Low Tech Fraud in a High Tech World:
Embezzlement
eCheck Fraud
Holder in Due Course

Becky Woodard
Treasury Manager
Apex Capital
(800) 511-6022
Becky.Woodard@ApexCapitalCorp.com

Greg Litster
President
SAFEChecks
(800) 755-2265
Greg@SAFEChecks.com
The Apex Capital Story: *It All Started With Four Desks*....

Apex Capital Corp buys freight bills, assists and inspires growth and success in small to medium-sized trucking companies. Apex is the leading full-service factoring company for truckers. Serving world-class customer service since 1995, Apex is a company that makes a difference....
CORE VALUES:

● Do the right thing.
● Make a difference in the lives of truckers.
● Take care of employees and clients.
● Create a work environment that promotes positivity, loyalty, sincerity, teamwork.
● Strive for efficiency and energy.
● Give back to the community.
Apex Capital and Fraud Prevention
Embezzlement
What is Embezzlement?

- Perpetrator takes a company’s money or materials without company consent
- Usually happens little by little; can be all at once
- Can include falsifying records and/or moving funds from account to account
- Often goes undetected for years

Source: Kas Henry, PhD © ALL Rights Reserved by KasHenry Inc.
There are 6 common behavioral red flags found in every internal fraud study by the Association of Certified Fraud Examiners (ACFE) since 2008. Managers, employees and auditors should be educated on these behavioral red flags to spot fraudulent activity.

Ignore these red flags at your peril!
Behavioral Red Flags

- Living beyond one’s means
- Financial difficulties
- Being too close to a vendor/customer
- Control issues, e.g. being unwilling to share duties or take vacations
- Divorce/Family problems
- A “wheeler-dealer” attitude
In 92% of the cases analyzed by the Association of Certified Fraud Examiners (ACFE), the fraudster displayed at least one of these red flags, and in 64% of cases, multiple red flags were observed before the fraud was detected.

Profile of an Embezzler

1. No single set of characteristics

2. Corroborating circumstances and Red Flags
Profile of an Embezzler

3. They must:
   a. Hold a position of confidence within the organization
   b. Be able to recognize an opportunity for theft
   c. Possess the technical skills needed to steal

4. Have the Ability to Rationalize stealing
Front Profile of an Embezzler
Profile of an Embezzler

Primary Position Held:
Finance/Accounting = 68%
Lone Perpetrator = 85%
Conspiracy = 15%
Profile of an Embezzler

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

Do background checks.

DON’T RELY SOLELY on background checks…

THIS IS WHY:
Embezzlement via “shell” vendors

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 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, in amounts under the $2,500 threshold that would have required a supervisor's approval.
Embezzlement: The Fraud Triangle

✓ Three primary components lead to internal fraudulent behavior
✓ Opportunity is the component employees have control over
✓ “Perceived opportunity” reduced by monitoring, surprise audits
Embezzlement: The Fraud Triangle

✓ Three primary components lead to internal fraudulent behavior
✓ Opportunity is the component employees have control over
✓ “Perceived opportunity” reduced by monitoring, surprise audits

Rationalization - Real or Perceived:
Vast majority (95%) are first-time offenders with no criminal past, view themselves as “honest people caught between a rock and hard spot” … temporarily; not as a criminal

Personal
• I am only borrowing the money, I’ll return it next week
• I had no choice, I have to pay the doctor bill
• My employer “owes me” for…

Motivation or pressure to commit the crime can be financial or non financial:
• Inability to pay one’s bills
• Increase sales or other productivity targets
• Drug or gambling addictions
• Status symbol driven
• A frame of mind or ethical character that allows employees to intentionally misappropriate cash or assets and justify their dishonest actions

Possible when employees have access to assets and information that allow them to commit and conceal fraud
• A belief that their activities will not be detected. Opportunity is created by poor internal controls, oversight
• The person is allowed to use or abuse their position of authority and trust
• Preferred approach: “Low and Slow” where detection is delayed and more damage can be done
Accidental Fraudster vs Career Criminal

Accidental Fraudsters
✓ Law-abiding individual who never thought of committing fraud, break the law or harm people
✓ Usually first time offender; and the reason they commit fraud is because of non-sharable problem that can only be solved with money
✓ Rationalize actions aligned with opportunity

Predators
✓ Often start out as an accidental fraudster
✓ Actively look for target organization where they can commit crime
✓ Harder to detect because their fraud schemes are usually better organized

Source: Chegg, Forensic Accounting and Fraud Examination study aids

Source: ACFE, Bill Blend, MSL
Types of Embezzlement

- Billing Fraud: 18%
- Cash On Hand: 15%
- Theft and Larceny: 11%
- Check and Payment Tampering: 10%
- Payroll: 10%
- Skimming: 9%
- Cash Larceny: 9%
### Embezzlement Methods

<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 by check fraud schemes occurred at small companies. 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>

Hiscox Embezzlement Study
Profile of an Embezzler

Studies vary on whether males or females embezzle more often, but **males always cause the greatest losses.**
Profile of an Embezzler

While the majority of embezzlers are in their early 40s, the greatest losses come from people over 60.
Profile of an Embezzler

Median loss caused by regular employees = $50K

Median loss caused by managers = $150K

Median loss in the schemes committed by owner or executive = $850K
Profile of an Embezzler

30% of schemes lasted 5 years
Longest scheme lasted 41 years!
“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.
Separation of Duties:

Embezzlement via **Bogus Vendors**
Texas Case: A Small Company

Company was so small that it used QuickBooks and 3-on-a-page hand-written checks

Trusted bookkeeper embezzled $2,400,000 over 6 years
Dishonest "Trusted Bookkeeper"

Trusted bookkeeper did the accounting, entered payables into QuickBooks, paid the bills, wrote & signed checks, reconciled the account.

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

Bogus vendor payments were entered into the computer and invoice numbers written on the check stubs — BUT…
Dishonest Trusted Bookkeeper

The checks were made payable to *bogus account numbers* and deposited into bookkeeper’s personal account at the bank teller line.

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

UCC: One-Year Statute of Limitations!

After one year, the bank has NO LIABILITY even if the bank was negligent in the transaction.

Caveat - Consumer Protections
15 U.S. Code § 1693g - Consumer liability

(a) Unauthorized electronic fund transfers; limit

Notwithstanding the foregoing, reimbursement need not be made to the consumer for losses the financial institution establishes would not have occurred but for the failure of the consumer to report within sixty (60) days of transmittal of the statement (or in extenuating circumstances such as extended travel or hospitalization, within a reasonable time under the circumstances) any unauthorized electronic fund transfer or account error which appears on the periodic statement provided to the consumer under section 1693d of this title.
Embezzlement via
Unauthorized Payments
Front Profile of an Embezzler
Side Profile of an Embezzler

Robert Rizzo
Former City Manager
Bell, CA
Robert Rizzo

Sentence: 12 years
Rev. Jonathan Wehrle, the founding pastor of St. Martha's Church in Okemos, is accused of stealing $5 million from the church.
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

Sentence: 17 years

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.”
Maria Louisa Mason, 80, a retired state employee, has been charged with embezzling $73,000 in public money intended to build a memorial statue in honor of Cesar Chavez.
Embezzlement via Diverted Deposits
To deter employee theft of checks, Control Incoming & Outgoing Mail
Santa Monica, CA
Big Blue Bus
$1,075,000
County of Los Angeles mailed $1,075,000 check to Santa Monica for Big Blue Bus (Federal Transportation Money)
Big Blue Bus

Check was stolen

Deposited into brokerage account in Colorado

Account opened via mail with totally fake ID
Big Blue Bus

Check was stolen

Deposited into brokerage account in Colorado

Account opened via mail with totally fake ID

Securities were purchased, then sold

All the money wired out

Money was not discovered missing for 6 months!!
Check was NOT Altered

Endorsement was forged
Big Blue Bus

Check was NOT Altered

Endorsement was forged

Forged endorsements are the liability of

the Bank of First Deposit for 3 years

(Except in Florida and Georgia: One Year)
Big Blue Bus

Brokerage firm would not be liable if check was stolen by an employee.
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 for citizenship failed to include prison time in North Carolina for check fraud.

Part of $20,000,000 scheme

 Arrested by Houston Postal Inspector
$800,000 was spent on legal fees by both sides before the case was settled!

(settlement was only a fraction of the $1,075,000 loss)
Controls to Prevent Internal Fraud
To prevent Embezzlement via 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!
If you suspect embezzlement and intend to prosecute

DO NOT tamper with the 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. Search the mirror.
Controls to Prevent Fraud

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

- **Skimming of Cash**
  - Segregation of Duties
  - Policy on Voids / Credits
  - Pre-numbered Receipts / Information
  - Regular + **Frequent** Surprise Cash Counts
  - Match Cash deposits to the bank statement
Controls to Prevent Fraud

Add and vet new vendors by someone without a direct reporting relationship to the person approving vendor payments.
Controls to Prevent Fraud

- Vendors
  - Segregate approval of vendors from authorization of payments
  - Current authorized signer list
  - System that won’t allow duplicate payments
  - Timely vendor payments including verification of goods / services
  - Timely reconciliation of paid checks and review of check images to records
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.
- Confirm deposit appears on the bank statement.
- Don't let the auditee explain away exceptions to your tests.
- Prosecute if possible. Inform employees what happened.
A “Tip Hotline” is a very effective tool to detect embezzlement. Tip hotlines should be accessible by:

1. Employees
2. Vendors
3. Customers
4. Outsiders
Anonymous Tip Line (with a $$$ Reward)

Tips are the #1 means of detecting embezzlement
eChecks – A new twist on check fraud
The Fraud Bulletin
Volume 15

The Interconnections of Fraud

Inside This Issue
1. The Evolution of Check Fraud
2. Positive Pay Lawsuit
3. Fraud In A Pocket
   . . . . Mobile Phons
4. BEC Scams
5. Corporate Imposter Fraud
6. Cyber Crime – A Never-Ending Challenge
7. Check 21: The Hidden Liability
8. Court Cases: Holder In Due Course
    Check Fraud Scams
9. The Evolution of Check Fraud
10. Laser Printing and Check Fraud
11. Positive Pay, ACH, and Secure Check Writing Software
12. Check Fraud Prevention – Best Practices
13. Check Security Features – Why They Matter
14. Abagnale SuperBusinessCheck
15. SAFEChecks
16. Supercheck
17. Embezzlement
18. Ransomware
19. Identity Theft
20. Wine Trafficking
21. An Explosive
22. Same Day Innovation
23. ACH Fraud
24. Cybercrime
25. ACH Fraud

Detecting and Deterring Embezzlement in the 21st Century
By Frank W. Abagnale
November 2020

“If you make it easy for people to steal from you, they will.”

Over the years I have found this simple principle to hold true: Most crimes committed are crimes of opportunity. For example, if you do not want to be a victim of check fraud, use highly secure checks and Payee Positive Pay. If you do not want to be embezzled, follow appropriate internal safeguards. In most embezzlement cases, basic controls would have prevented or substantially reduced the losses.

Each year for the last several years, embezzlement has made new records, surpassing the previous season’s “blockbuster year.” With the turmoil and disarray caused by COVID-19, it’s likely the upward spiral of internal fraud will continue for some time to come.

The following is a summary of research to better understand the mechanisms of embezzlement and protocols to detect and deter it. In developing this list of recommendations, I have solicited the comments and experience of Greg List, president of SAFEChecks, a former 18-year senior-level banker and expert witness in national and international embezzlement cases, and the research of Robin Johnson of SAFEChecks, MBA and MAPP (Master of Applied Positive Psychology, Penn). Their insights also draw from embezzlement studies conducted by the Association of Certified Fraud Examiners (ACFE), Hiscox USA, Marquet International, and others. (See Resources below.)

Real Life Examples
- Two sisters working as “lunch ladies” embezzled almost $500,000 from two school cafeterias over five years. Officials found inconsistencies in how cash was handled and asked police to investigate.
- A high-end New York department store suffered $430,000 in fraudulent purchases by employees who used stolen credit card information to buy designer goods on store computers. The employees then sold the designer goods on the black market before being caught.
- The chief fiscal officer of a state agency wrote checks to herself using the agency’s bank account and with the help of her son who also worked there, created bogus invoices from vendors. During a seven-year period the CFO and her son embezzled over $1 million from the organization.

Every type and size of organization has suffered embezzlement losses, and a typical organization loses 5% of annual revenue to fraud. This has resulted in bankruptcy or layoffs, cutbacks, and damaged reputations. The victims are not only the organizations, but their partners, suppliers, vendors, customers, clients, and families. The 2020 Hiscox Embezzlement Study found that typical losses from “occupational fraud” in the United States surpassed $500,000, and 55% of victim organizations recovered none of their losses.

The Psychology of Embezzlement

Internal fraud occurs when the “fraud triangle” is present – motive, opportunity, and rationalization. Workplace conditions are a major predictor of fraud, and usually reveal overconfidence on the part of owners and managers and a lack of preparation in establishing effective fraud prevention controls. In almost 30% of cases there were no internal controls to prevent embezzlement, and the number rose...
eChecks is a new technology designed to move money quickly and efficiently. The concept is simple: Send money to the intended recipient by email. The email includes a link to a file that contains a check image payable to the recipient, and an access code to open the file and download and print the check. The check image can be downloaded only once for printing.

The flaw is the recipient’s ability to print the eCheck as a high resolution PDF, which can be reprinted and cashed multiple times. Every check appears genuine. Fraudsters have already exploited this flaw.

A company in the West with hundreds of small vendors in 40 states switched to eChecks. Over a few months the company issued about 9,000 eChecks, and soon had over $17,000 in check fraud losses!

More than 50 of the eCheck recipients downloaded and saved the check images as high resolution PDFs. Then, they printed and cashed or deposited those duplicate checks, getting paid multiple times on the same check. Over 300 duplicate eChecks hit the company’s bank account.

Banks have used software to detect duplicate checks for decades. The process is based upon check numbers and dollar amounts. In this case, the bank could not identify many of the duplicate eChecks because about 10 percent of the total eChecks issued had a check number that was not readable or captured by the bank’s Character Recognition (OCR) software.

As the duplicate eChecks were discovered by the company and presented to the bank, the bank began reimbursing the company. However, as the dollar losses grew, the bank told the company it should have been using Positive Pay, even though the bank had never before mentioned Positive Pay.

The bank refused to reimburse the company for additional losses. (Positive Pay will work with eChecks, but would be difficult because of the high percentage of unreadable check numbers, each of which would have become a Positive Pay exception item.)

One of the company’s vendors had its email system hacked. The hacker intercepted the eCheck email, and downloaded and printed the $2500 check image. The hacker then cashed the check at a check cashing store after forging the endorsement. The company has filed an affidavit of forged endorsement with its bank and expects to recover the $2500 from the bank of first deposit; however, this does not spare them the harassment of dealing with the fraud.

eCheck users should be mindful of their legal liability for duplicate checks under UCC § 3-302, Holder In Due Course. If a check looks “genuine,” the drawer can be held liable for the face value of the check, even if the check is counterfeit. (See Page 9, Robert Triffin v. Somerset Valley Bank and Hauser Contracting Co.) Because every eCheck can be printed/saved as a PDF that appears “genuine,” eCheck users are strongly encouraged to buy check fraud insurance.
How eChecks work

How eChecks work:

1. Create & send
   Log in to your eChecks account or integrate with QuickBooks and other software to send checks in a few clicks.

2. Receive, retrieve & print
   Recipients receive a link in their email, retrieve their eCheck from our secure online portal and print the check from any home or office printer.

3. Deposit the check
   An eCheck is deposited just like any other check - at a bank branch, through an ATM or using Remote Deposit Capture on a smartphone.
The Flaw in eChecks

✓ The **flaw** in eChecks is a dishonest recipient's ability to download & print the eCheck as a **high-res PDF**.

✓ A high-res pdf can be **reprinted & cashed 1000+ times**

✓
The Flaw in eChecks

✓ The **flaw** in eChecks is a dishonest recipient's ability to download & print the eCheck as a **high-res PDF**.

✓ A high-res pdf can be **reprinted & cashed 1000+ times**

✓ Each printed eCheck looks identical to the very first printed eCheck; each **looks** genuine and **is** genuine.
The Flaw in eChecks

Under the UCC, **every eCheck is a negotiable instrument** for which the drawer can be held liable under UCC’s “Holder In Due Course” (HIDC): each check appears genuine.

Even if a duplicate eCheck is caught on Positive Pay, the issuer can still be held liable for the face value of the check because of HIDC.

HIDC **trumps Positive Pay.**
An eCheck Fraud Example
An eCheck fraud example

In one eCheck fraud case, the company’s bank could not read the check number on about 10% of the eChecks presented for payment.

The dollar amount of each check appeared as a debit on the bank statement, but without the check number.

Reconciliation was not possible without the check number, which was on the image.
An eCheck fraud example

Check images are pulled by check number. Customer had its bank pull hundreds of check images using each item’s “trace number”

300 eCheck images were duplicates

Every duplicate was identical to other checks

One check was printed & deposited 50 times
100% Satisfaction Guaranteed
(but only for 60 days!)

100% Satisfaction Guarantee

eChecks are guaranteed to save you time and money. If, within 60 days, you’re not completely satisfied with your eChecks experience, we will refund the unused portion of your eChecks order.
100% Satisfaction Guaranteed (but only for 60 days!)

100% Satisfaction Guarantee

eChecks are guaranteed to save you time and money. If, within 60 days, you’re not completely satisfied with your eChecks experience, Xxxxxx will refund the unused portion of your eChecks order.

“Xxxxxx eChecks are guaranteed to save you time and money. If, within 60 days, you’re not completely satisfied with your eChecks experience, Xxxxxx will refund the unused portion of your eChecks order.”
There is No Solution

eChecks work in a society where everyone is HONEST
There is No Solution

eChecks work in a society where everyone is HONEST

In today’s society eChecks carry an immitigable risk that paper checks don’t have
There is No Solution

eChecks work in a society where everyone is HONEST

In today’s society eChecks carry an immitigable risk that paper checks don’t have

Get an Indemnity Agreement that covers losses and costs from duplicate eCheck presentments

Include Attorney and CPA fees
Uniform Commercial Code (UCC) §3-302

Holder in Due Course

Web: FraudTips.net
Uniform Commercial Code §3-302
The Fraud Bulletin
Volume 15

The Interconnections of Fraud

Inside this Issue

1. The Evolution of Check Fraud
2. Positive Pay Lawsuit
3. Fraud in a Pocket... Mobile Phones
4. BEC Scams
5. Corporate Imposter Fraud
6. Cyber Crime – A Never-Ending Challenge
7. Check 21: The Hidden Liability
8. Court Cases: Holder in Due Course
9. Check Fraud Scams
10. Laser Printing and Check Fraud
11. Positive Pay, ACH, and Secure Check Writing Software
12. Check Fraud Prevention – Best Practices
13. Check Security Features – Why They Matter
14. Abagnale SuperBusinessCheck
15. SAFECheks
16. Supercheck
17. Embezzlement
18. Ransomware
19. eCheck
20. Identity Theft
21. Wire Transfer Fraud – An Explosion in Cyber Space
22. Same Day ACH – Innovation in Payments
23. ACH Fraud – On the Rise...
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.

Holder in Due Course trumps stop payments and Positive Pay exceptions. Further, an HIDC can assign, sell, give, or otherwise transfer its rights to another party, who assumes the same legal rights as the original Holder.

In the 2012 AFP Payments Fraud and Control Survey, 48 percent of organizations’ check fraud losses were a result of payouts to check cashers (bank and non-bank) from HIDC claims. This is up from 37 percent in the 2009 survey, indicating a growing and serious concern.

Prudent companies use controlled high security checks to protect themselves from some HIDC claims.

The following three Federal Appellate Court cases illustrate the far-reaching power of Holder in Due Course laws.

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%
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

Appellate Court

Lawsuits / Court Cases
Placing a Stop Payment on a check ends your legal responsibility to pay the check.

- True
- False
Pop Quiz (open book): True or False?

Placing a Stop Payment on a check ends your legal responsibility to pay the check.

- True
- False

FALSE

Holder in due course trumps Stop Payments
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 this 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.

Recommendaion: 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-163-00T5 lawlibrary.rutgers.edu/courts/appellate/a4000-95.opn.html
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

Whomever accepts an “expired” negotiable instrument has no legal standing as a Holder in Due Course.
You cannot be held liable for a check you did not issue or authorize.
You cannot be held liable for a check you did not issue or authorize.

**FALSE**

If a counterfeit check looks "genuine" you can be held liable under **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 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 cashing agencies, claimed HDC 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 cashing 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. SAFE_checks and Supercp Business Check are controlled check stocks.

Superior Court of New Jersey, Appellate Division, A-163-00T5
lawlibrary.rutgers.edu/courts/appellate/a0163-00.opn.html
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

Robert Triffin v. Somerset Valley Bank and Hauser Contracting Company

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

HIDC & Controlled Check Stock

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
Every new check order is verified with the bank

SAFEChecks has never had a check replicated or used in a scam in 24 years
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.
Robert Triffin v. Pomerantz Staffing Services

- 18 counterfeit checks drawn on Pomerantz’ account cashed at a check cashing store. Every check under $400

http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html
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
• 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. Pomerantz 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
Holder in Due Course (HIDC)

- 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**

Pomerantz Staffing Services used high security checks that included heat sensitive (thermochromic) ink on the back and a warning banner on the face that said, “THE BACK OF THIS CHECK HAS HEAT SENSITIVE INK TO CONFIRM AUTHENTICITY.” Someone made copies of Pomerantz’s checks, 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 Holder in Due Course status, and sued Pomerantz. Pomerantz counter-sued 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 HIDC and had no rights to transfer to Mr. Triffin.

This case illustrates the value of check security features, a properly worded warning band, and a controlled check stock. Pomerantz was protected by his checks.

**Recommendation:** Use high security checks with overt and covert security features, including explicitly worded warning bands. Such security features will also help prevent other kinds of check fraud. The **SuperBusinessCheck** is a properly designed high security check with 16 security features.

Visit [www.fraudtips.net](http://www.fraudtips.net) for an in-depth article, *Holder in Due Course and Check Fraud*, written by Frank Abagnale and Greg Litster. Click on Holder in Due Course.