Fast, Furious & Gone - Embezzlement, Cyber Crime and Check Fraud –
The New Faces of Fraud

Greg Litster
SAFEChecks
(800) 949-2265
greg@safechecks.com
This presentation contains 211 slides. To facilitate your review, these are the topics and slide numbers:

- Embezzlement 3-47
- Cyber Crime 48-103
- Track Your Kids’ Keystrokes 94
- Track Your Kids’ Cell Phones 98
- Check Fraud 104-176
  - Altered and Added Payee Names 118
  - Controlled Check Stock 130
  - $154,000 Lawsuit over an Altered Payee 143
- Check 21 177-198
- Holder in Due Course 199-210
- Contact Info 211
Embezzlement
11,000 people were arrested for embezzlement in 2011

*The Marquet Report On Embezzlement, 2012*
Categories of Embezzlement
(aka “Occupational Fraud”)

• Fraudulent payments/disbursements

• Theft of cash (greenbacks)

• Theft of property or information

Association of Certified Fraud Examiners “Report to the Nations” 2010
### ALL Industries Are Vulnerable

<table>
<thead>
<tr>
<th>Industry</th>
<th># Cases</th>
<th>$ Gross Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>58</td>
<td>$86,792,000</td>
</tr>
<tr>
<td>Healthcare</td>
<td>49</td>
<td>$24,679,000</td>
</tr>
<tr>
<td>Non-profit</td>
<td>58</td>
<td>$24,650,000</td>
</tr>
<tr>
<td>Food &amp; Agriculture</td>
<td>10</td>
<td>$20,228,000</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>30</td>
<td>$20,119,000</td>
</tr>
<tr>
<td>Real estate</td>
<td>24</td>
<td>$19,887,000</td>
</tr>
<tr>
<td>Government</td>
<td>44</td>
<td>$18,832,000</td>
</tr>
<tr>
<td>Apparel</td>
<td>1</td>
<td>$16,000,000</td>
</tr>
<tr>
<td>Education</td>
<td>18</td>
<td>$14,607,000</td>
</tr>
<tr>
<td>Automotive</td>
<td>10</td>
<td>$14,305,000</td>
</tr>
<tr>
<td>Construction</td>
<td>16</td>
<td>$13,943,000</td>
</tr>
<tr>
<td>Business Services</td>
<td>12</td>
<td>$8,599,000</td>
</tr>
</tbody>
</table>
## 2009 → 10 Largest Embezzlement Cases

<table>
<thead>
<tr>
<th>Name</th>
<th>Victim Organization</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sujata &quot;Sue&quot; Sachdeva</td>
<td>Koss Corp.</td>
<td>$31,000,000</td>
</tr>
<tr>
<td>Ricardo Figueredo</td>
<td>Bank of America</td>
<td>$29,592,000</td>
</tr>
<tr>
<td>Yolanda Serrano</td>
<td>Southeast Petro Distributors</td>
<td>$12,700,000</td>
</tr>
<tr>
<td>Jerry D. Cash</td>
<td>Quest Resources Corporation</td>
<td>$10,000,000</td>
</tr>
<tr>
<td>Annette C. Yeomans</td>
<td>Quality Woodworks</td>
<td>$ 9,900,000</td>
</tr>
<tr>
<td>Rick Eddleman</td>
<td>Decipher, Inc.</td>
<td>$ 8,900,000</td>
</tr>
<tr>
<td>James T. Hammes</td>
<td>G&amp;J Pepsi-Cola Bottlers</td>
<td>$ 8,711,000</td>
</tr>
<tr>
<td>Thom W. Williams</td>
<td>Verso Paper Co.</td>
<td>$ 8,710,000</td>
</tr>
<tr>
<td>Rev. John Skehan</td>
<td>St. Vincent Ferrer Catholic Church</td>
<td>$ 8,600,000</td>
</tr>
<tr>
<td>Nathan John Mueller</td>
<td>ING Reinsurance Corp.</td>
<td>$ 8,500,000</td>
</tr>
</tbody>
</table>
## 2010 → 10 Largest Embezzlement Cases

<table>
<thead>
<tr>
<th>Name</th>
<th>Victim Organization</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Melissa G. King</td>
<td>Sandhogs’ Union Local 147</td>
<td>$42,608,232</td>
</tr>
<tr>
<td>Arnold Mullen</td>
<td>Paul and Phyllis Fireman Foundation</td>
<td>$25,000,000</td>
</tr>
<tr>
<td>Nancy Saldana Moreno</td>
<td>Davis-Lynch Inc.</td>
<td>$15,000,000</td>
</tr>
<tr>
<td>Donna White</td>
<td>John W. Stone Oil Distributor LLC</td>
<td>$12,700,000</td>
</tr>
<tr>
<td>Charles Antonucci, Sr.</td>
<td>US TARP Program</td>
<td>$11,200,000</td>
</tr>
<tr>
<td>Terry Scott Welch</td>
<td>Wachovia Bank</td>
<td>$11,200,000</td>
</tr>
<tr>
<td>Douglas Ross Zuber</td>
<td>Harvard Investments, Inc.</td>
<td>$11,000,000</td>
</tr>
<tr>
<td>Bernie D. Metz</td>
<td>Center Valley Federal Credit Union</td>
<td>$8,989,484</td>
</tr>
<tr>
<td>Lori Lockman Julian</td>
<td>William C. Webb Co.</td>
<td>$7,345,050</td>
</tr>
<tr>
<td>Chris Orsaris</td>
<td>Major Automotive Companies</td>
<td>$7,000,000</td>
</tr>
<tr>
<td>Alleged Perpetrator</td>
<td>Victim Organization</td>
<td>$ Embezzled</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Gary Foster</td>
<td>Citigroup</td>
<td>$22,000,000</td>
</tr>
<tr>
<td>Judy Del Galdo</td>
<td>Hi-Fashion Fabrics Inc.</td>
<td>$16,000,000</td>
</tr>
<tr>
<td>Linda Speaks Tribby</td>
<td>Wachovia Bank</td>
<td>$14,170,000</td>
</tr>
<tr>
<td>Patricia K. Smith Baierl</td>
<td>Acura</td>
<td>$10,200,000</td>
</tr>
<tr>
<td>Susan A. Curtis</td>
<td>Webster Bank &amp; B of A</td>
<td>$6,200,000</td>
</tr>
<tr>
<td>George Todd Powers</td>
<td>Iowa State Bank</td>
<td>$5,987,000</td>
</tr>
<tr>
<td>Stephen Marich</td>
<td>First National Bank of Ely</td>
<td>$5,900,000</td>
</tr>
<tr>
<td>Kinde L. Durkee</td>
<td>Various Calif Democratic Political Campaigns</td>
<td>$5,844,000</td>
</tr>
<tr>
<td>Stephen C. Greb</td>
<td>La Salle University</td>
<td>$5,600,000</td>
</tr>
<tr>
<td>Georgia A. Engelhart</td>
<td>Tanklages Construction</td>
<td>$4,800,000</td>
</tr>
</tbody>
</table>
Embezzlement happens when:

...the "Fraud Triangle" is present –

- Motive
- Opportunity
- Rationalization

and

Effective controls to prevent fraud are lacking.
One Embezzlement Cause

An inappropriate “tone” set by upper management significantly contributes to fraud – overriding established safeguards, unethical behavior or attitudes, pressuring employees to meet unrealistic goals.
Embezzlement Reasons

- False sense of “entitlement”
- Financial need
- Lavish lifestyle
- Gambling issue
- Shopping addiction
- Substance abuse
- Support a personal business
- Support significant other
They believe that:

• They must save a family member in dire circumstances

• They are in a desperate financial situation, and “all could be lost”

• No outside or other help exists

• They are only “borrowing” the money

• The consequences of their actions will be minimal

• What they are doing is NOT wrong – “management deserves it” or “everyone does it”
Profile of an Embezzler

1. No single set of characteristics
2. Corroborating circumstances and “warning signs”
3. They must:
   a. Hold a position of confidence within the organization
   b. Be able to recognize an opportunity for fraud
   c. Possess the technical skills necessary for theft
4. Personal financial need + the ability to rationalize stealing company funds

“The amount that can be stolen is directly proportionate to the amount of power, responsibility and trust associated with a specific position.”
Profile of an Embezzler
(for losses over $100,000)

**Age**

*Average Age when Starting:* 42 Years Old

*Average Age when Arrested:* 46 Years Old

*Average Length of Duration:* 4 Years

Over 50% of all cases are committed by people 31 to 45

The greatest losses come from people over 60
Profile of an Embezzler

Position Held:
Finance/Accounting = 87%

Lone Perpetrator = 83%

Conspiracy = 17%
Profile of an Embezzler

(Amounts > $100,000)

• Women = 65%

• Men = 35%  (Men steal 25% more money)

• 85% of perpetrators had never been charged or convicted of a fraud-related offense

Over-reliance on background investigations is unwise.
## Embezzlement Schemes

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Number</th>
<th>%</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forged/unauthorized checks</td>
<td>172</td>
<td>38%</td>
<td>$106,408,000</td>
</tr>
<tr>
<td>Unauthorized electronic transfers</td>
<td>60</td>
<td>13%</td>
<td>$90,442,000</td>
</tr>
<tr>
<td>Diversion of cash receipts</td>
<td>92</td>
<td>21%</td>
<td>$56,296,000</td>
</tr>
<tr>
<td>Bogus Vendors</td>
<td>24</td>
<td>5%</td>
<td>$44,306,000</td>
</tr>
<tr>
<td>Payroll shenanigans</td>
<td>39</td>
<td>9%</td>
<td>$17,578,000</td>
</tr>
<tr>
<td>Credit card abuse</td>
<td>29</td>
<td>7%</td>
<td>$15,488,000</td>
</tr>
<tr>
<td>Fraudulent reimbursements</td>
<td>22</td>
<td>5%</td>
<td>$10,112,000</td>
</tr>
<tr>
<td>Bogus loan scheme</td>
<td>7</td>
<td>2%</td>
<td>$1,969,000</td>
</tr>
<tr>
<td>Theft from Tax or Benefit accounts</td>
<td>2</td>
<td>4%</td>
<td>$973,000</td>
</tr>
<tr>
<td>Inventory or equipment theft</td>
<td>1</td>
<td>2%</td>
<td>$414,000</td>
</tr>
<tr>
<td>Category</td>
<td>Examples</td>
<td># of Mos.</td>
<td>Median Loss</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Fictitious Billing</td>
<td>Employee <em>creates a shell company</em>; submits invoices for payment.</td>
<td>24</td>
<td>$128,000</td>
</tr>
<tr>
<td>Check Tampering</td>
<td>- Employee <em>steals blank checks or voids pre-printed checks</em>, and makes payable to self or accomplice.</td>
<td>24</td>
<td>$131,000</td>
</tr>
<tr>
<td></td>
<td>- Employee <em>steals outgoing vendor checks</em>, alters and deposits them.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deposit Fraud</td>
<td>Sale is recorded on Company books, but money is stolen/diverted and not deposited.</td>
<td>18</td>
<td>$100,000</td>
</tr>
<tr>
<td></td>
<td><strong>Invoices in A/R are offset with Credit Memos.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Solutions

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Tampering</td>
<td>Employee steals checks</td>
<td><strong>Separation of Duties;</strong>&lt;br&gt;<strong>Timely Reconciliation;</strong>&lt;br&gt;<strong>On-line review of paid checks</strong></td>
</tr>
<tr>
<td>Fictitious Billing</td>
<td>Employee creates a shell company and submits invoices for payment;</td>
<td>New vendors must be reviewed by second person;&lt;br&gt;<strong>Separation of Duties</strong>&lt;br&gt;<strong>Surprise audits</strong></td>
</tr>
<tr>
<td>Deposit Fraud</td>
<td>Sale is recorded on Company books, but money is stolen, and deposits are diverted.&lt;br&gt;Invoice in A/R is offset with a Credit Memo; account is not delinquent</td>
<td><strong>Control Incoming Receipts!</strong>&lt;br&gt;Open mail in dual custody,&lt;br&gt;<strong>Use Your Bank’s Lockbox Service</strong>&lt;br&gt;<strong>Hire your CPA</strong>&lt;br&gt;to audit A/R for credit memos</td>
</tr>
</tbody>
</table>
Embezzlement via "shell" Companies
Embezzlement via “shell” Companies

Anita Collins, 67, Charged With Stealing $1 Million From NY Archdiocese

January 30, 2012
NEW YORK  A 67-year-old woman with a criminal record for theft has been charged with siphoning $1 million in donations while working in a finance office of the Roman Catholic Archdiocese of New York, church officials announced Monday (Jan. 30, 2012).

The archdiocese said it did not conduct a criminal background check when the employee, Anita Collins, was hired in 2003. Church officials were unaware until recently that she had been convicted of grand larceny in one case and pleaded guilty to a misdemeanor in another.

Officials said that over seven years Collins sent fake invoices to the archdiocese, then issued 450 checks on accounts she controlled, all in amounts under the $2,500 threshold that would have required a supervisor's approval.
Embezzlement via Diverted Deposits
Use Your Bank’s Lockbox Service

Cost: $5/day + $0.25 - 0.30/item

Lockbox completely eliminates the risk of diverted deposits.
And, you cannot hire someone that inexpensively!
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 Detection
Detection of Embezzlement

- Tip: 40.2%
- Management Review: 15.4%
- Internal Audit: 13.9%
- By Accident: 8.3%
- Account Reconciliation: 6.1%
- Document Examination: 5.2%
- External Audit: 4.6%
- Surveillance/Monitoring: 2.6%
- Notified by Police: 1.8%
- Confession: 1.0%
- IT Controls: 0.8%
Small companies are very susceptible to fraud, due in part to the limited resources they devote to anti-fraud controls.
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
SOLUTIONS
Educate Your Employees

Employees are the best detection source. Educate them about what fraud is, how it hurts everyone, and how to report it.
Additional Tools and Strategies

• Separation of duties
  UCC: Company is responsible for acts of its employees

• Review bank statements / check images

• Bankers: Teach Owners how to access online banking to view check images
Additional Tools and Strategies

- Income Statement and Balance Sheet must be current EVERY month.


- Examine A/R detail for “credit memos.”

- Inside A/R, look at individual customers’ history for credit memos.

- Bank Reconciliation performed by someone other than the in-house bookkeeper.
Establish support systems for employees with addiction, emotional or mental issues.

Increase defalcation (embezzlement) insurance coverage

Add Cyber Crime, Check Fraud insurance
Surprise Audits are an effective psychological deterrent against potential embezzlers.
An Anonymous Tip is the #1 method of discovering Embezzlement.

Set up a “Tip Hotline” accessible by:

1. Employees
2. Vendors
3. Customers
4. Outsiders
Impact of Hotlines on Detection

- **Tip**: 47.1% (Organizations With Hotlines) 33.8% (Organizations Without Hotlines)
- **Internal Audit**: 16.5% (Organizations With Hotlines) 11.2% (Organizations Without Hotlines)
- **Management Review**: 15.7% (Organizations With Hotlines) 15.7% (Organizations Without Hotlines)
- **Account Reconciliation**: 4.7% (Organizations With Hotlines) 7.8% (Organizations Without Hotlines)
- **By Accident**: 4.6% (Organizations With Hotlines) 11.9% (Organizations Without Hotlines)
- **Document Examination**: 3.7% (Organizations With Hotlines) 6.5% (Organizations Without Hotlines)
- **Surveillance/Monitoring**: 3.0% (Organizations With Hotlines) 2.2% (Organizations Without Hotlines)
- **External Audit**: 1.4% (Organizations With Hotlines) 7.3% (Organizations Without Hotlines)
- **IT Controls**: 1.4% (Organizations With Hotlines) 0.4% (Organizations Without Hotlines)
- **Notified by Police**: 1.0% (Organizations With Hotlines) 2.3% (Organizations Without Hotlines)
- **Confession**: 0.9% (Organizations With Hotlines) 1.1% (Organizations Without Hotlines)
Please review Pages 2 – 3 in the Abagnale Fraud Bulletin, Volume 11 published by SAFEChecks.
Cyber Crime
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 redirect a legitimate website’s traffic to a fraudulent website.

Hacker is paid by the click.
**Trojan Horse**

*Trojan Horse* - a malicious program concealed in something innocuous.

Facebook
MySpace
Pictures
Video
Free music downloads
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.
Target Banks
Facebook
900 Million Users
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.
“Smishing” –
Using a text message to get personal information.
“Vishing” – Using the telephone to get personal information, using real names known to the victim.
“Physical” Attacks –

“Skimmers” in credit/debit card devices
Infected flash/thumb drives
Ramnit Worm Threatens Online Account

Facebook Targeted by Fraudsters Seeking Log-in Credentials
Hi Jeff,

www.facebookk.com

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
Phishing Hosts
Phishing Hosts

Hard to tell the difference?

Fake URL address.
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.
Who won the lawsuit?
The Customer!
WHY did the Bank lose?

1. Bank wired out funds **exceeding** 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, but

4. Was **not** awarded attorney fees (> $250K)
Solutions
Use a properly configured FIREWALL, which helps make your computer invisible on the Internet.
Online Banking

Require 2 different computers to move money.

1. Computers #1-99 to “originate”

2. Computer #100 to “release”
Smartphone & Tablet Security

Free app: MyLookout.com

Anti-virus and Malware Protection
Lost Device (Locate and scream)
Data Backup
**Scenario:** A title insurance company gives John Doe a check at a closing. John Doe deposits check via mobile app, then gives the check back, asking that it be made payable to John Doe and Jane Doe. A Stop Payment is not placed on the first check.
1. If a check leaves your possession and is returned for a replacement, place a stop payment on the returned check.

2. Recipient MUST sign an affidavit stating the check was not “deposited”, and recipient is responsible for all legal fees for an act of fraud.

3. An Affidavit does not provide protection, only a right to sue and collect legal fees.
What’s a Company’s Biggest Security Risk? YOU.

- Opening an unexpected email attachment from a colleague
  - **HOW YOU SEE IT:** Being a good co-worker
  - **HOW HACKERS SEE IT:** An opportunity to install a virus inside the corporate network; spreading the firewall

- Bringing a new personal gadget to the work network
  - **HOW YOU SEE IT:** An opportunity to keep up with the latest technology
  - **HOW HACKERS SEE IT:** A new route for viruses and malware to make their way into corporate systems

- Using personal Web email for work
  - **HOW YOU SEE IT:** Making it easier to work from home or to move files between computers
  - **HOW HACKERS SEE IT:** A path to access critical data from secretly unprotected servers

- Posting job details on LinkedIn
  - **HOW YOU SEE IT:** Creating a professional presence and finding another potential job
  - **HOW HACKERS SEE IT:** Reconnaissance data to map out company hierarchies and target specific users with social-engineering attacks

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...
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-cripping 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 breached. Here's a look at what to do when it happens to you.
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
Blocking Email Phishing Attacks and Spam
Email Server Protection

(Better protection with more users)

- 7 Million email accounts
- $50/month
- 40 users, 1 domain, $.99/ addl user

AppRiver.com
Antivirus, Anti-Spyware Software

Software to identify, neutralize or eliminate malicious code

- Monitors behavior of all programs.
Utilize Layered Approach for ACH & Wire Transactions

- Dual Authorization
- “Out of Band” Authentication
- Tokens
- Transactional Alerts via Text, E-mail or Voice Calls
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.
Password Assault Figures

6.5  Average number of passwords for a Web user with 25 accts

100,000,000+  Passwords posted online in the past year

8.2 billion  Password combinations per second able to be tried by a PC running a single AMD Radeon HD7970 GPU.
5 Years Ago

The Time it Took a Hacker to Randomly Guess Your Password

<table>
<thead>
<tr>
<th>Length</th>
<th>lowercase</th>
<th>+ Uppercase</th>
<th>+ numbers and symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 Characters</td>
<td>10 Minutes</td>
<td>10 Hours</td>
<td>18 Days</td>
</tr>
<tr>
<td>7 Characters</td>
<td>4 Hours</td>
<td>23 Days</td>
<td>4 Years</td>
</tr>
<tr>
<td>8 Characters</td>
<td>4 Days</td>
<td>3 Years</td>
<td>463 Years</td>
</tr>
<tr>
<td>9 Characters</td>
<td>4 Months</td>
<td>178 Years</td>
<td>44,530 Years</td>
</tr>
</tbody>
</table>
Today:
It Takes a Hacker 12 Hours
to Randomly Guess Your Password

<table>
<thead>
<tr>
<th>Length</th>
<th>Upper + Lower + Numbers + symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Characters</td>
<td>12 Hours</td>
</tr>
</tbody>
</table>

This $12,000 computer containing 8 AMD Radeon GPU cards can brute force the entire keyspace for any eight-character password in 12 hours.
Track Your Kids Keystrokes
Kids keep 2 Facebook Accounts
(Mom only sees one)
Track Your Kids’ Keystrokes

Home and Office
SPECTOR PRO 2010
Powerful Monitoring, Extreme Ease of Use
Records Every Exact Detail of Their Computer and Internet Activity.

eBLASTER 2010
Remote Monitoring Software
Knowing EVERYTHING They Do Online is as Easy as Checking Your Email.
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.
Record and Forward Text Messages

Protect Your Child with eBLASTER Mobile for Android

Cell Phone Monitoring from SpectorSoft has arrived. Now you can monitor your child's Android phone from anywhere, whether you're in another room at home, at work, across town, or thousands of miles away.

With eBLASTER Mobile, you'll see:

If Your Child Is Where They Are Supposed To Be

Set up virtual fences around key locations, such as homes, schools, malls, libraries, sports facilities, friends' houses, work locations ... and be notified when your child enters or leaves those important places.

Have a Question?
Call Toll-Free 24/7
888-598-2788

Special Offer:
$69.95
Buy Now!

FREE SAMPLE REPORT

Enter your email address to receive a FREE Sample eBLASTER Mobile Activity Report.
Track Your Employees

**Corporate Solutions**

**SPECTOR 360**
Company-Wide Monitoring

*Know What All Your Employees Are Doing Online by Viewing Simple Reports and Charts.*

**SPECTOR CNE**
Corporate Network Edition

*Record, Archive and Review your Employees’ PC and Internet Activity.*
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)  Aso Sex Location (Race/Picture)
BF/GF  Boyfriend/Girlfriend
BBB  Be Right Back
C9  Code 9 - means parents are around
GNOC  Get Naked On Cam (webcam)
GTG  Get to Go
IDK  I don't know
(L)MIRL  (Lets) meet in real life
LOL  Laugh Out Loud
MofF  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
PR  Parent In Room
POS  Parent Over Shoulder
PRON  Porn
PRW  Parents Are Watching
S2R  Send To Receiver (pictures)
TDIM  Talk Dirty To Me
# Sexting Slang Terms

**Common Sexting Slang Terms**

*Warning: some of these terms are vulgar.* This list is nowhere close to exhaustive, words can be combined, removed, and invented on the fly.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Code for an anus</td>
</tr>
<tr>
<td>143</td>
<td>Big clit</td>
</tr>
<tr>
<td>cu46</td>
<td>Cum iphone 4/6</td>
</tr>
</tbody>
</table>
| DUM  | Dummies 
| GNOC | A girl's crotch |
| GYPO | Gypsy oops |
| GNRM | Gnome run me |
| FMH  | Fuck me hard |
| IWS  | I want sex |
| IIT  | I'm in theme |
| Q2C  | Queen to cum |
| RUH  | A rub 
| TDTM | Teen dirt my mouth |
| S2F  | Squirting flu |
| NIFOC | No I will face on computer |
| SorG | Songs on ring 
| JO   | Jump off |
| PAW  | Panty around waist |
| PIR  | Panty in the ring |
| POS  | Panty off skirt |
| YWS  | You will see |
| WYCM | Wank your cum man |

---

*Slang Dictionary*

Word Definitions, Translate & More.
Download Dictionary Boss Today!


*Parenting Classes Online*

Get a Parenting Classes Online Your Source For Online Education.
[VirtualStudies.com](http://VirtualStudies.com)

*Is He Cheating On You?*

1) Enter His Email Address 
2) See Hidden Pics & Social Profiles Now!
[Speakeo.com/Cheating-Sp...](http://Speakeo.com/Cheating-Sp...)

*Improve Attention Today*

Successful program for improving focus, attention, and communication
[www.learn2listen.com](http://www.learn2listen.com)

---

Please review Resources listed in the Abagnale Fraud Bulletin, Volume 11, Page 11 published by SAFEChecks.
Check Fraud...

Why talk about Check Fraud?
“Despite advances in fraud protection and prevention in recent years, the rate of payment fraud attacks remains stubbornly high.... notwithstanding the precipitous drop in check volume over the last several years, **checks continue to be widely used and abused**, and **fraud via check payments remains the overwhelming threat faced by companies.**”

Association for Financial Professionals (AFP) 2011 Payments Fraud and Control Survey
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%)

- CHECKS 91%
- ACH DEBITS 28%
- Consumer Debit/Credit Cards 18%
- Corporate Cards 14%
- ACH Credits 7%
- Wire Transfers 6%
Fraud Losses by Method
(How Dollars were actually lost)

Percentage

- CHECKS 60%
- Consumer Debit/Credit Cards 20%
- Corporate Cards 10%
- ACH DEBITS 5%
- ACH Credits 3%
- Wire Transfers 1%
ACH Debit Fraud

- Utilize ACH Debit Filter/Block
- Select “Return All” as your default item instructions for ACH Debit Filter
- Set maximum debit limit for all Approved Vendors
- Stay on the alert for small dollar ACH credits
Frank Abagnale

*Catch Me If You Can*

Technology is making Frank Abagnale’s “gift” achievable by mere mortals
Check Fraud Scams

...if it seems too good to be true....

It’s NOT!
Many variations – same scam:

● “You have won...” an online lottery or large prize
Many variations – same scam:

- You are paid with a check for more than the value of the item you’re selling...
Many variations – same scam:

- You are paid with a bogus Cashier’s Check after banking hours so the check cannot be verified...
The Evolution of Check Fraud and Banker Solutions
Counterfeit Checks

...Banks developed Positive Pay
Altered Payees

...Banks developed Payee Positive Pay
Added Payee Names

(Printed 2 lines above the original Name)

NO BANKER SOLUTION!
Added Payee Names

Checks pass right through Payee Pos Pay!

How?
Typical Check Layout

Open Areas Where Forgers Add A New Payee Name
Strategies to Prevent Check Fraud
#1. 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. Reduces bank per-item fees
4. Increases payment float by 40+ days
5. Reduces interest expense
6. Potential for Rebates or Rewards
7. Terminating a card is easier than closing a checking account.
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
Check Fraud prevention strategies begin with a high security check.
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
**Controlled Check Stock** is the first and most important security feature. Controlled check stock has an identifier that is unique to each company.

**Uncontrolled check stock** is off-the-shelf, generic check stock that can be purchased entirely blank by 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

- SuperBusinessCheck designed by Frank Abagnale
  - 16 security features
#2. Payee Positive Pay

Web: PositivePay.net
Positive Pay...

...a powerful tool!
Transmit Check Data to your Bank

1. Company Issues Checks
2. Transmit Check Data to your Bank
Company Releases Checks

They Deposit Checks

To Employees

To Vendors

Releases Checks
Company

Issues Checks

Employees

Vendors

Deposit Checks

Other Banks Present Checks to your Bank

① Company

Issues Checks

Employees

Vendors

Deposit Checks

Other Banks Present Checks to your Bank
Company Issues Checks

Employees

Vendors

Issues Checks

Deposit Checks

Other Banks Present Checks to your Bank

your Bank Matches Checks to Issuance Data

Issued Data
- CK #123 $50.00
- CK #124 $10.00
- CK #125 $150.00
- CK #125 $1500.00
- CK #729 $200,000

Paid Checks
- CK #123 $50.00
- CK #124 $10.00
- CK #123 $50.00
- CK #125 $1500.00
- CK #729 $200,000

- NO CK ON FILE
- CK #729 $200,000
Company

Issues Checks

Employees
Vendors

Deposit Checks

Other Banks Present Checks to your Bank

Issued Data
CK # 125 $150.00
NO CK ON FILE

Issued Data

Paid Checks
CK #125 $1500.00
CK #729 $200,000

your Bank sends you the Exceptions Daily
Company

Issues Checks

Deposits Checks

You tell the bank to Pay or Return Exception Items

Other Banks Present Checks to your Bank

your Bank sends you the Exceptions Daily
Added or Altered Payee Names
Lawsuit

Cincinnati Insurance Company

v.

Wachovia Bank

$154,000 Loss from an Altered Payee
UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

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

v.

WACHOVIA BANK, NATIONAL ASSOCIATION,
Defendant.

Case No. 08-CV-2734-PJS-JJG
Preceding Events

2002: Two (2) counterfeit checks paid against Schultz Food’s account.

2003: $410 check altered to be $3,942.68.

2004: Fraudulent check drawn on Schultz Food’s account is deposited in Oklahoma; no loss.
Facts

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

2. Check is stolen; payee name changed to “Kenneth Payton.”

3. Kenneth Payton deposited check into TCF Bank; Wachovia pays the check.

4. Kenneth Payton keeps $3,500; wires balance to Singapore…“to help a refugee South African family…”

5. Money disappears.


Facts

10. Wachovia Bank pursues TCF Bank for $154,000.

11. TCF Bank hires attorneys to defend TCF.

12. TCF Bank’s attorneys take Wachovia’s “defense” and act on behalf of Wachovia (UCC § 3-119); Attorneys are paid by TCF.

13. Wachovia’s “defense” is its Deposit Agreement.
Resolution:

Wachovia Bank Wins!

You can have a great relationship with your bank and still lose a lawsuit!
UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

COURT ORDER

Based on the foregoing and on all of the files, records, and proceedings herein, IT IS HEREBY ORDERED THAT:

1. The motion of defendant Wachovia Bank, National Association for summary judgment is **GRANTED**.

2. Plaintiff’s complaint is **DISMISSED WITH PREJUDICE AND ON THE MERITS.**

LET JUDGMENT BE ENTERED ACCORDINGLY.

Dated: July 14, 2010

Patrick J. Schiltz
United States District Judge
If...

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

(Exception: Added Payees)
How to Protect Against

Altered or Added Payee Names
A Primer on Laser Printing
Preventing Altered 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**
Altered Payee Names

and

“Secure Seal” Barcode Technology
Secure Seal

is an

*image-survivable*

encrypted barcode
Typical Check Layout

Open Areas Where Forgers Add A New Payee Name
Identical Check Data, Strengthened by the Printer Driver

Secure Seal barcode
Barcode is created by a Printer Driver

For more details, call Greg Litster (800) 949-2265 or email greg@safechecks.com
Barcode contains Payee Positive Pay info:

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 piece of data
9. Date and Time Check was printed
10. Laser Printer used
11. The employee that ran the job
Payee: GREG LITSTER

Payee: GREG LITSTER
SAFEChecks
8934 Eton Avenue
Canoga Park, CA 91304

Payee name: GREG LITSTER

Check amount: $89,562.23

Check date: 3/8/2010

Check number: 300257

14 point font

Upper and lower case fonts converted into ALL UPPER CASE LETTERS
Secure Name Font 18 point

14 point font

Upper and lower case fonts converted into ALL UPPER CASE LETTERS
Secure Name Font 18 point
14 point font
Secure Number Font
Upper and lower case fonts converted into ALL UPPER CASE LETTERS
There is no room for Added Payee
Printer driver can also:

1. Accumulate check data for Positive Pay
2. Change Font size
3. Add Barcode, Secure Name & Number fonts
4. Be configured to send formatted 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
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
Uniform Commercial Code (UCC)
Ordinary Care (Bank)

- Electronic Check Presentment
- Check Truncation (Imaging)
- Selective Check Inspection
Uniform Commercial Code

“...reasonable commercial standards do not require the bank to examine the instrument 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...”
“...in the case of a person engaged in business means observance of reasonable commercial standards, 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)

That negligence contributes substantially to the forgery...

NO LIABILITY TO THE BANK
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

**Gives** legal equivalence to:
- a properly prepared “substitute check”
  (aka “image replacement document” or 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.

Frank W. Abagnale
P.O. Box 8372
Van Nuys, CA 91409-8372
(800) 755-2265

February 14, 2006

Pay to the Order of

Substitute Check Sample

Two Hundred Ninety Five and 45/100 DOLLARS

Your Bank
Los Angeles, CA

MEMO

0145

www.FraudTips.net
Check 21

Two Warranties:
- Substitute check is properly prepared
- No “double debit”

Indemnity:
- Converting bank/company 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.”
What Triggers the Indemnity?

1. Original check has non-image survivable security features, such as
   - True watermark in paper
   - Thermochromatic ink
   - Ultraviolet (UV) Ink
   AND

2. The bank would have physically inspected the check (what are your bank’s Sight Review limits?)
Indemnity Claims

An Indemnity claim can be filed one year from the Cause of Action

- Cause of action begins to run the date the injured party first learns of the loss.

- Claims must be made within 30 days after the person has reason to know or further losses cannot be claimed.

- Comparative negligence still applies
Remote Deposit Capture
aka “eDeposit”

- Technology that streamlines the deposit process
- Company scans, truncates the checks it would send to the bank for deposit
- 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
- Bank wherever & with whomever you like
  - Clients outside the bank’s traditional footprint
Remote Deposit Risks

- The company that truncates a paper check issues two *warranties* and one *indemnity* on every truncated item
  - Truncating party can be held liable for some losses that result from truncating the check
- Statute of limitations is one (1) year from when the injured party discovers the loss.
- One year is *minimum*, no maximum
“...Remote Deposit Capture is not without financial risk. First, depending on the company’s agreement with its bank, the company may need to store the original check in a secure location for a period of time in case it is needed. Second, because banks are likely to protect themselves from potential losses associated with the Remote Deposit Capture process, a company may be held liable for any Check 21 warranty and indemnity loss. The statute of limitations in the law for these types of losses is one year after the cause of action accrues.”
Big Regional Bank Remote Deposit Capture Agreement:

“… you will be liable to us to the same extent that we are liable under federal and state law regulation… including… damages, to the maker/drawer of the original check that you imaged and sent to us electronically… if: ...(c) the maker/drawer of a check you imaged and transmit to us suffered a loss that could have been prevented had the original item been presented for clearing and payment. By way of example only… if the dollar amount of the original check was $10 but was altered to read $100 before you imaged it and the maker’s account was debited for $100… You will have liability… if (i) the check in its altered state were presented in its original form (not imaged) and (ii) the alteration would have been detected.”

(Nothing about counterfeit checks or 1-year minimum timeframe.)
14. **Customer Indemnification.**

“Customer will indemnify and hold harmless (Small) Bank for liability and other losses that result from: …(v) any claim by any recipient of a Substitute Check corresponding to an item processed by Customer… that such recipient incurred a loss due to the receipt of the Substitute Check instead of the Original Check.”

16. **(Small) Bank’s Liability.**

“(Small) Bank will not be liable to Customer for any of the following… (iv) any refusal of a Payor Financial Institution to pay the Item or Substitute Check that was allegedly unauthorized, was a counterfeit, had been altered, or had a forged signature.”

*(Very clear and thorough)*
Remote Deposit Capture

Q: Is this technology bad?

A: NO! But it is not appropriate in every situation, for every company, or for every check.

- High-dollar checks carry greater risk
  - Companies issuing higher-dollar checks often pay up for high security checks with features that will protect it, and trigger the indemnity
  - Low dollar checks are safer because very few banks inspect low-dollar checks
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
“Informed Consent”

- Remote Deposit Capture needs full disclosure from the banks
  - Bank agreements must be complete and divulge all the risks
- Customers will decide if benefits outweigh risks, given their business
  - Small dollar vs. high dollar mix
Two Sides of Check 21

1. **Truncating of checks** by Bank or Company
   - Risk of indemnity charge-back

2. **Truncated checks** (corporate or personal)
   - “Injured party” could file indemnity claim if:
     - Their original check contained security features that did not carry through onto the image, **AND**
     - Payor bank would have inspected the in-clearing item based upon its dollar value, etc.
Check 21 Strategies

- Banks recommend high security checks:
  - Good for the bank and good for client

- Control what you can control
  - Use high security checks with non-image survivable features
  - Use Positive Pay w/ Payee Name Recognition
  - Reconcile bank accounts immediately
  - Separate financial duties; background checks
  - Protect incoming and outgoing mail -- stolen!
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

- Contacted Once: 22%
- Contacted 2 - 10 Times: 66%
- Contacted More Than 10 Times: 12%

Percentage
Holder in Due Course

- Paid Full Value Of Check Or More 53%
- Did Not Pay 47%
- Still In Dispute 27%
- Other 7%

Percentage
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: 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
Someone who accepts an Expired Instrument Has No Legal Standing!

As a Holder in Due Course
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
How to Obtain **Controlled Checks**?

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

  or

- SuperBusinessCheck designed by Frank Abagnale
  - 16 security features
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!
If you have a question about this presentation, feel free to call or email me:

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