Low Tech Fraud in a High Tech World: Embezzlement and Check Fraud

John Perri ● Finance Manager
SEIU Healthcare Minnesota

Greg Litster ● President
SAFEChecks
Embezzlement
Embezzlement Schemes differ across industries and by company size. Study these Resources for details about your organization:

2017 Hiscox Embezzlement Study (also see prior years)

Association of Certified Fraud Examiners


Frank Abagnale Fraud Bulletin, Volume 15
(also see prior Volumes)
Highlights

Small businesses (> 500 employees) face higher embezzlement costs than large firms.

More embezzlement events are committed by women, by a small margin. (51% v 49%)

More embezzlement actual cash losses are caused by men, by a large margin. (Almost 70%)
Highlights

More perpetrators have positions in finance and accounting, but embezzlement happens in every department, at any level.

The financial services industry continues to have the most embezzlement, but every industry has been hit.
Highlights

• $1.13 million Average (mean) loss
• $319,350 Median loss
• 37% of cases had losses of > $500,000.
• 23% had losses of > $1 million.
• 55% of companies had < 100 employees
• 68% of companies had < 500 employees
Highlights

• 37% of cases were by finance or accounting
• Median age: 48
• 29% of schemes lasted > five years
• Longest scheme lasted 41 years!
Comparison between small and large firms

2017 Hiscox Embezzlement Study
# No Industry is Immune

<table>
<thead>
<tr>
<th>Industry Class</th>
<th>% of Cases</th>
<th>Median $ Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>17.8%</td>
<td>273,843</td>
</tr>
<tr>
<td>Municipality/Government</td>
<td>12.4%</td>
<td>68,705</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>10.2%</td>
<td>558,172</td>
</tr>
<tr>
<td>Real Estate/Construction</td>
<td>9.6%</td>
<td>352,805</td>
</tr>
<tr>
<td>Labor Union</td>
<td>6.1%</td>
<td>36,647</td>
</tr>
<tr>
<td>Other Services</td>
<td>6.1%</td>
<td>165,000</td>
</tr>
<tr>
<td>Healthcare</td>
<td>5.1%</td>
<td>437,016</td>
</tr>
<tr>
<td>Retail</td>
<td>4.3%</td>
<td>485,800</td>
</tr>
<tr>
<td>IT/Telecom</td>
<td>3.3%</td>
<td>2,400,000</td>
</tr>
</tbody>
</table>

2017 Hiscox Embezzlement Study
<table>
<thead>
<tr>
<th>Schemes</th>
<th>What is it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funds Theft</td>
<td>Perpetrators take cash or bank deposits and transfer the funds to an account they control.</td>
</tr>
<tr>
<td>Check Fraud</td>
<td>Checks are altered or forged to be made payable to the perpetrator.</td>
</tr>
<tr>
<td>Vendor Invoicing and False Billing</td>
<td>Invoices from vendors are fabricated or inflated, or fictitious vendor companies are invented.</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>Company credit cards are used for personal purchases, or unauthorized credit cards are issued.</td>
</tr>
</tbody>
</table>

Almost 70% of embezzlement schemes using check fraud occurred at small companies.

2017 Hiscox Embezzlement Study
Embezzlement happens when –

The “Fraud Triangle” is present –

• Motive
• Opportunity
• Rationalization

and effective controls to prevent fraud are lacking
Embezzlement Reasons

• False sense of “entitlement”
• Financial need
• Lavish lifestyle
• Gambling issue
Embezzlement Reasons

• Shopping addiction
• Substance abuse
• Support a personal business
• Support significant other
“Oftentimes the most damaging cases result from simple skimming of relatively small amounts over time; just enough to fly below the radar. There may be no long-term diabolical plot at all. The employee errs, thinking ‘I’ll never do it again.’ And it gets easier and easier to do the next time, and the next.”

M. Jeffrey Beatrice, Partner and Bradley Former Managing Director and General Counsel for Anti-Money Laundering at Citigroup and longtime Assistant US Attorney in the Washington DC
An inappropriate “tone” set by upper management significantly contributes to fraud – unethical behavior/attitudes, overriding established safeguards, pressuring employees to meet unrealistic goals.
“Most major embezzlers appear to have been motivated by a desire to live a relatively more lavish lifestyle, rather than being driven by financial woes.”

The desire for a lavish lifestyle accounted for 65% of cases.
2nd most common motivator:

Gambling addiction = 27% of cases

Lifestyle and Gambling –
Dwarfed all other motivations
Profile of an Embezzler

96% of perpetrators had never been charged or convicted of a fraud-related offense.

Do background checks, but over-reliance on background investigations is unwise.
Profile of an Embezzler

1. No single set of characteristics

2. Corroborating circumstances and "warning signs"
Profile of an Embezzler

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
Profile of an Embezzler

Position Held:
Finance/Accounting = 68%
Lone Perpetrator = 85%
Conspiracy = 15%
### Early Warning Signs of Cash Misappropriation

- Decreasing ratio of cash to credit card sales.
- Increasing accounts receivable compared with cash.
- Delayed posting of accounts receivable payments.
- Credits against individual accounts receivable.

- Unexplained cash discrepancies.
- Altered or forged deposit slips.
- Customer billing and payment complaints.
- Increasing “soft” expenses, such as consulting.
- Employee home address matches a vendor’s address.
- Vendor address is a post office box or mail drop.
- Excessive voided, missing, or destroyed checks.

### Embezzlement Prevention Checklist
Red Flags

**Extravagance**
Embezzlers often (not always) flaunt their wealth, so watch for employees who are clearly living a lifestyle that is out of proportion to their salary.

**Egotistical risk-taker**
“Rule breaker” in and out of work life – from speeding tickets to overusing sick time.
Red Flags

**Disgruntled**
An employee who feels they are being treated unfairly may be tempted to steal to ‘even the score.’ They may be unable to relax, or may experience severe changes in behavior.

**Eager Beaver**
Be wary of the employee who comes in early, leaves late, and never takes a vacation. DO NOT ignore red flags because an employee has been with the company for a long time.
Embezzlement via Unauthorized Payments
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

Stole $50 million in improper tax refunds over 20+ years
Harriette Walters

Her 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.”

Sentence: 17 years
Rita Crundwell
Dixon, IL City Comptroller
Dixon, IL has a yearly budget of $9 million
Rita Crundwell

Embezzled $53 million in public funds over 22 years
Rita Crundwell

Crundwell opened a bank account named Reserve Sewer Development Account (RSCDA). She was the only signer.

She caused money to be deposited into an account called the Capital Development Fund, created fake invoices, and then wrote checks from the fund payable to "Treasurer", which she would deposit into the RSCDA account.
Rita Crundwell

Used the money to breed horses; had a $400K RV. No one found that curious?
Rita Crundwell

Sentence: 17 years
Crundwell told the mayor and City Council that the state was late in its payments to Dixon.
Separation of Duties: Embezzlement via Bogus Vendors
Embezzlement via "shell" vendors

Anita Collins, 67, Charged With Stealing $1 Million From NY Archdiocese
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 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.
Texas Case: A Small Company

Company was so small that it used hand-written checks

Trusted bookkeeper of 13 years embezzled $2.4 million over 6 years
…did the accounting, entered payables into Quickbooks, paid bills, wrote & signed checks, reconciled the account.

Every week for 6 years she would enter bogus invoices into computer, and pay those invoice numbers.

Vendor payments were entered into computer and invoice numbers written on check stubs.  BUT…
Trusted Bookkeeper

The checks were made payable to bogus account numbers and deposited via teller into her personal account that had a different account number.

(Payee and bank account deposited into did not match.)
Company sued the bank.
Who won the lawsuit?
The Bank!
How?
Why?

UCC: One-Year Statute of Limitations!

After one year, a bank has NO LIABILITY even if the bank was negligent in the transaction
Embezzlement via Diverted Deposits
Santa Monica, CA

Big Blue Bus
Santa Monica, CA

Big Blue Bus
County of Los Angeles mailed

$1,075,000 check

to Santa Monica for Big Blue Bus

(Federal Transportation Money)
Actual Big Blue Bus Check
Big Blue Bus

- Check was stolen
- Deposited into brokerage account in Colorado
- Account opened with fake ID
- Securities were purchased, then sold.
- ALL the money was wired out, gone!
- Money not identified as missing for 6 months!
Big Blue Bus

Check was NOT Altered

The Endorsement was forged

Forged endorsements are the liability of the bank of first deposit for 3 years
Brokerage Legal Strategy

Brokerage was willing to spend $200K in legal fees to uncover anything that will shift liability

**Discovery:** Nigerian temporary employee worked in Accounting Dept. Employed for 18 months; during that time 5 checks were stolen
Big Blue Bus

Federal Transportation money

FBI, Secret Service involved

Nigerian temp quit when FBI began interviews…but his picture was in FBI files
Big Blue Bus

$1,075,000 traced to Texas

Sam Roberts, naturalized Nigerian citizen. Application: Failed to include prison time in North Carolina for check fraud

Part of $20,000,000 scheme

Arrested by Houston Postal Inspector
$800,000 spent on legal fees before the case was settled!
Prevent Embezzlement by Diverted Deposits:

Have ALL checks mailed to your Bank’s Lockbox
Companies/Municipalities: Use your bank’s Lockbox Service

**Cost:** $6/day + $0.35 / item

Lockbox completely eliminates the risk of diverted deposits.

You cannot hire someone that inexpensively!
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
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 the person who handles money.
Surprise Audits

- 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 employee’s computer. Searching the employee’s computer is tampering with evidence.

Make a “mirror” of the hard drive and search the mirror.
If you suspect an employee is embezzling:

Create a team
Bring in outside help
Keep notes
Review records
Contain damage
Find witnesses
Fix internal controls
Report crime

Praise honesty
ADDITIONAL SOLUTIONS
Employee Awareness Education

Employees are an organization’s best detection source. Educate them about what constitutes fraud, how it hurts everyone, and how to report it.

Embezzlement Prevention Tools and Strategies
Embezzlement Prevention Tools and Strategies

Anonymous Tips are the #1 means to detect embezzlement.

A “Tip Hotline” is the most effective tool to detect embezzlement; should be accessible by:

1. Employees
2. Vendors
3. Customers
4. Outsiders
Embezzlement Prevention Tools and Strategies

Set up employee support programs to help those struggling with addiction, mental/emotional issues, financial problems, etc.
<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; Timely Reconciliation; 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; <strong>Separation of Duties</strong>; <strong>Surprise audits</strong></td>
</tr>
</tbody>
</table>
## Schemes & Solutions

| Deposit Fraud | Control Incoming Receipts!  
| Open mail in dual custody,  
| Use Bank’s lockbox service,  
| Hire your CPA to audit A/R for credit memos |
|---|---|
| Sale is recorded on Company books, but money is stolen, and deposits are diverted.  
Invoice in A/R is offset with a Credit Memo; account is not delinquent |
## Anti-Fraud Controls

### Median Loss and Duration of Schemes – Based on Presence of Anti-Fraud Controls

<table>
<thead>
<tr>
<th>Anti-Fraud Control</th>
<th>Loss with Control</th>
<th>Loss without Control</th>
<th>Duration with Control</th>
<th>Duration without Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Review</td>
<td>$100,000</td>
<td>$185,000</td>
<td>14 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Hotline</td>
<td>$100,000</td>
<td>$180,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Employee Support Programs</td>
<td>$100,000</td>
<td>$180,000</td>
<td>16 months</td>
<td>21 months</td>
</tr>
<tr>
<td>External Audit of ICOFR</td>
<td>$120,000</td>
<td>$187,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Fraud Training for Managers/Executives</td>
<td>$100,000</td>
<td>$158,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Internal Audit/FE Department</td>
<td>$120,000</td>
<td>$180,000</td>
<td>13 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Fraud Training for Employees</td>
<td>$100,000</td>
<td>$155,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Job Rotation/Mandatory Vacation</td>
<td>$100,000</td>
<td>$150,000</td>
<td>9 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Surprise Audits</td>
<td>$100,000</td>
<td>$150,000</td>
<td>10 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Anti-Fraud Policy</td>
<td>$100,000</td>
<td>$150,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Formal Fraud Risk Assessments</td>
<td>$100,000</td>
<td>$150,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Rewards for Whistleblowers</td>
<td>$100,000</td>
<td>$145,000</td>
<td>9 months</td>
<td>22 months</td>
</tr>
<tr>
<td>Code of Conduct</td>
<td>$120,000</td>
<td>$164,000</td>
<td>14 months</td>
<td>30 months</td>
</tr>
<tr>
<td>Independent Audit Committee</td>
<td>$125,000</td>
<td>$150,000</td>
<td>13 months</td>
<td>24 months</td>
</tr>
<tr>
<td>Management Certification of F/S</td>
<td>$138,000</td>
<td>$164,000</td>
<td>12 months</td>
<td>24 months</td>
</tr>
<tr>
<td>External Audit of F/S</td>
<td>$140,000</td>
<td>$145,000</td>
<td>17 months</td>
<td>24 months</td>
</tr>
</tbody>
</table>
Embezzlement Prevention Checklist

The most cost-effective way to limit fraud losses is to prevent fraud from occurring. This checklist will help organizations test the effectiveness of their fraud prevention program.

1. Is ongoing anti-fraud training provided to all employees of the organization?
2. Is an effective fraud reporting mechanism (tip hotline) in place?
3. Is the management climate/tone at the top one of honesty and integrity?
4. Are fraud risk assessments performed to identify and mitigate the company’s vulnerabilities to internal and external fraud?
5. Are strong anti-fraud controls in place and operating effectively?
6. Does the internal audit department have adequate resources and authority to operate effectively and without undue influence from senior management?
7. Does the hiring policy include thorough fraud prevention controls?
8. Are employee support programs in place to assist employees struggling with addictions, mental/emotional health, family or financial problems?
9. Are employees allowed to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?
What NOT to do

Don’t jump to conclusions
Don’t conduct group interviews
NEVER interview an employee by yourself
Don’t rush to confront
Never interfere with law enforcement
“Employee embezzlement schemes are often the product of an absence of proper internal controls or a breakdown of those controls. Regular audits and control testing can help to mitigate exposure.”

Steven J. Durham, Former Chief of the Fraud and Public Corruption Section United States Attorney’s Office, Washington D.C.
Mobile Banking Fraud
Mobile Banking Fraud – the newest twist on check fraud
A report on banking fraud released by American Bankers Association highlights the impact mobile banking fraud is having on institutions of all sizes, with 100% of the largest financial institutions reporting RDC fraud & a 400% growth in losses reported over two years across financial institutions of all sizes.
A report on banking fraud released by American Bankers Association highlights the impact mobile banking fraud is having on institutions of all sizes, with 100% of the largest financial institutions reporting RDC fraud & a 400% growth in losses reported over two years across financial institutions of all sizes.
Mobile Banking Fraud:

Double Deposits
Recent example of Double Deposits
Deposited via smart phone on 11-25-16

Heat-sensitive ink icons visible

Visible laid lines
Same check deposited later at a bank

Heat-sensitive ink icons NOT visible

Laid lines dropped out

Deposited later at a bank....
Mobile Banking Deposit Fraud

Scenario: A check is mailed to Dishonest Don

- Don uses a smart phone app to deposit check
  - Takes pix of front of check
  - Endorses the back of a different check
  - Uploads check; is pays at drawer’s bank

- 3 days later, Don cashes the same check at a check cashing store

✓ 2\textsuperscript{nd} 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 AND The Uniform Commercial Code (UCC): Holder In Due Course
The answer is found in the Rules governing Check 21 AND the Uniform Commercial Code (UCC): Holder In Due Course.
Mobile Banking & Check 21

1. Mobile depositing 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 (including mRDC)

4. The Rules determine who takes the loss
Check 21 Rules

Two Warranties:

✓ Image of check is clean; everything is legible; substitute check is properly created

✓ Check is presented for payment only one time; no double presentments.

The Fed did not envision Remote Deposit Capture desktop scanners or mobile banking smart phone apps in 2004!
§ 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.
Bank of First Deposit (BOFD) can charge the loss against its customer’s account.

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

A Breach of Warranty claim can be filed within 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 applies.
Actual Breach of Warranty Claim

Greg Litster

From: [redacted]@ca.us>
Sent: Wednesday, February 7, 2018 3:08 PM
To: [redacted]@com
Cc: [redacted]@safechecks.com; [redacted]@cityofspokane.org
Subject: Returned Check Notice Dated 12/7/17

Dear Ms. [redacted],

The purpose of this message is to update you on the status of this outstanding payment.

Upon receipt of your letter dated December 7, 2017 (copy attached), the City’s banking institution ([redacted] Bank) filed a Check 21 Breach of Warranty Claim against the Bank of First Deposit (Bank of America). Today, I received confirmation that Bank of America has agreed to honor the claim and reimbursement in full for the check amount and returned check charge will be credited to the City’s checking account.

Upon receipt of the funds, a check will be issued and mailed to [redacted].

Should you have any questions, please don’t hesitate to contact me at [redacted].

Sincerely,

[redacted]
Chief Deputy City Treasurer
Subject: Re: UNRESOLVED: Check 21 Breach of Warranty Claim - City of

Thank you for the update. I will look for the $30.00 credit and will contact the check cashing store to let them know that reimbursement for the $125.00 check and $30.00 returned check charge are forthcoming.

Sent from my iPhone

On Feb 7, 2018, at 10:42 AM, bank.com wrote:

Hi [Name] and [Name],

According to our back office, a Breach of Warranty claim was submitted to Bank of America on January 12, 2018. The claim was honored and Bank of America’s recourse will be to seek reimbursement from their customer, and we have credited $30 to City as well.

Thank you,
Loose Ends...

Multiple Payee Names on checks

&

ACH Filters and Blocks
Multiple Payee Names

If **Multiple** Payee Names on a check do not include the word “**and**” after the names—

the Payee is “ambiguous” and **legally** means

“**OR**”

A forward slash [virgule, vər-gyʊl “/” ] = **OR**
**ACH Filters and Blocks**

Prevent **unauthorized** ACH debits from paying against your bank account.

An unauthorized ACH debit **MUST** be returned within 24 hours after it posts or it **CANNOT BE RETURNED**!

**ACH Filters and Blocks are available through your Bank**
PROTECTION

PASSWORD

PROTECTION
FBI: 10 Most Popular 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
Cracking Passwords
8 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>

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

Today: 8 Characters, all lower case = 12 hours
Today: **12 Hours**!

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

This $12,000 computer containing 8 AMD Radeon GPU cards can brute force the entire keyboard for any eight-character password in 12 hours!
The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

Bill Burr’s 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error.
The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

Bill Burr’s 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error.

By Robert McMillan
Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.
New Recommendations:

Use LONG Passwords

correcthorsebatterystaple (25 characters)
correct horse battery staple

Isolemnlyswearthatiamuptonogood (31 characters)
I solemnly swear that i am up to no good

Repeat after me: Dad is always right (30 characters)
Repeat after me: Dad is always right
Check Fraud
Check Fraud

Why talk about Check Fraud?
Check Fraud

Produces more $ Losses

than all other types of payment fraud!
The *FIRST* Check Fraud Lawsuit in 1762

Price sued Neal for check fraud

Price v. Neal, England
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.”
The jury found a verdict for the Plaintiff; and assessed damages of 80£ and costs 40s. (Bank had NO liability... even in 1762!)
Check fraud has continued unabated for 250 years!

(but with few public hangings)
“Checks remain the most-often targeted payment method by those committing fraud attacks.

Check fraud also accounts for the largest dollar amount of financial loss due to fraud.”
Association for Financial Professionals

Payments Fraud Survey

50% of large organizations
(plus millions of smaller companies)
still issue checks

Check fraud is not going away!
Fraudulent Payment Attempts (by Method)
(Respondents were hit multiple ways-- total > 100%)

- CHECKS: 75%
- Wire Transfers: 46%
- Corporate Cards: 32%
- ACH Debits: 30%
- ACH Credits: 11%
Fraud LOSSES (by Method)
(How Dollars were actually lost)

- CHECKS: 43%
- Wire Transfers: 23%
- Corporate Cards: 20%
- ACH Debits: 10%
- ACH Credits: 5%
Frank Abagnale

*Catch Me If You Can*

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

and

Holder in Due Course
Quick Quiz

True or False?
1) Placing a Stop Payment on a check ends your legal responsibility to pay the check.
FALSE

Holder in due course trumps Stop Payments
2) Positive Pay will catch all check fraud attempts.
FALSE

Pos Pay won’t catch Altered Payee Names or counterfeit checks using the same check number
1) Placing a Stop Payment on a check ends your legal responsibility to pay the check.

2) Positive Pay will catch all check fraud attempts, including added payee names.

3) **Payee** Positive Pay will catch **all** check fraud attempts including **added** payee names.

QUIZ: True or False?
FALSE

Won’t catch ADDED Payee Names placed two (2) lines above the original payee name
1) Placing a Stop Payment on a check ends your legal responsibility to pay the check.

2) Positive Pay will catch all check fraud attempts.

3) Payee Positive Pay will catch all check fraud attempts, including altered/added payee names.

4) If you’re using Payee Positive Pay the quality of your check stock doesn't matter.
If the counterfeit checks looks “genuine” you can be held liable for the check under Holder in due course (See Triffin v. Somerset Valley Bank and Hauser Contracting Co.)
HOLDER IN DUE COURSE

Holder in Due Course, a powerful part of the Uniform Commercial Code, can adversely impact an organization’s liability for check fraud, including those checks on which a “stop payment” has been placed.

Who or what is a Holder in Due Course? A Holder in Due Course (HIDC) is anyone who accepts a check for payment, and on the face of the check there is no evidence of alteration or forgery, nor does the recipient have knowledge of any fraud related to the check.

Under these conditions, the recipient is an HIDC and is entitled to be paid for the check. The statute of limitations under the UCC for an HIDC to sue the check’s maker for its full face value is 10 years from the issue date, or three years from the date the check was deposited and returned unpaid, whichever comes first.

Frequency of HIDC Claims

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

Actions Taken in Response to Holder in Due Course Claims

- Paid Full Value of Check or More: 53%
- Did Not Pay: 47%
- Still in Dispute: 27%
- Other: 7%

ROBERT J. TRIFFIN v. CIGNA INSURANCE

Placing A Stop Payment Does Not End Your Obligation To Pay A Check

In July 1993, Cigna Insurance issued James Mills a Workers’ Compensation check for $484. Mills falsely claimed he did not receive it due to an address change, and requested a replacement. Cigna placed a stop payment on the initial check and issued a new check, which Mills received and cashed. Later, Mills cashed the first check at Sun’s Market (Sun). Sun presented the check for payment through its bank.

Cigna’s bank dishonored the first check, stamped it “Stop Payment,” and returned the check to Sun’s bank, who charged it back against Sun’s account. Sun was a Holder in Due Course, and if Sun had filed an HIDC claim against Cigna as the issuer of the check, it would have been entitled to be paid. Apparently, Sun did not know about HIDC, because it merely pinned the check on a bulletin board in the store, where the check stayed for two years.

Robert Triffin bought the check from Sun, assumed its HIDC rights, and filed the lawsuit in August 1995, over two years after the check was returned unpaid (statute of limitations is three years). The Court ruled in favor of Robert Triffin, and ordered Cigna to pay him $484, plus interest.

Recommendation: Allow a check to “expire” before replacing it, or you may be held liable for both checks. A party that accepts an expired check has no legal standing to sue as a Holder in Due Course if the check is returned unpaid.

Print an expiration statement on the check face such as, “THIS CHECK EXPIRES AND IS VOID 30 DAYS FROM ISSUE DATE.” If a check is lost, wait 30 + 2 days from the initial issue date before reissuing. Many companies print “VOID AFTER 90 DAYS” but cannot reasonably wait that long before re-issuing a check.

Superior Court of New Jersey, Appellate Division, A-169-00T5 lawlibrary.rutgers.edu/courts/appellate/a4000-95 opin.html

An analysis of court cases can be downloaded from www.safechecks.com.
Click on Fraud Prevention Tips, then Holder in Due Course.
ROBERT J. TRIFFIN v. SOMERSET VALLEY BANK AND HAUSER CONTRACTING CO.
You May Be Held Liable For Checks You Did Not Issue or Authorize

Hauser Contracting Co. used ADP for payroll services. A thief obtained check stock that looked identical to ADP’s checks and created 80 counterfeit paychecks totaling nearly $250,000 that were identical to the ADP checks used by Hauser Contracting Co.

A retailer who knew Mr. Hauser became suspicious and called him. Somerset Valley Bank also called, Mr. Hauser reviewed the in-clearing checks, which looked just like his, and confirmed the checks were unauthorized and the payees were not his employees. The bank returned the checks marked as “Stop Check - Do Not Present Again.”

Robert Triffin bought 18 of these checks totaling $8800 from four check cashing agencies, claimed HDC status, and wasted Mr. Hauser and his bank for negligence for not safeguarding the payroll checks.

ROBERT J. TRIFFIN v. POMERANTZ STAFFING SERVICES, LLC
High Security Checks May Protect You From Some Holder in Due Course Claims

Pomerantz Staffing Services used high security checks that included high security features. They used high security features but without the thermo ink on the back. They cashed 18 checks totaling $7000 at Friendly Check Cashing Company. Friendly’s cashiers failed to heed the warning on the check face, and did not look for the thermo ink on the back. All 18 checks were returned unpaid, likely caught by Positive Pay.

Robert Triffin bought the checks, claimed HDC status, and sued Pomerantz. Pomerantz countersued and won! The judge correctly asserted that if Friendly had looked for the thermo ink as instructed, they could have determined the checks were counterfeit. Because they were provided a means to verify authenticity and failed to do so, they were not an HDC and had no rights to transfer to Mr. Triffin.

This case illustrates the value of check security features, specificity warned by banks, and a controlled check stock. Pomerantz was protected by its checks.

CHECK FRAUD SCAM — IT CAN HAPPEN TO ANYONE
Greenberg, Trager & Herbst, LLP v. HSBC Bank, USA 17 N.Y.3d 565 (2011)

In a landmark decision, the New York Court of Appeals upheld that the depositor of a counterfeit check is responsible for risk of loss “until the settlement becomes final.” Statements concerning “clearing” of a check and funds availability are irrelevant.

A New York City law firm (Greenberg) received an email requesting legal services from a potential client in Hong Kong. As part of the transaction, the client requested that the law firm accept a check for $197,750, direct $10,000 for its fee, and wire the balance to another firm in Hong Kong. (This should have been the first clue that this was a scam.) The law firm deposited the check, which appeared to be drawn on a Citibank account, into its account at HSBC Bank.

The next business day, HSBC provisionally credited the firm for $197,750, per federal funds availability regulations. A day later, the law firm called HSBC, asking if the check had “cleared” the account. Being told that it had, the firm wired $197,750 to the other firm in Hong Kong as instructed. The check ultimately proved to be counterfeit, and HSBC charged back $197,750 to the Greenberg account.

Greenberg sued Citibank for “failing to discover that the check was counterfeit” and sued HSBC for “negligent misrepresentation” for stating that the check had cleared when in fact it had been returned to HSBC, re-routed to a different Citibank processing center, and then returned again as counterfeit to HSBC.

The New York Supreme Court issued summary judgment for both banks and dismissed all of Greenberg’s claims. Upon appeal, the Court of Appeals upheld the first court’s decision. Citing the Uniform Commercial Code, Citibank had no obligation to detect fraud for Greenberg because Greenberg was not Citibank’s client. Its only obligation was to pay the check, return it, or send written notice and that it had been dishonored. It had returned the check within the prescribed deadline.

Both claims against HSBC were also dismissed. The bank’s contract specifically stated that clients may not pursue claims based on a bank employee’s oral representations. The Court also held that the term “if check has cleared” is ambiguous and not definitive that final settlement had occurred.

Furthermore, the Court rejected Greenberg’s argument that both banks should have had procedures in place that would have prevented the fraud. The Court said that the law firm itself was in the best position to prevent fraud, and had a responsibility to know its client.

This scam was a text-book case of a legal firm accepting a check for more than the amount due and then wire fraud. Visit www.safechecks.com for additional fraud prevention tips.
ROBERT J. TRIFFIN v. SOMERSET VALLEY BANK AND HAUSER CONTRACTING CO.

You May Be Held Liable For Checks You Did Not Issue or Authorize

Hauser Contracting Co. used ADP for payroll services. A thief obtained check stock that looked identical to ADP’s checks and created 80 counterfeit payroll checks totaling nearly $25,000 that were identical to the ADP checks used by Hauser Contracting Co.

A retailer who knew Mr. Hauser became suspicious and called him. Somerset Valley Bank also called. Mr. Hauser reviewed the in-clearing checks, which looked just like his, and confirmed the checks were unauthorized and the payees were not his employees. The bank returned the checks marked as “Stolen Check - Do Not Present Again.”

Robert Triffin bought 18 of these checks totalling $8800 from four check casing agencies, claimed HIDC status, and sued both Mr. Hauser and his bank for negligence for not safeguarding the payroll checks and facsimile stamp. Because the counterfeit and authentic checks looked identical, the lower court ruled for Triffin. Hauser appealed, but the Federal Appellate Court upheld the lower court. The Court said the counterfeit check met the definition of a negotiable instrument, and because the check and signature were identical to an authentic check, the check casing agency could not have known it was not authentic.

**Recommendation: Use a controlled check stock**, which means using checks that are uniquely designed or customized for your organization and are not available blank to others. **SAFEChecks** and the **SuperBusinessCheck** are controlled check stocks.

Superior Court of New Jersey, Appellate Division, A-163-00T5
lawlibrary.rutgers.edu/courts/appellate/a0163-00.opn.html
5) In a Check 21 world, check security features don’t matter if you’re using Payee Positive Pay.
FALSE

Holder in due course trumps Payee Pos Pay
QUIZ: True or False?

6) Your payables are processed by a third party (your bank) that uses Payee Positive Pay. The quality of the check stock they use doesn't matter to you because if there's loss, they'll take the hit.
Depends
on what the contract says.
If it is silent, you have liability.
5) In a Check 21 world, check security features don't matter if you're using Payee Positive Pay.

6) Your payables are processed by a third party (your bank) that uses Payee Positive Pay. The quality of the check stock they use doesn't matter to you. If there's fraud loss, they'll take the hit.

7) If you have a great relationship with your bank, you’ll never be held liable for a check fraud loss.

QUIZ: True or False?
HA!

Cincinnati Insurance Co. vs. Wachovia Bank
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.

ORDER

Case No. 08-CV-2734 (PJS/JJG)
CINCINNATI INSURANCE COMPANY v. WACHOVIA BANK

Wachovia Bank Wins Lawsuit Over Customer That Refused Positive Pay

Schultz Foods Company issued a check for $153,856 to Amerada Hess Corporation. Thieves stole the check out of the mail, changed the name of the payee, and convinced the new bogus payee (an unwitting accomplice) to endorse the check and deposit it into his bank.

His bank presented the check for payment to Schultz Foods’ bank, Wachovia Bank, and Wachovia charged $153,856 against Schultz Foods’ account. Before Schultz Foods discovered the fraud, the funds had been wired out, and the money disappeared.

When the fraud was discovered, Schultz Foods reported the altered check to Wachovia and demanded its account be re-credited. Wachovia refused, citing that Schultz Foods had been offered the chance to implement “Positive Pay” after three previous check fraud incidents, but had declined. Instead, Shultz Foods had purchased a check fraud insurance policy from Cincinnati Insurance Co. Positive Pay, however, would have prevented this loss.

Schultz Foods made a $153,856 claim under its policy with Cincinnati, who paid the claim and filed suit against Wachovia to recover its loss. Cincinnati contended that the altered check was not “properly payable” and Wachovia was liable for the loss. However, the Wachovia deposit agreement signed by Schultz Foods contained a list of precautions that a customer should take to protect their account. The Agreement included a conditional release of Wachovia’s liability: “You agree that if you fail to implement . . . products or services [that are designed to deter check fraud], . . . you will be precluded from asserting any claims against Wachovia for paying any unauthorized, altered, counterfeit or other fraudulent item . . . .”

Wachovia had not required Schultz Foods to absorb any losses from the prior incidents, even though Schultz Foods never implemented Positive Pay. Cincinnati argued that Schultz Foods “had an expectation that Wachovia would reimburse Schultz Foods’ account” for unauthorized charges if Schultz Foods took precautions such as closing its account. However, that expectation was contrary to Wachovia’s deposit agreement, which contained an anti-waiver provision, allowing it to waive enforcement of the terms of the Agreement.

Even though Wachovia voluntarily shielded Schultz Foods from past check fraud losses, its deposit agreement protected it from liability.

The Court agreed with Wachovia’s argument that the deposit agreement between Wachovia and Schultz Foods required Schultz Foods either to implement Positive Pay or to assume responsibility for any fraud losses caused by its failure to implement Positive Pay.

For the complete court case and commentary, visit www.safechecks.com/articles.
Yesterday’s generation
“I rob banks because that’s where the money is.”

Willie Sutton
Profession: Bank Robber
(1901 - 1980)
“You know, you can do this just as easily online.”
Today’s generation

What once was “old” is NEW
Street Gangs Venture into White-Collar Crime

By JACOB GERSHMAN
Mar 8, 2016 1:19 pm ET
Outlaw Gangsta Crips, Brooklyn, NY
“...Gangs traditionally associated with drugs and violent crimes are increasingly committing financial frauds.

Gangs are getting into crimes like check fraud and identity theft because they are more lucrative, harder to detect, and carry lighter prison sentences....”

Wall Street Journal, March 8, 2016
“We think of gang members being knuckleheads, but these guys are using a sophisticated thought process and getting involved in stuff that requires technology and an understanding of the banking system.”

Wall Street Journal, March 8, 2016
When federal agents arrested a group of Outlaw Gangsta Crips last summer in Brooklyn, N.Y., the 38-page indictment included robbery, attempted murder and cocaine distribution. But it also included an atypical charge for a street gang case: bank fraud.
“Check fraud has become especially popular...fraudsters are familiar with checks and so are able to commit check fraud with relative ease with the help of sophisticated equipment.”

Wall Street Journal, March 8, 2016
What has changed are the size and scale of the operations. “The sums of money involved are staggering...the potential amount of money involved and damage to people’s financial accounts is greatly out of proportion to other gang crimes....”

Wall Street Journal, March 8, 2016
“Prosecutors said the gang members created and deposited fake checks, and then quickly withdrew money from the accounts before the banks could identify the checks as fake.

The alleged scheme reaped more than $500,000 for the group....”

Wall Street Journal, March 8, 2016
Twelve members of a group known as the Van Dyke Money Gang were accused last summer of bilking banks out of more than $1.5 million.

Manhattan federal prosecutors say the gang, mostly men in their 20s living in Brooklyn, fraudulently obtained money orders and cashed them at bank accounts along the East Coast.
Strategies to Prevent Check Fraud
Don’t Write Checks!

- Use Commercial Purchase Cards
- Pay electronically (ACH)
But, if you’re going to write checks...
Use High Security Checks
Strategies to Prevent Check Fraud

1. High Security Checks
2. Positive Pay
3. Payee Positive Pay
4. ACH Filters or Blocks
Effective check fraud prevention strategies begin with a high security check.
Which security features matter most?
1. Controlled check stock
Controlled check stock are checks that are not sold entirely blank unless the face has been customized for that company.
Uncontrolled check stock
Uncontrolled check stock are checks that are sold entirely blank, or are sold indiscriminately to whomever orders them, without being authenticated or verified.
How is Uncontrolled Check Stock a problem?
Fraudsters Create Counterfeit Checks

Fraudsters use:

1. Adobe Illustrator
2. Scanner
3. Buy ORIGINAL blank check stock (uncontrolled) to create authentic-looking counterfeit checks—including Cashiers Checks and Official Checks.
Who Sells Blank, Uncontrolled Checks?

- Virtually ALL accounting software & check writing software vendors
Who Sells Blank, Uncontrolled Checks?

- Virtually ALL check printers, including:
  1. Large, national check printers
  2. Small print brokers buying from wholesalers
I bought high-security checks from

XXXXX (Major National Check Printer)
I bought high-security checks from XXXXX...

...using a bogus name and

...a **closed** account number!
ATTN: R GREGORY LITSTER
ATTN GREG LITSTER
ABAGNALE ADVISOR
8934 ETON AVE
THIS ACCT WAS CLOSED IN 2013
Uncontrolled Checks
Uncontrolled Checks

<table>
<thead>
<tr>
<th>QUANTITY</th>
<th>50</th>
<th>250</th>
<th>500</th>
<th>1000</th>
<th>2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSLT104-3 Parts/TriPLICATE</td>
<td>$125.99</td>
<td>$288.99</td>
<td>$416.99</td>
<td>$663.99</td>
<td>$1,143.99</td>
</tr>
</tbody>
</table>

We recommend this quantity.

1. Quantity: 500
2. Part: Select

Customize Now »

Add Matching Companion Envelopes
Save time and money with these perfectly matched envelopes. See shopping cart for product details and pricing.
THIS ACCT WAS CLOSED IN 2013
I used this **CLOSED** Account Number
Check Printer **did not verify** Bogus Name / Closed Account # / Address
Fraudsters use **ACTIVE** Account Numbers
Fraudsters ADD a Name & Logo
You Gotta Be Kidding Me! Productions, LLC
1075 Diplomatic Drive
Abuja, Nigeria

PAY TO THE ORDER OF

Address of the US Embassy in Nigeria

Bogus Name printed on after the blank checks were received

MEMO
I used this **closed** account number...
And a BOGUS Name; Intuit did not verify!
I used this **closed** account number...
And a BOGUS Name; Costco did not verify!
You've Got To Be Kidding Me! LLC
Operating Account
P.O. Box 981
Simi Valley, CA 93063-0981

PAY TO THE ORDER OF

$-

Dollars

MEMO

THIS CHECK IS NON-NEGOTIABLE

Authorized Signature

You've Got To Be Kidding Me! LLC
You’ve Got To Be Kidding Me! LLC
Operating Account
P.O. Box 981
Simi Valley, CA 93063-0981

PAY
TO THE
ORDER OF

MEMO
In contrast with other check printers...

SAFEChecks does not sell checks entirely blank unless the face of the check has been uniquely designed and customized for that customer or end user.

For customers that use entirely blank checks we can print the company’s website along the edge, or a customized logo on the face, or something that is unique to that customer.
SAFEChecks pays its employees $100 if they catch an unauthorized person trying to buy checks using someone else's account number.
Every new check order is verified with the bank.

SAFEChecks has **never** had a check replicated or used in a scam in over 20 years.
Additional Security Features

1. **Controlled** check stock.
   Dual-tone True watermark
   Thermochromatic ink
   Correctly worded warning banners
   Toner anchorage
   Copy void pantograph
   Chemical sensitivity
   Chemical wash detection box
   Inventory control numbers
Positive Pay
Legal Reasons to use Positive Pay
Cincinnati Insurance v. Wachovia Bank

Wachovia Bank Wins Lawsuit Over Customer That Refused Positive Pay
The Legal Rational to Implement Positive Pay and High Security Checks

Frank W. Abagnale
Abagnale & Associates
(800) 237-7443

Greg Litster
SAFEChecks
(800) 755-2265
greg@safечecks.com

In what may well become a precedent-setting case, Wachovia Bank won a lawsuit against a customer’s insurance company after the customer failed to implement Positive Pay and later suffered a $153,856.46 check fraud loss. The bank had repeatedly recommended that the customer use Positive Pay, but the customer declined.

Background

In late 2005, Todd’s Snax, Inc., dba Schultz Foods Company (“Schultz Foods”), issued a check in the amount of $153,856.46 to Amerada Hess Corporation drawn on Wachovia Bank. Thieves stole the check out of the mail, changed the name of the payee to “Kenneth Payton,” and induced Payton (an unwitting accomplice) to endorse the check and deposit it into his account at TCF Bank. Payton was a minister who had been beguiled by the fraudsters into believing he was helping with an urgent humanitarian need in Singapore, demonstrating that no good deed goes unpunished.
Commercial Customer Who Rejects Positive-Pay Bears Risk of Resulting Check Fraud Loss (Posted September 2010)

In a recent decision from Minnesota, a company that had been offered a positive-pay product by its bank but rejected the offer was liable when the bank later paid a big check that had an altered payee that would have been caught by a positive-pay fraud filter. The bank won the case because of language contained in its deposit agreement.

The Minnesota case. In Cincinnati Ins. Co. v. Wachovia Bank, N.A., 2010 WL 2777478 (D. Minn. 7/14/10), Schultz Foods maintained a commercial checking account with Wachovia (now Wells Fargo). Over the course of this relationship, Schultz Foods was the victim of check fraud four times. On the first three occasions, Schultz Foods closed the compromised account and opened a new account, and Wachovia absorbed the loss. In 2005, Schultz Foods issued a check in the amount of $153,856.46 to Amerada Hess Corporation. The check was stolen before it reached the intended payee. In a classic "washing" scheme, the thieves removed the name of the intended payee and substituted the name of Kenneth Payton, who was an unwitting accomplice of the thieves. Payton indorsed the check and deposited it into his account at TCF Bank. The altered check was then presented to Wachovia and paid.
A Pennsylvania judge's ruling in a recent check-fraud case could wind up coercing more small businesses into buying anti-fraud protection services from their banks.

The case was Schultz Foods Co. vs. Wachovia Corp., which stemmed from Wachovia's decision in 2005 not to cover a nearly $154,000 loss Schultz incurred due to check fraud. After Wachovia covered its losses on three previous occasions, Schultz assumed Wachovia would have its back after a fourth time. But Wachovia balked, triggering the lawsuit.

In August, a federal court sided with Wachovia and threw out the case, largely due to a specially crafted deposit agreement from Wachovia that required Schultz to pay for certain anti-fraud services in order to be covered for losses.

U.S. District Judge Patrick Schiltz ruled that Wachovia had "reasonable" cause for the stipulation because of three prior fraud incidents. Still, Schultz had refused the fee-based "positive pay" service, which could have alerted Wachovia to the stolen check by cross-matching it for possible alterations against a master list of issued checks.
A Pennsylvania judge’s ruling in a recent check-fraud case could wind up coercing more small businesses into buying anti-fraud protection services from their banks.

The case was Schultz Foods Co. vs. Wachovia Corp., which stemmed from Wachovia’s decision in 2005 not to cover a nearly $154,000 loss Schultz incurred due to check fraud. After Wachovia covered its losses on three previous occasions, Schultz assumed Wachovia would have its back after a fourth time. But Wachovia balked, triggering the lawsuit.

In August, a federal court sided with Wachovia and threw out the case, largely due to a specially crafted deposit agreement from Wachovia that required Schultz to pay for certain anti-fraud services in order to be covered for losses.

U.S. District Judge Patrick Schultz ruled that Wachovia had "reasonable" cause for the stipulation because of three prior fraud incidents. Still, Schultz had refused the fee-based "positive pay" service, which could have alerted Wachovia to the stolen check by cross-matching it for possible alterations against a master list of issued checks.
A Pennsylvania judge's ruling in a recent check-fraud case could wind up coercing more small businesses into buying anti-fraud protection services from their banks.

The case was Schultz Foods Co. vs. Wachovia Corp., which stemmed from Wachovia's decision in 2005 not to cover a nearly $154,000 loss Schultz incurred due to check fraud. After Wachovia covered its losses on three previous occasions, Schultz assumed Wachovia would have its back after a fourth time. But Wachovia balked, triggering the lawsuit.

In August, a federal court sided with Wachovia and threw out the case, largely due to a specially crafted deposit agreement from Wachovia that required Schultz to pay for certain anti-fraud services in order to be covered for losses.

U.S. District Judge Patrick Schultz ruled that Wachovia had "reasonable" cause for the stipulation because of three prior fraud incidents. Still, Schultz had refused the fee-based "positive pay" service, which could have alerted Wachovia to the stolen check by cross-matching it for possible alterations against a master list of issued checks.

The case even attracted the attention of Frank Abagnale, the famed 1960s fraudster-turned-security consultant. "Based upon this lawsuit, banks will almost certainly be reviewing and re-writing their deposit agreements to include the kinds of provisions Wachovia Bank included," Abagnale wrote in a shared memo with SAFEChecks CEO Greg Litster.
Positive Pay provides

No Protection Against

1. Altered Payee Names
2. Added Payee Names
3. Counterfeit Checks using identical check number and dollar amount
Payee Positive Pay
Payee Positive Pay will catch Altered Payee Names
Payee Positive Pay provides

No Protection Against

• **Added Payee Names** printed 2 lines above the original payee name
Payee Positive Pay provides **No Protection Against**

- **Added Payee Names** are printed 2 lines above the original payee name

**Banks** have **NO solution** for checks with a bogus name printed 2 lines above the original payee name
The “Solution” is a Secure Name Font
Typical Check Layout

Open Areas Where Forgers Add A New Payee Name
This is the IDENTICAL check-issue data after being printed using special software.
Secure Name Font
printed TWO LINES above original payee name
Secure Name Font
printed TWO LINES above original payee name

The Secure Name Font is created by special software
Leaves No Room for Adding Bogus Payee
Secure Name & Number Fonts are created by special software.

The software interfaces with your computer. When printing checks, the check issue data passes through the software and the checks print out on your laser printer with the Secure Name and Number fonts on the check.
Secure NUMBER font blocks out area to prevent an Added Payee Name
Deterrence: Add **WARNINGS** to the Check
Deterrence: Add **WARNINGS** to the Check
Encrypted barcode

The Encrypted Barcode is created by special software.
Helps deter fraudsters and embezzlers
Encrypted 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 (deters embezzlement)
The Secure Name Font, Barcode, and a Positive Pay file to send to the bank is created by the special software.
The Secure Name Font, Barcode, and a Positive Pay file to send to the bank is created by the special software.

Requires **NO** Technical Skills to create a Positive Pay file.
The special software can:

1. **Accumulate** check data for Positive Pay
2. **Change Font size to 14 pt & ALL CAPS**
3. **Add Barcode, Secure Name & Number** fonts
4. **Be configured to send Pos Pay files to the bank automatically**
5. **Reposition** where the check actually prints
Typical Check Layout –
Check is on top and shows thru window envelope

Special Software can reposition the check
Typical Check Layout –
Check is on top and shows thru window envelope

Special Software can Reposition the Check

Special software can repposition check placement
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.
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 issue date
  - 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

HIDC & Stop Payments

Robert Triffin v. Cigna Insurance

- Two year old check; payment stopped
- No “expiration date” printed on check
- 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 (a check) has no legal standing as a holder in due course.
Robert Triffin v. Somerset Valley Bank and Hauser Contracting Company

- 80 counterfeit checks totaling $25,000 on authentic-looking ADP check stock
- Bank returned the checks as counterfeits

**HIDC & Controlled Check Stock**

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

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

HIDC & Controlled Check Stock

- Lower court ruled 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

HIDC & Controlled Check Stock

Robert Triffin v. Pomerantz Staffing Services

• 18 counterfeit checks drawn on Pomerantz’ acct cashed at check cashing store. Every check under $400

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html
HIDC & Controlled Check Stock

Robert Triffin v. Pomerantz Staffing Services

• Each check had a warning printed on the face: “THE BACK OF THIS CHECK HAS HEAT SENSITIVE INK. RUB TO CONFIRM AUTHENTICITY”

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html
HIDC & Controlled Check Stock

Robert Triffin v. Pomerantz Staffing Services

• Check cashier cashed the checks, did not examine the back of the checks
Counterfeit checks looked authentic on face, but DID NOT HAVE heat-sensitive ink on the back

- Because cashier did not verify heat-sensitive ink on the back, it could not claim Holder in Due Course status

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html
HIDC & Controlled Check Stock

Robert Triffin v. Pomerantzn Staffing Services...

- Triffin LOST because the security feature was absent, and forged signature was not specifically disavowed

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html
HIDC & Controlled Check Stock

Robert Triffin v. Pomerantz Staffing Services...

- Pomerantz’ check security features saved him!

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html
Wire Fraud
Wire Fraud Court Case

Choice Escrow and Land Title

vs.

BancorpSouth Bank
Choice Escrow and Land Title
vs.
BancorpSouth Bank

Important Link

Choice Escrow and Land Title vs. BancorpSouth Bank

March 17, 2010: Bank received an online banking wire transfer request to wire $440,000 from Choice Escrow’s Trust Account

Wire transfer $440K to Republic of Cyprus

Request NOT legitimate – Choice Escrow employee’s computer had been hacked; taken over by fraudsters

Computer Takeover: **NO “Dual Control”**

1. **The wire to Cypress** was initiated using the User ID and password of a Choice Escrow employee.

2. Wire was initiated from IP address registered to Choice.

3. Bank authenticated employee’s computer by detecting the ID secure token device the Bank had installed.

4. 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 until the next day. The money was gone!
Bank: Customer failed to implement Dual Control

- Bank required online banking customers sending wires to utilize “Dual Control”
  (Dual Control  =  2 computers, 2 different logins, 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 Legal Argument against using 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.
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.
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.**
"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 of defendant BancorpSouth Bank.”
John Perri, Finance Manager
SEIU Healthcare, Minnesota
651-294-8162

john.perri@seiuhcmn.org
Greg Litster, President
SAFEChecks
(800) 755-2265
(818) 383-5996 cell
greg@safechecks.com
GLITSTER@aol.com