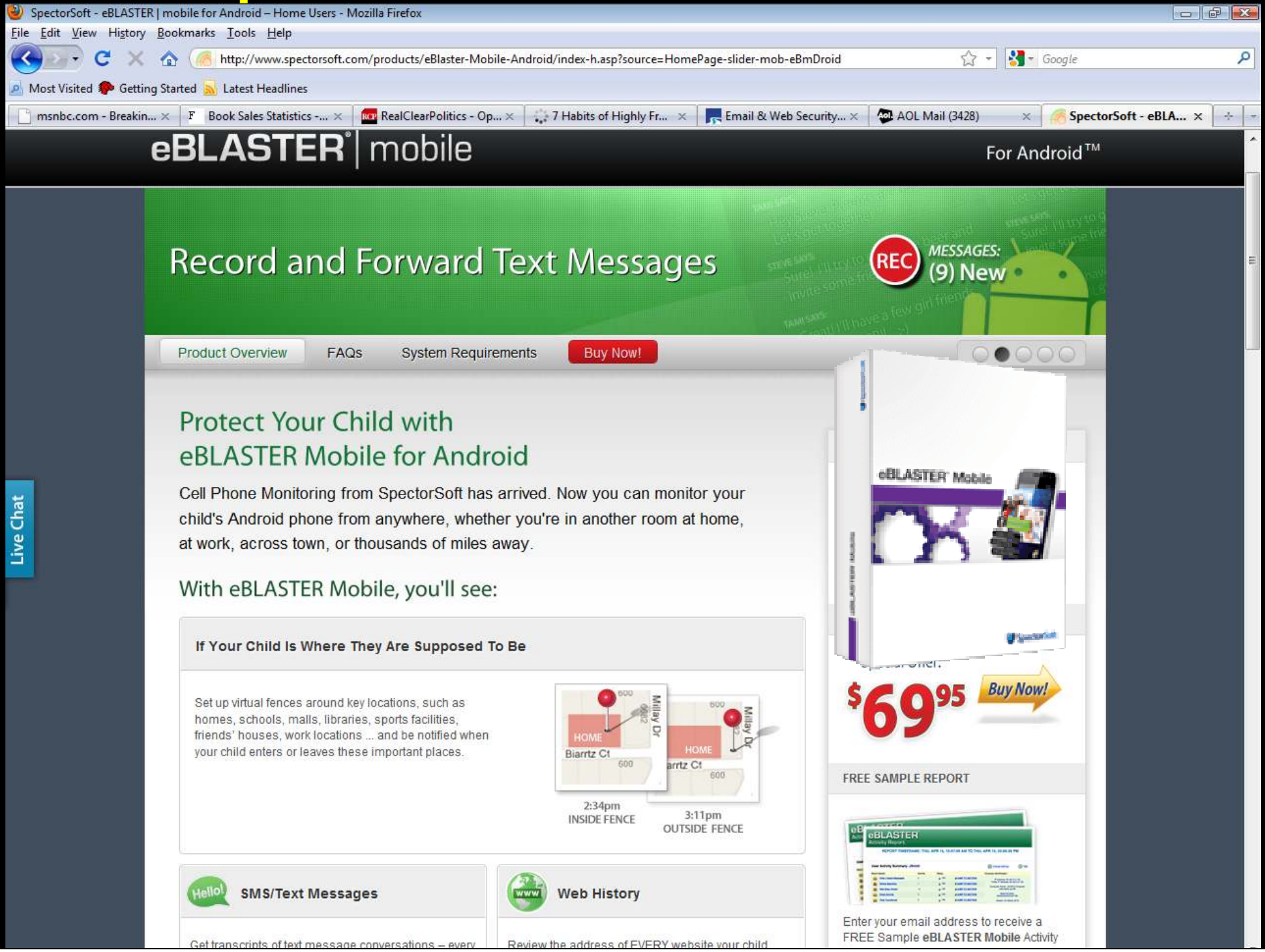
SpectorSoft

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



www.phonesheriff.com

phonesheriff reviews

phonesheriff

MONITOR & FILTER SMARTPHONES & TABLETS

Parental Control Software for Mobile Phones and Tablets

1-888-475-5345

Worried about your child or employee's **phone or tablet usage?**

- **Block phone numbers** from calls and text messages
- Set custom **time restrictions** and **block apps** you choose
- Monitor **text messages** and get custom activity alerts
- Real time **location tracking** and **lock commands**

See Features **Purchase now**

Block Activity

more info

Block any phone number from texting, calls, or both.

Set Time Limits

more info

Lock the device during certain times of day or just restrict calls.

Track GPS

more info

Get instant locations or remotely lock/unlock the device.

Monitor Online

more info

Login to a secure online control panel to view the logs.

www.NoSlang.com

Internet Text and Drug Slang Translator & Dictionary

Internet Slang Dictionary & Translator
Confused by net slang? Can't read a text message?
Translate internet slang and acronyms.

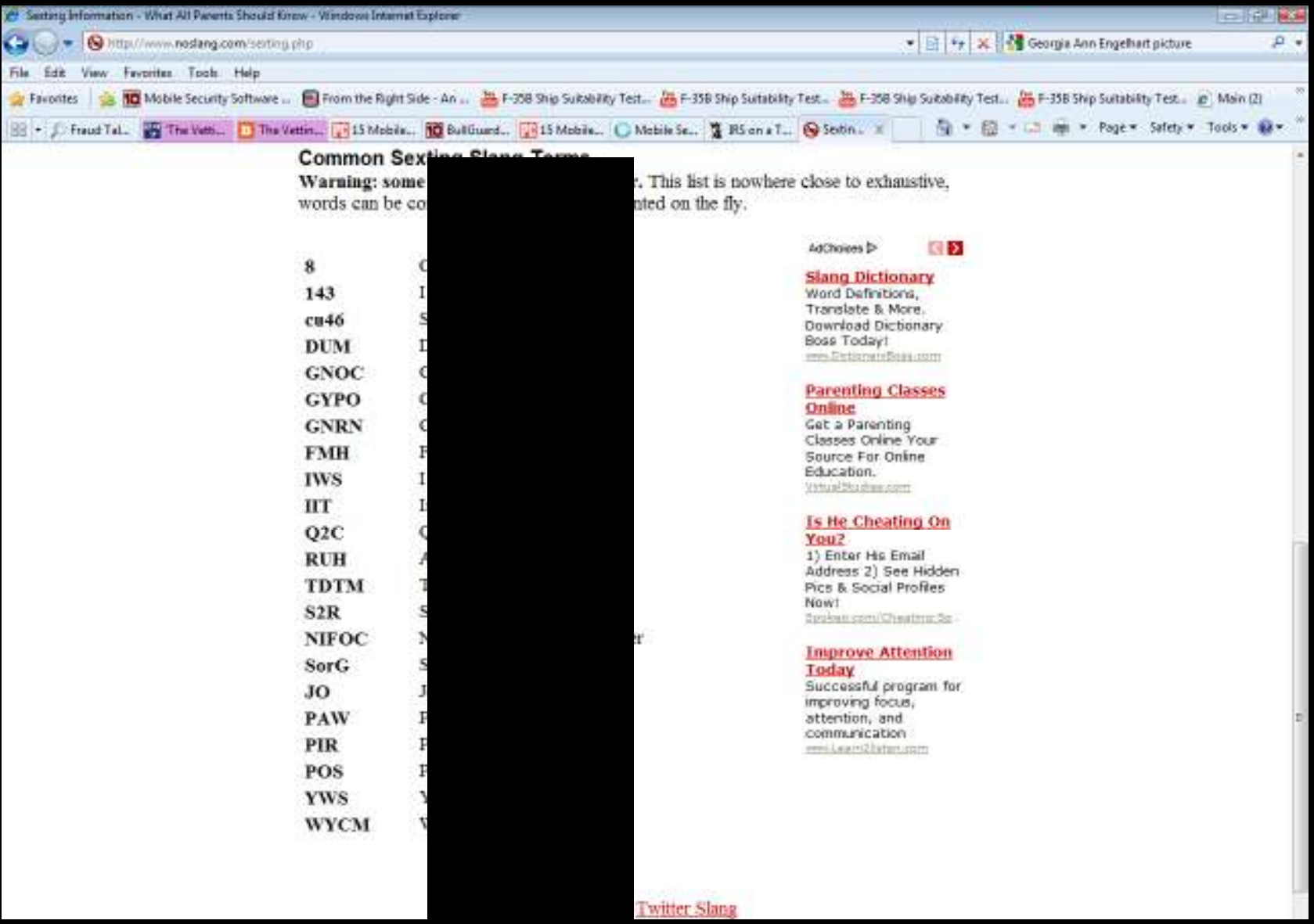
25 Internet Slang Terms All Parents Should Know:

Do you know what these terms mean? Your kids do!
Chances are they're using them online to talk to their friends. Some of them may shock you.
(sometimes used letters are in parentheses)

Also, make sure you read the What Every Parent Must Know article.

ASL(RP)	Age Sex Location (Race / Picture)
BF / GF	Boyfriend / Girlfriend
BRB	Be Right Back
CD9	Code 9 - means parents are around
GNOC	Get Naked on Cam (webcam)
GTG	Got to Go
IDK	I don't know
(L)MIRL	(Lets) meet in real life
LOL	Laugh Out Loud
MorF	Male or Female
MOS	Mom Over Shoulder
NIFOC	Naked in Front of Computer
Noob	Newbie - often an insult to somebody who doesn't know much about something.
NMU	Not much, you?
P911	Parent Emergency
PAW	Parents are Watching
PIR	Parent In Room
POS	Parent Over Shoulder
PRON	Porn
PRW	Parents Are Watching
S2R	Send To Recieve (pictures)
TDTM	Talk Dirty To Me

Sexting Slang Terms



Sexting can create serious long-term legal conse-quences for your child.

www.NoSlang.com

snapchat

What is Snapchat?
Snapchat is the fastest way to share a moment on iPhone and Android. You control how long you want your friends to view your messages. We'll let you know if we detect that they've taken a screenshot!

Is there any way to view an image after the time has expired?
No, snaps disappear after the timer runs out. You can save snaps that you capture by pressing the save button on the preview screen.

What if I take a screenshot?
Screenshots can be captured if you're quick. The sender will be notified if we detect you have taken a screenshot.

snapchat

What is Snapchat?

Snapchat is the fastest way to share a moment on iPhone and Android. You control how long you want your friends to view your messages. We'll let you know if we detect that they've taken a screenshot!

Is there any way to view an in

No, snaps disappear [illegible] that you [illegible] preview

W[illegible]shot?

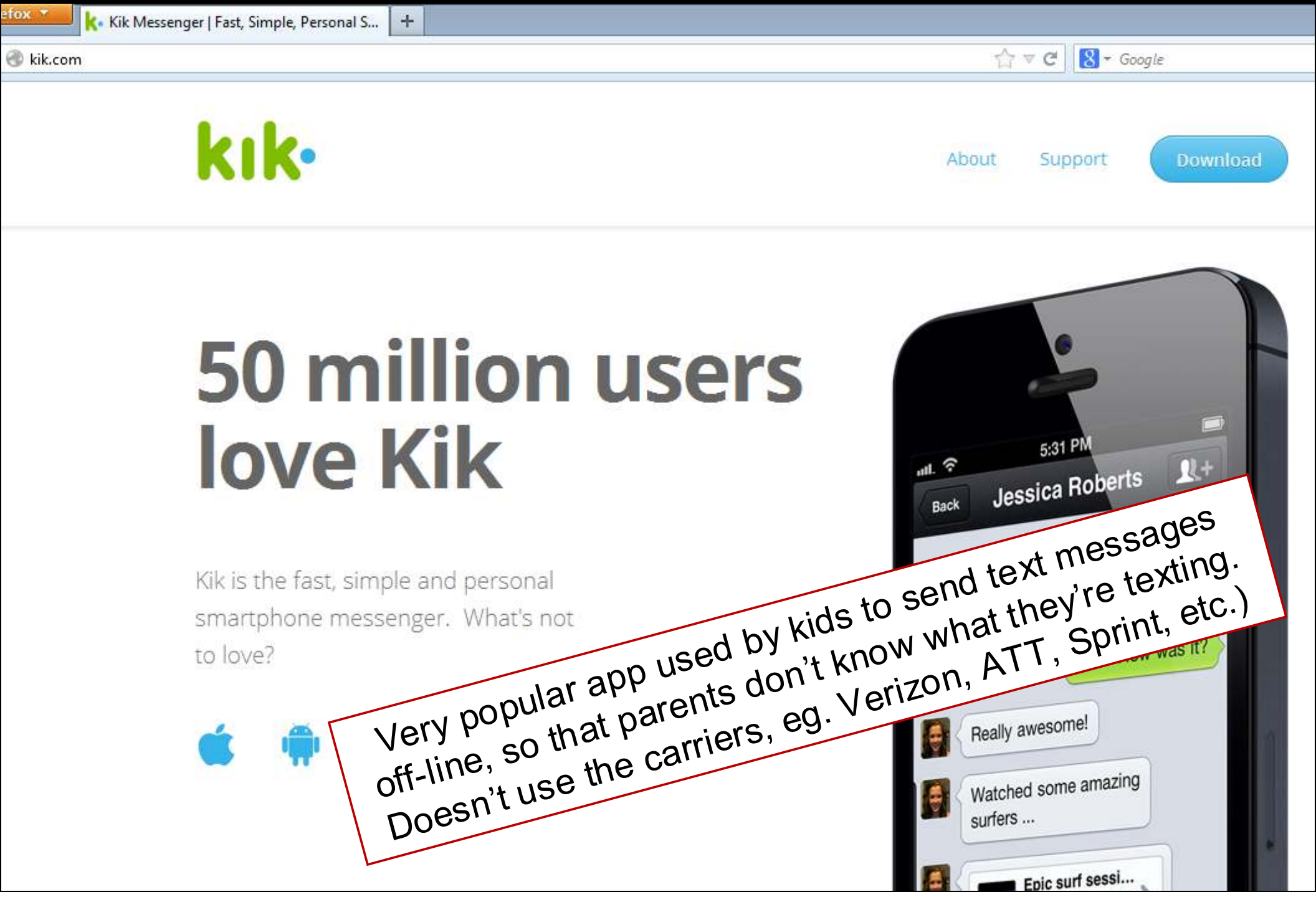
Sc[illegible]s can be captured if you're quick. The sender will be notified if we detect you have taken a screenshot.

A very popular app among teenagers that can be used to send pixs, including pornography. The pix ("snap") disappears in 10 seconds… Unless it doesn't… because it was saved quickly by the recipient and turned over to a very angry parent… and law enforcement.

Texting app


Kik Messenger | Fast, Simple, Personal S...
kik.com
Google
kik
About
Support
Download
50 million users love Kik
Kik is the fast, simple and personal smartphone messenger. What's not to love?
ovi
5:31 PM
Back
Jessica Roberts
3 minutes ago
Hey! I'm back from Hawaii!
Cool! How was it?
Really awesome!
Watched some amazing surfers ...
Epic surf sessi...

Texting app


Kik Messenger | Fast, Simple, Personal S...
kik.com
Google
kik
About
Support
Download
50 million users love Kik
Kik is the fast, simple and personal smartphone messenger. What's not to love?
5:31 PM
Back
Jessica Roberts
Really awesome!
Watched some amazing surfers ...
Epic surf sessi...
Very popular app used by kids to send text messages off-line, so that parents don't know what they're texting. Doesn't use the carriers, eg. Verizon, ATT, Sprint, etc.)

Check Fraud

Check Fraud

Why talk about Check Fraud?

Check Fraud

Produces more $ Losses

than all other types of payment fraud

COMBINED!

In 1762…

Price sued Neal for check fraud

Price v. Neal, England

(The FIRST Check Fraud Lawsuit)

Plaintiff, Price, argued that:

Defendant, Neal, was indebted to him for 80£ for money had and received: and damages were laid to 100£. Plaintiff should recover back the money he paid them by mistake believing "that these were true genuine bills."

Plaintiff, Price, argued that:

Defendant, Neal, was indebted to him for 80£ for money had and received: and damages were laid to 100£. Plaintiff should recover back the money he paid them by mistake believing "that these were true genuine bills."

Plaintiff "could never recover it against the drawer, because no drawer existed;

Plaintiff, Price, argued that:

Defendant, Neal, was indebted to him for 80£ for money had and received: and damages were laid to 100£. Plaintiff should recover back the money he paid them by mistake believing "that these were true genuine bills."

Plaintiff "could never recover it against the drawer, because no drawer existed; nor against the forger, because he is hanged."

Plaintiff, Price, argued that:

Defendant, Neal, was indebted to him for 80£ for money had and received: and damages were laid to 100£. Plaintiff should recover back the money he paid them by mistake believing "that these were true genuine bills."

Plaintiff "could never recover it against the drawer, because no drawer existed; nor against the forger, because he is hanged."

The jury found a verdict for the Plaintiff; and assessed damages of 80£ and costs 40s.

Check fraud has continued unabated for 250 years!

Check fraud has continued unabated for 250 years!

but with fewer public hangings.

AFP 2014 Payments Fraud Survey

In 2013

70% of organizations

still issued checks.

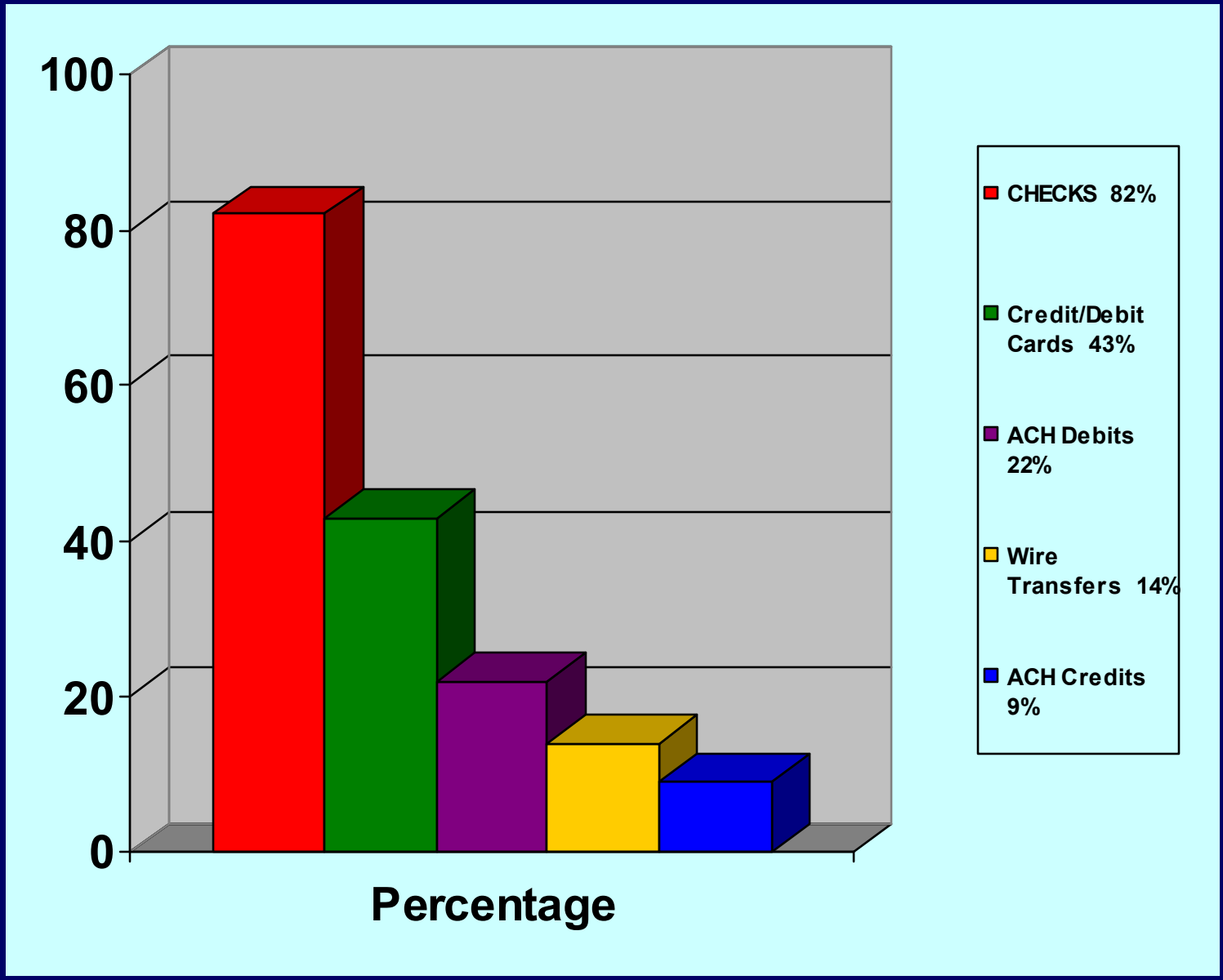
Check fraud will never go away!

AFP 2014 Payments Fraud Survey

"…checks continue to be the dominant payment form targeted by fraudsters," with 82% of affected organizations reporting that their checks were targeted."

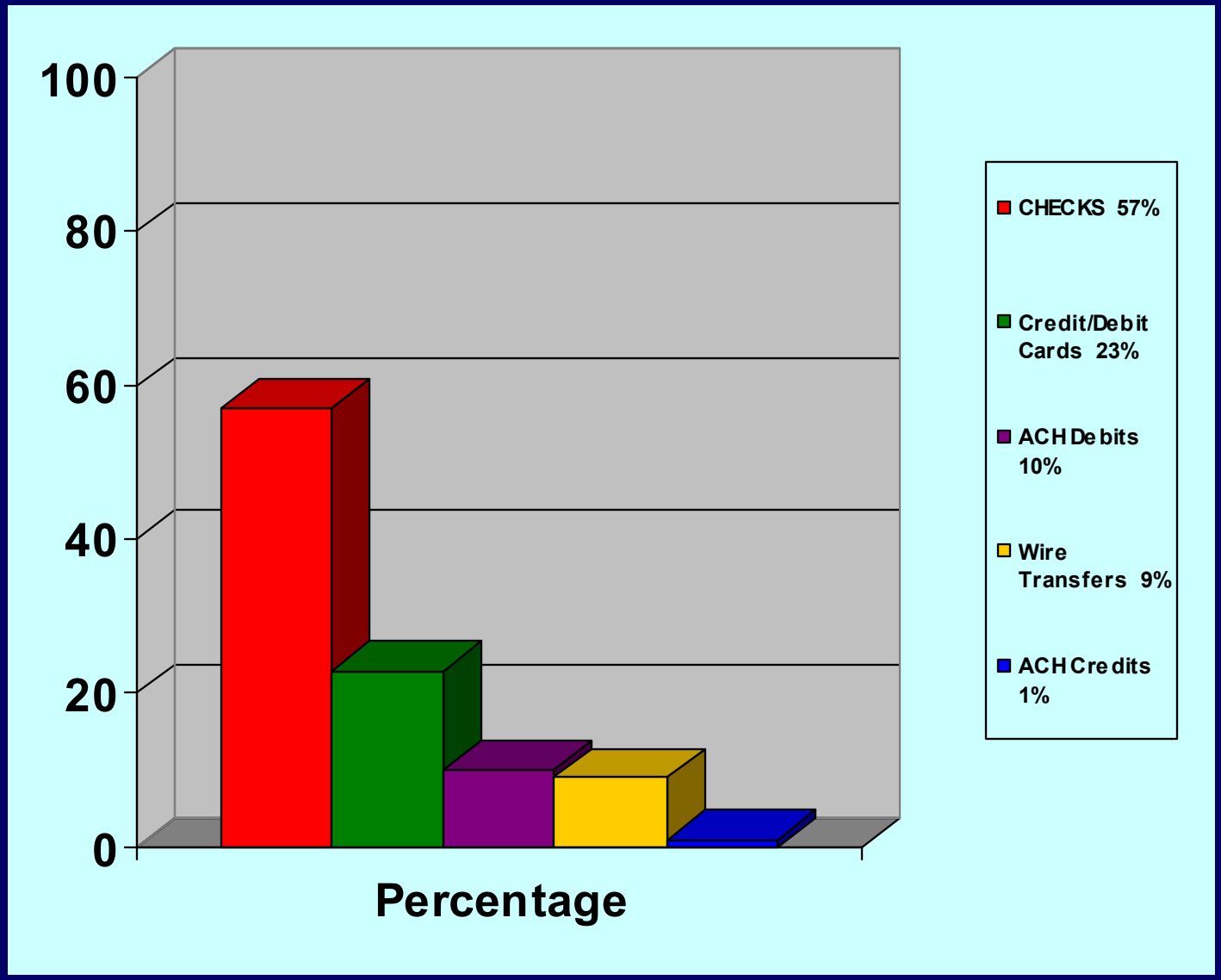
Fraudulent Payments by Method

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



Fraud Losses by Method

How Dollars were actually lost



Frank Abagnale

Catch Me If You Can

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

Boston's #1 Seller

The Evolution

of

Check Fraud

and

Banker Solutions

Counterfeit Checks

(since 1762)

…Banks developed Positive Pay

Altered Payees

…Banks developed Payee Positive Pay

Added Payee Names

Checks blow right through Payee Positive Pay!

Typical Check Layout

<u>Added Payee</u> printed 2 lines above original name

will not be detected by Payee Positive Pay

Multiple Payees:

If it doesn't say **AND**,

it is "ambiguous" and legally means

"**OR**"

A forward slash [virgule, vər-gyül "/"] = **OR**

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. 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 mailing expense and bank fees
4. Pay 1 invoice at a time, or
5. Pay multiple invoices and email remittance detail

But, if you're going to write checks...

#1. High Security Checks

Effective check fraud prevention strategies begin with a high security check.

AFP 2014 Payments Fraud Survey

Types of Check Fraud Alterations:

1. **Payee Name Alterations = 52%**
2. **Dollar Amount Alterations = 37%**

AFP 2014 Payments Fraud Survey

Types of Check Fraud Alterations:

1. **Payee Name Alterations = 52%**
2. **Dollar Amount Alterations = 37%**

This is up from 49% and 22% respectively, in the 2013 Survey….

High Security Checks

1. Thwart forgers' attempts to replicate or alter the check

2. Deter the forger (psychological warfare)

3. Provide legal protection from some Holder in Due Course claims (UCC § 3-302)

What makes a check secure?

10+ safety features

Important Security Features

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

www.safechecks.com

Controlled Check Stock

- Is a critical security feature
- Checks should be unique in some way to every other organization's check stock
- No two organizations should have the exact, identical check stock

Uncontrolled Check Stock

- Is NOT uniquely designed or customized for each end-user
- It is often sold entirely blank to countless entities / organizations, and fraudsters, by print brokers all over the USA

Who Sells Blank, Uncontrolled Checks?

- Virtually ALL accounting / check writing Software Vendors

- Virtually ALL check printers
  1. Large, national printers
  2. Small print brokers that buy from wholesalers

Ask your check supplier this question:

Has your check stock ever been sold entirely blank to other companies?

Obtaining Controlled Check Stock

1. Custom-manufacture checks using an ORIGINAL design, true-watermarked paper, and at least 10 security features, OR
2. Buy from a supplier that sells controlled check stock that has never been replicated or used in a check fraud scam.

#2. Payee Positive Pay

Positive Pay…

…a powerful tool!

PositivePay.net

However…. Positive Pay

Provides <u>NO PROTECTION</u> Against

However…. Positive Pay

Provides <u>NO PROTECTION</u> Against

<u>Added</u> Payee Names!

CINCINNATI INSURANCE COMPANY v. WACHOVIA BANK, NATIONAL ASSOCIATION

CASE NO. 08-CV-2734 (PJS/JJG).

CINCINNATI INSURANCE COMPANY, as Subrogee of Todd's Snax, Inc., d/b/a Schultz Foods Company, Plaintiff,

v.

WACHOVIA BANK, NATIONAL ASSOCIATION, Defendant.

United States District Court, D. Minnesota.
July 14, 2010.

Lawsuit

Cincinnati Insurance Company

v.

Wachovia Bank

$154,000 Loss from an Altered Payee

Facts

Prior to the $154,000 loss, Schultz Foods had three (3) separate check fraud events.

Facts

Prior to the $154,000 loss, Schultz Foods had three (3) separate check fraud events.

Wachovia Bank covered their losses; told Schultz to use Positive Pay or close their account.

Facts

Prior to the $154,000 loss, Schultz Foods had three (3) separate check fraud events.

Wachovia Bank covered their losses; told Schultz to use Positive Pay or close their account.

Each time Schultz closed their account, but never implemented Positive Pay.

Facts

Schultz buys check fraud insurance from Cincinnati Insurance.

Facts

Schultz Foods issues $154,000 check payable to Amerada Hess Corporation.

Check is stolen. Payee Name altered.

Name changed to "Kenneth Payton"

Kenneth Payton, a minister, deposits $154,000 check into TCF Bank and wires $150,000 to Singapore to help a South African refugee family.

Facts

6 weeks later, Schultz Foods notifies Wachovia of altered payee; demands repayment.

Facts

6 weeks later, Schultz Foods notifies Wachovia of altered payee; demands repayment.

Wachovia won't pay until it recovers $ from TCF.

Facts

6 weeks later, Schultz Foods notifies Wachovia of altered payee; demands repayment.

Wachovia won't pay until it recovers $ from TCF.

Schultz files a claim with Cincinnati Insurance; Cincinnati pays the claim and sues Wachovia.

Facts

6 weeks later, Schultz Foods notifies Wachovia of altered payee; demands repayment.

Wachovia won't pay until it recovers $ from TCF.

Schultz files a claim with Cincinnati Insurance; Cincinnati pays the claim and sues Wachovia.

Under UCC § 3-119, TCF Bank (the liable party) hires attys to defend Wachovia, using Wachovia's signed "deposit agreement" against Cincinnati Insurance.

Wachovia's Deposit Agreement (Contract)

"You agree that if you fail to implement any of these products or services, or you fail to follow these and other precautions reasonable for your particular circumstances, you will be precluded from asserting any claims against [Wachovia] for paying any unauthorized, altered, counterfeit or other fraudulent item that such product, service, or precaution was designed to detect or deter, and we will not be required to re-credit your account or otherwise have any liability for paying such items."

Because of the signed deposit agreement,

Wachovia Bank Wins!

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

Fact

If Schultz Foods had used Positive Pay, the check may not have paid and there may not have been a loss!

Fact

If Schultz Foods had used Positive Pay, the check may not have paid and there may not have been a loss!

(Exception: Added Payee Names)

Preventing Altered Payees

- **High-security checks**
- **14 point font for Payee Name**
- **High-quality toner**
- **Hot laser printer**
- **Payee Positive Pay**

Frank Abagnale's Fraud Bulletin on Laser Check Printing

What about Added Payee Names?

It Is A Fact:

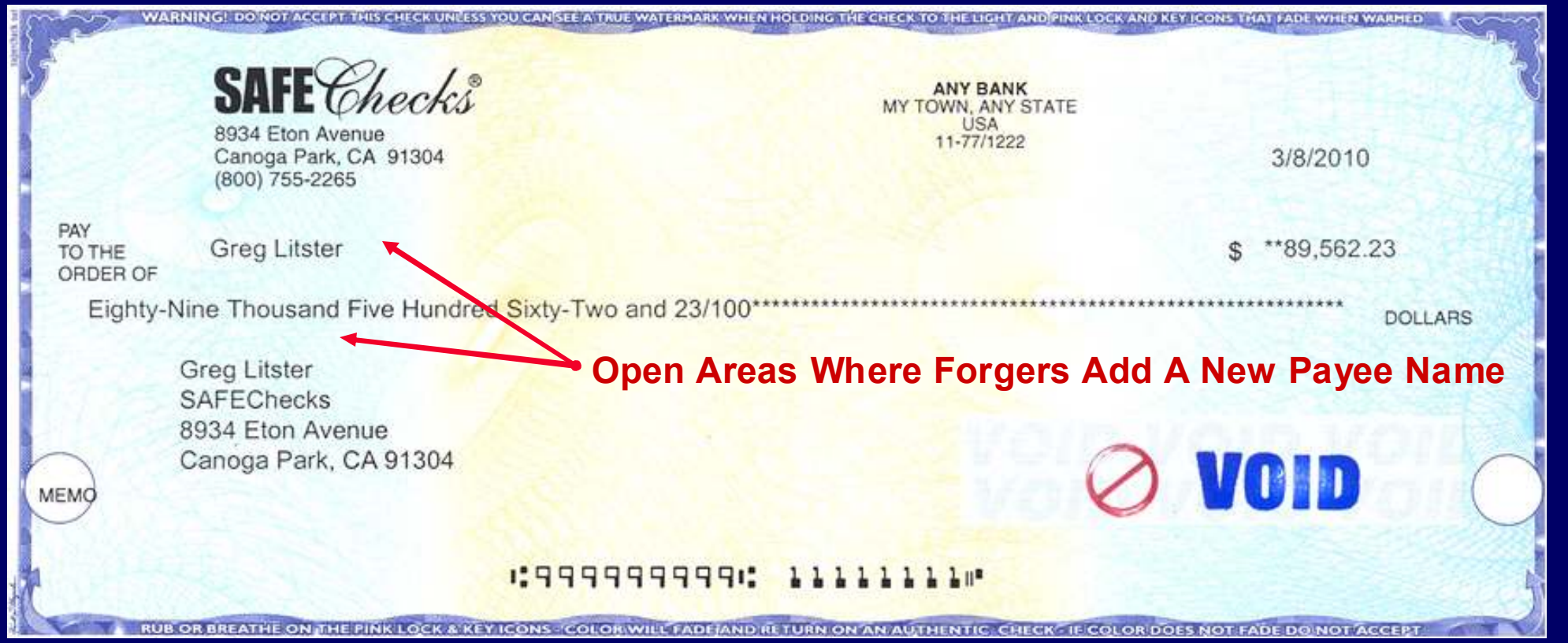
Payee Positive Pay systems are not detecting

Added Payee Names…

…printed 2 lines above the original payee name.

There is NO banker solution!

Typical Check Layout



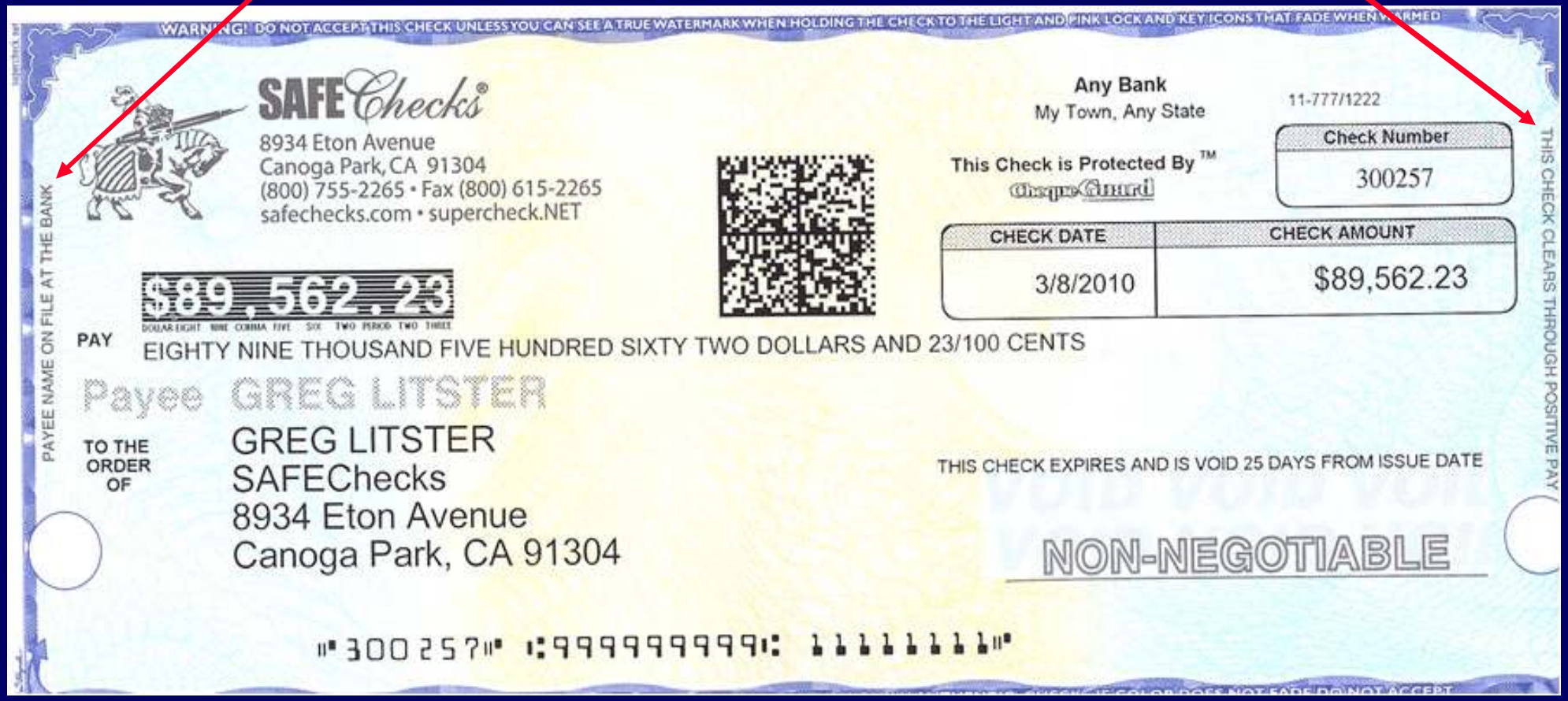
Fix it: Use a Secure Name Font

Secure Name Font printed above original payee name
helps eliminate Added Payee Name Risk

Leaves No Room for Adding Bogus Payee

Secure Name Font printed above original payee name
helps eliminate Added Payee Name Risk

Deterrence: Add Text to the Check



Deterrence: 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. Date and Time Check was printed
9. Laser Printer used
10. 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

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

Typical Check Layout –

Check is on top and shows thru window envelope

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

8934 Eton Avenue
Canoga Park, CA 91304

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

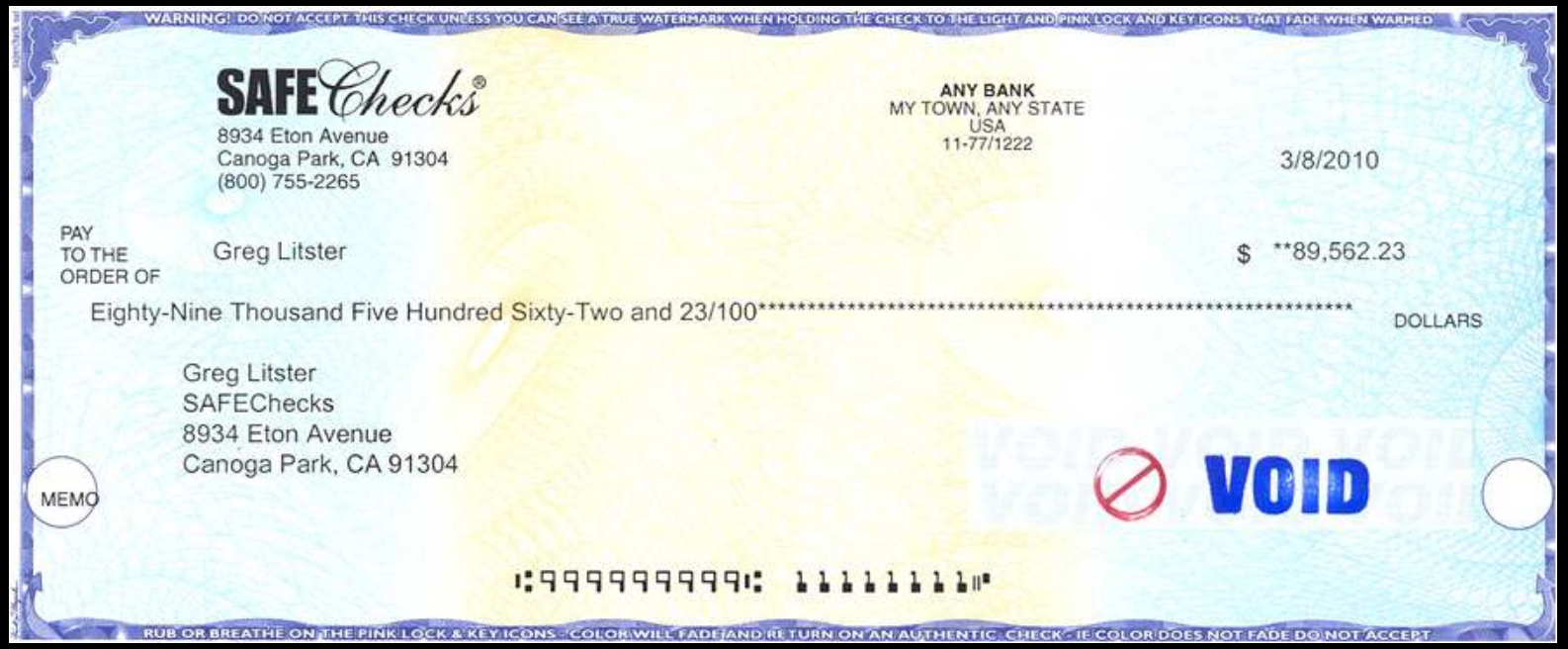
Payee Name, Address, is printed in TOP white panel.

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?



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

Federal Appellate Court

Lawsuits

HIDC & Stop Payments

Robert Triffin v. Cigna Insurance

- Two year old check; payment stopped
- No "expiration date" printed on check
  - **UCC: Check valid for 10 years or 3 years**
- Print on checks: "This check expires and is void 25 days from issue date"
  - ✓ **Don't re-issue check until first check expires**

http://caselaw.findlaw.com/nj-superior-court-appellate-division/1093442.html

http://www.jurispro.com/files/documents/doc-1066206627-article-2071.pdf

Someone who accepts an

expired Instrument

Has No Legal Standing!

As a Holder in Due Course

HIDC & Controlled Check Stock

- Robert Triffin v. Somerset Valley Bank and Hauser Contracting Company

  - 80 counterfeit checks totaling $25,000 on authentic-looking check stock

  - Bank returns them as counterfeit

  - Triffin buys $8,800 in returned checks from four check cashing stores, and as a HIDC, sued Hauser for NEGLIGENCE for not controlling his check stock.

http://caselaw.findlaw.com/nj-superior-court-appellate-division/1315264.html

HIDC & Controlled Check Stock

- Lower court rules in favor of Triffin, saying **the** checks looked "genuine"
- Hauser appealed; claimed he never had possession of the checks or authorized their issuance.
- **Federal Appellate Court UPHELD lower court; ruled the checks looked "genuine"**
- **Hauser Contracting ordered to pay Triffin $8,800**
- **Solution: Use controlled, high security checks**

http://caselaw.findlaw.com/nj-superior-court-appellate-division/1315264.html

HIDC & Controlled Check Stock

Robert Triffin v. Pomerantz Staffing Services

- 18 counterfeit checks drawn on Pomerantz' acct cashed at check cashing store. All checks under $400.
- Each check had a PRINTED warning: "THE BACK OF THIS CHECK HAS HEAT SENSITIVE INK TO CONFIRM AUTHENTICITY."
- Check casher cashed the checks without examining the checks

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html

HIDC & Controlled Check Stock

Robert Triffin v. Pomerantz Staffing Services…

- Counterfeit checks looked authentic on face, but had no heat-sensitive ink on the back
  - Because casher failed to verify heat-sensitive ink on back, it could not claim Holder in Due Course status
  - Triffin **LOST** because the security feature was absent, and forged signature was not specifically disavowed
- Pomerantz' check security features helped save him

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html

Embezzlement

Embezzlement

Embezzlers

Embezzlers

Robert Rizzo

Former City Manager, Bell, CA

Robert Rizzo

Russell R. Wasendorf, Sr.

The largest embezzlement case in 2012: **$215 million**, stolen over 20 years from 13,000 clients of Peregrine Financial Group, aka BFGBest! **Wasendorf, 64**, of Cedar Falls, Iowa.

Russell R. Wasendorf, Sr.

Sentence: 50 years

Harriette Walters

Served as **Tax Assessments Manager**
for the District of Columbia

Harriette Walters

Sentence: 17 years

Atty: "She had a rough childhood. She stole the money so that she could give some of it away, which made her feel better about herself."

Control Incoming Mail to Avoid Employee Theft

Companies should use their bank's

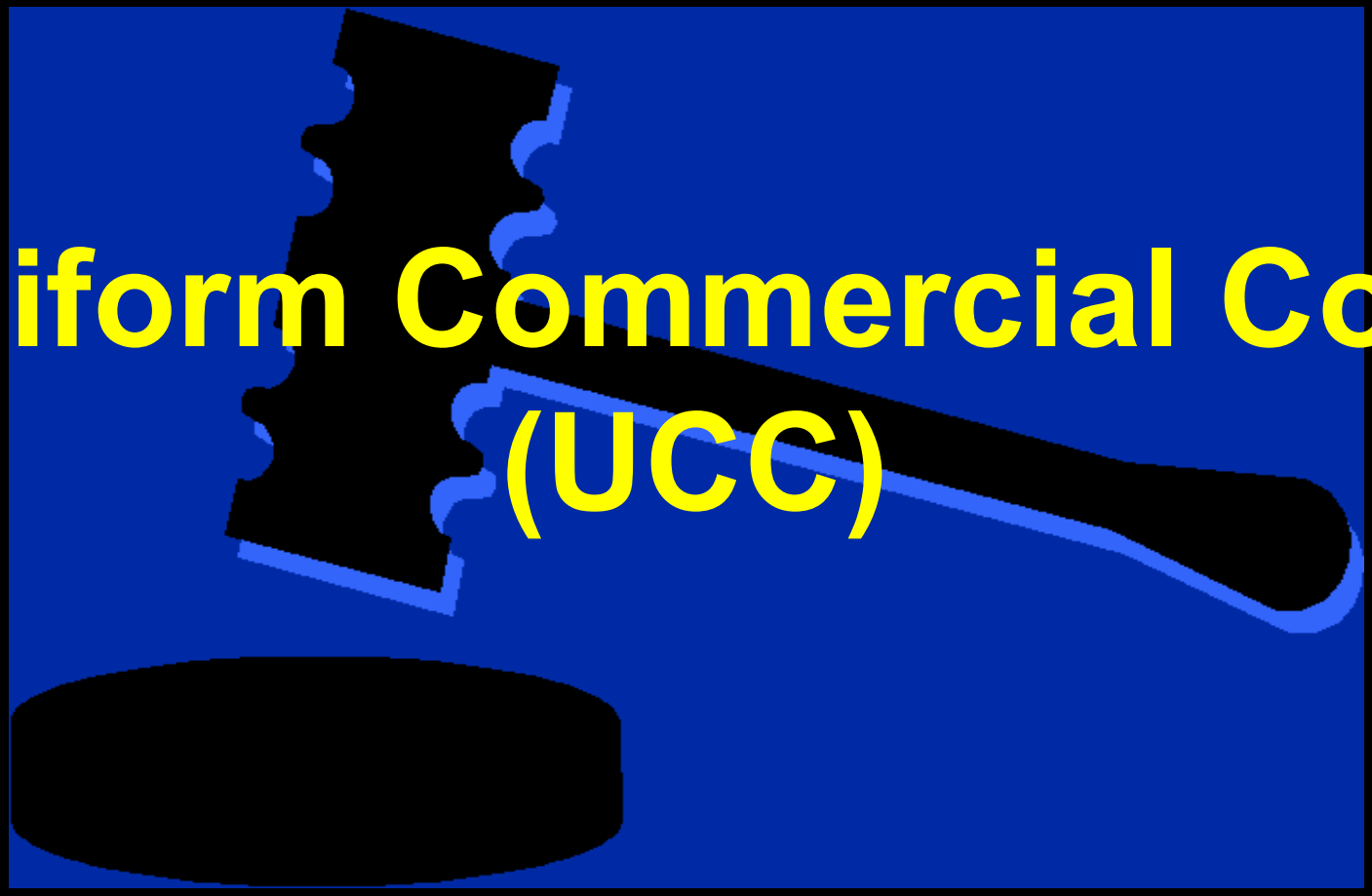
Lockbox Service

Cost: $5/day + $0.35 / item

Lockbox completely eliminates the risk of diverted deposits.

You cannot hire someone that inexpensively!

Uniform Commercial Code (UCC)



"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

Control Outgoing Mail to Avoid Employee Theft

Deterrence

Surprise Audits

Surprise Audits are an effective psychological deterrent against potential embezzlers.

Surprise Audits

- ✓ Obtain and audit original source documents
- ✓ Don't let the auditee retrieve the documents. Pull them yourself if possible
- ✓ Adequate segregation of duties is the key. (In small organizations, find someone to monitor person who handles money)
- ✓ Test the composition of the cash collected with the composition of deposit
- ✓ Don't let the auditee explain away exceptions to your tests
- ✓ Prosecute if possible. Inform employees what happened

If you suspect embezzlement and intend to prosecute, DO NOT tamper with evidence.

DO NOT physically search the computer.

Make a "mirror" of the hard drive and search the mirror. Searching the computer is tampering with evidence.

“Common Sense” Controls to Prevent Fraud

- Vendors
  - Segregate approval of vendors from authorization of payments
  - Current authorized signer list
  - System that won’t allow duplicate payments
  - Timely vendor payments including verification of goods / services
  - Timely reconciliation of paid checks and review of check images to records

“Common Sense” Controls to Prevent Fraud

- **Purchasing (CC’s / P Cards)**
  - **Written Policy with guidelines**
  - **Cardholder acceptance / Signature**
  - **Merchant / Category restrictions**
  - **Timely review of charges**

- **Skimming of Cash**
  - **Segregation of Duties**
  - **Policy on Voids / Credits**
  - **Pre-numbered Receipts / Information**
  - **Regular and Frequent Surprise Cash Counts**

Embezzlement Detection

Warning Signs

Warning Signs

- **Extravagant lifestyle** that seems incongruent with employee compensation
- **Unusual behavior** of key employees, such as depression or mood swings
- **Reluctance** of key employees to take **vacations**
- **Discomfort or unease** when another employee must fill in for them

Warning Signs

- First major purchase is usually a new vehicle
- Home renovations
- Boats
- Exotic vacations
- Second homes

Embezzlement Prevention Strategies

Educate Your Employees

Employees are your best detection source.

Educate them about what fraud is, how it hurts everyone, and how to report it.

Embezzlement Prevention Strategies

- Separation of duties

  UCC: Organizations are responsible for acts of its employees

- Review bank statements / check images

Embezzlement Prevention Strategies

- Bank Reconciliation performed by someone other than the check issuers
- Income Statement and Balance Sheet must be current EVERY month
- Examine Income Statement, Balance Sheet, Accounts Payable, Accounts Receivable monthly
- Examine A/R detail for "credit memos."
- Inside A/R, look at individual customers' history for credit memos.

Embezzlement Prevention Strategies

- Establish confidential support systems for employees with addiction, emotional or mental issues.
- Increase Embezzlement insurance
- Add Cyber Crime, Check Fraud insurance

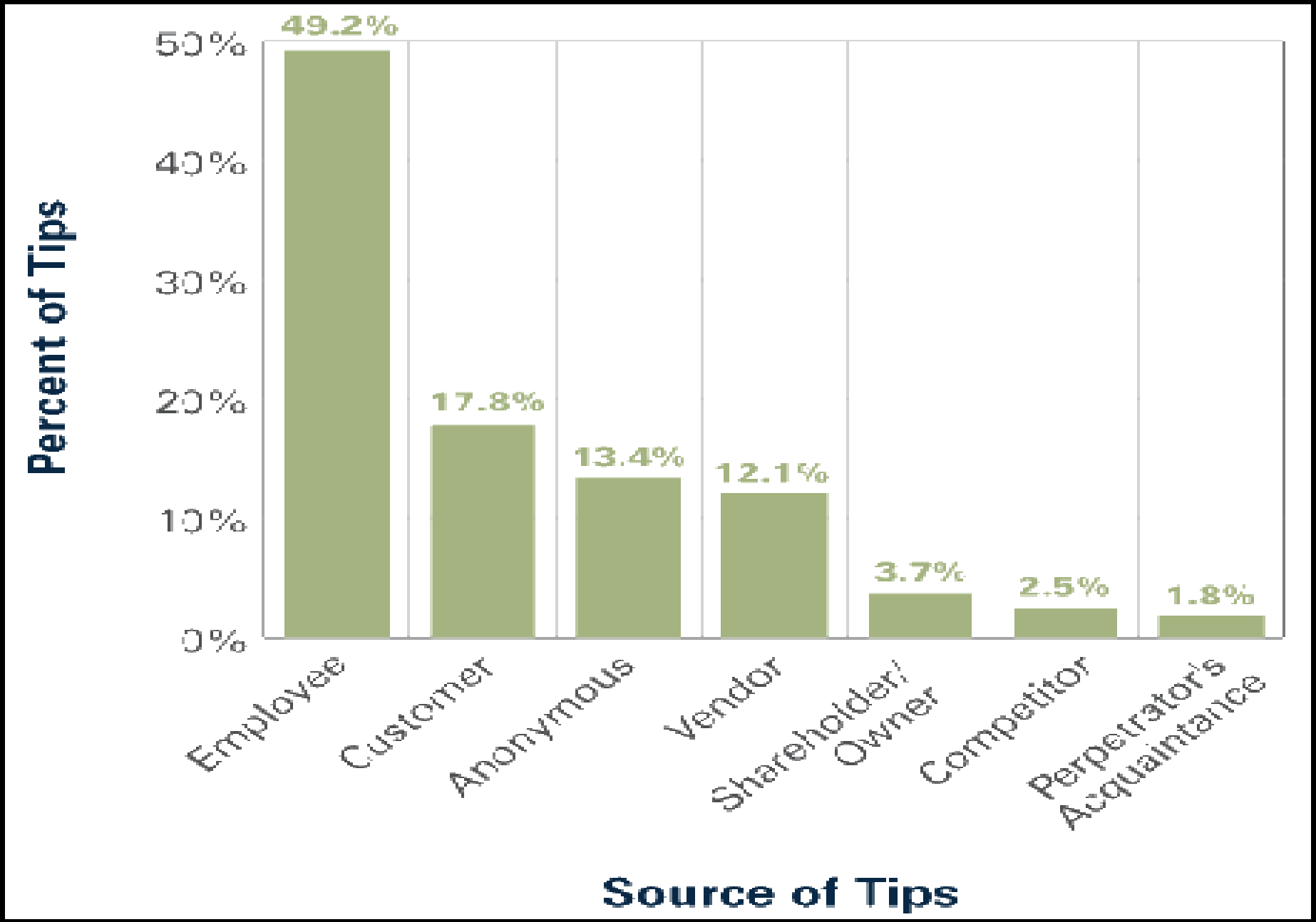
Tip Hotline

Anonymous Tips: #1 method of discovering embezzlement

Set up an anonymous "Tip Hotline" accessible by:

1. Employees
2. Vendors
3. Taxpayers
4. Outsiders

Source of Tips



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

Please review Embezzlement

in

Frank Abagnale's Fraud Bulletin

www.safechecks.com

Greg Litster
President
SAFEChecks
(800) 949-BANK
(818) 383-5996 cell
greg@safechecks.com
glitster@aol.com