Financial Fraud Trifecta: BEC Scams, Wire Fraud, Check Fraud – Part II

Greg Litster, President
SAFEChecks

"Business Email Compromise"

AKA the **BEC Scam**

FBI WARNING

In 2015, FBI issued two **BEC scam** alerts.

By First Quarter 2016, over **12,000** companies have been compromised.

→ → → **Losses: $2 Billion!**

Today, many organizations still have not heard about BEC scams, and are still falling prey to them!

BEC Scams target ORGANIZATIONS & BUSINESSES not banks.

BEC Scams rely on a legitimate request from an authorized user to their bank.

Association for Financial Professionals Payments Fraud and Control Survey 2016:

64% reported their organizations have been exposed to business email compromise (BEC).

Wire transfer is the preferred payment method.

The problem is not the bank's wire transfer system.

It's a human failure.

Somebody falls for a clever social engineering scam.

✓ Criminals acquire info on targeted company from public sources (social media, press releases)

✓ They study organizational structure, vendors, customers, CEO/CFO travel plans

✓ They decide which executive to impersonate, which subordinate to target, and what type of message will be most believable.

✓ They study the style, language, content of emails of the executive they're impersonating

They research wire transfer protocols and amounts typical for that person

They strike the target when the executive is out of the office (not available for confirmation).

Criminals deliver the message by email.

They compromise the executive's email account,

– controlling email flow to avoid detection –

redirecting emails, editing Settings for replies

If they can't compromise an executive's email account, they CREATE a new email account:

Fraudsters send a well-written email (supposedly from the CEO, CFO, etc.) to another targeted person in the organization, directing them to send a wire transfer

– The targeted person sends wire request to bank

– If the bank calls to confirm request, the targeted person approves the request

This scam would likely fail if EFT protocols required a second approval by a second person.

BEC Scams can include:

1. Email from an executive requesting a wire transfer
2. Fake instructions from a vendor with "updated" remittance instructions
3. Change-of-bank and PO Box remittance sent to its own customers, instructing them to remit to a new bank or PO Box

Email requesting Wire Transfer

New | Reply | Forward

Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

High Importance

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

Fake Vendor Invoices:

- Criminals target someone in the Finance Dept
- They review invoices from legitimate vendors that the Finance department has received via email
- They create a fraudulent invoice replicating real invoices received

Fake Vendor Invoices:

- The fake invoice has updated banking information, with the account controlled by the criminals
- They send a fake invoice using an email address very similar to that of the real vendor
- The Finance Department pays the invoice, remitting to the new account.
- If questioned by the Bank, the transaction is approved because the invoice looks legitimate

Solutions to BEC Scams

- Verify that the email address source is correct.

(Addresses are often changed by a single letter!)

- Implement a detection system that flags e-mails with extensions that are similar to the company e-mail

- Spoofed emails used in BEC scams are unlikely to set off spam traps because the targets are not mass emailed

Solutions to BEC Scams

- Be suspicious of urgency and/or secrecy in a wire transfer request

- Look for consistency with prior requests, from CEO, CFO, etc. and also from vendor companies.

- Look at wording, phrasing of email – it may have a different style than normal, misspellings, errors.

Solutions to BEC Scams

- Use alternate forms of communication to confirm the request, e.g. if the request came via email, confirm via phone.

- Use a known phone number, not one shown in the email request

- Confirm that the request actually originated with a "C" level executive, especially if the request says no more confirmation is needed

Solutions to BEC Scams

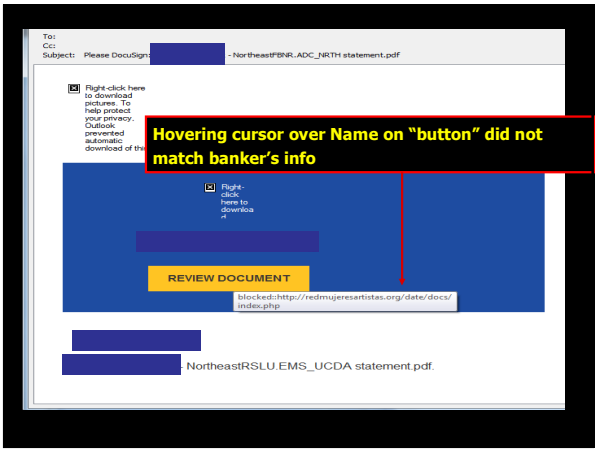
- Use dual controls for wire transfers – two people must always approve a wire transfer

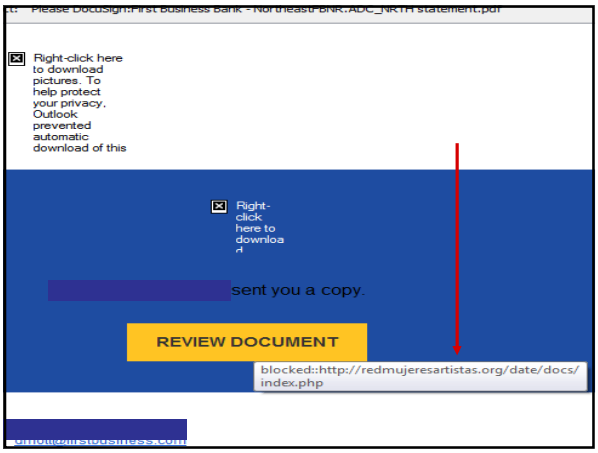
Solutions to BEC Scams

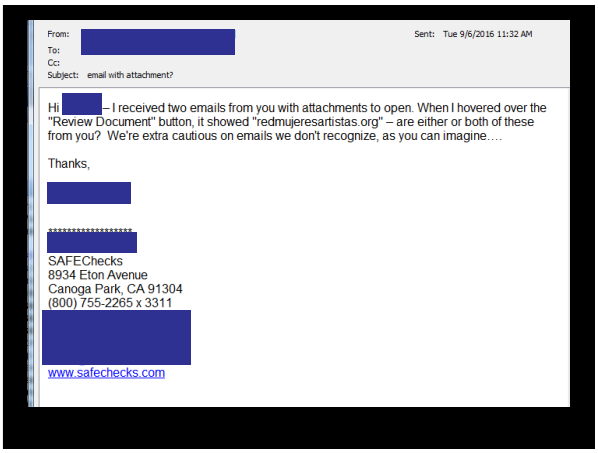
- Use dual controls for wire transfers – two people must always approve a wire transfer

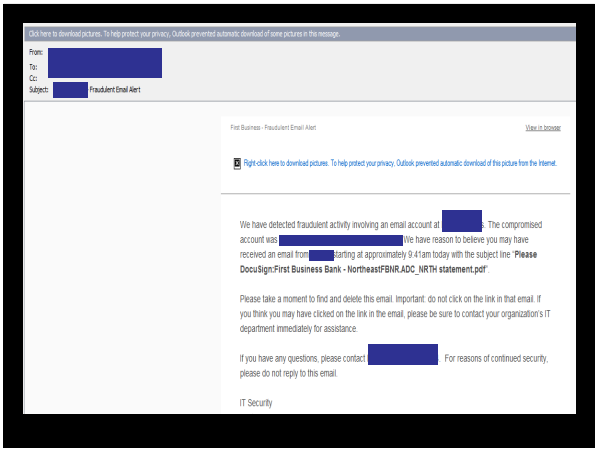
- Ideally, there should not be a direct reporting relationship between those two people

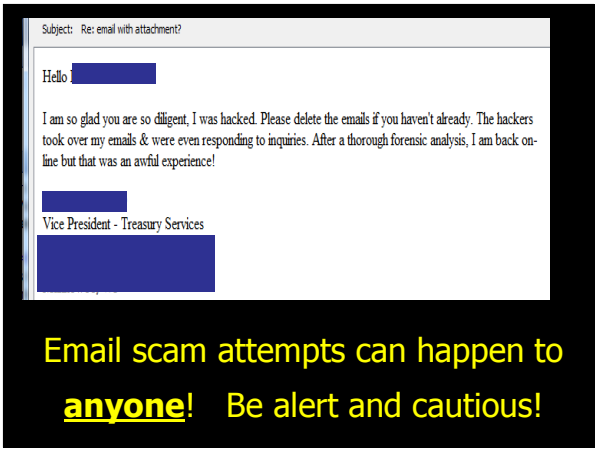
Recent email scam attempt at SAFEChecks –











Email scam attempts can happen to **anyone**! Be alert and cautious!

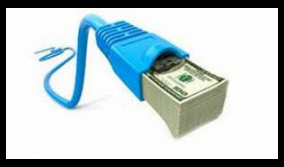
Video

Preventing Unauthorized Wire Transfers

In 2010, wire transfer fraud represented on 3% of payment fraud.

In 2015, it represented 27%.

Today, it represents 48%!



Preventing Unauthorized Wire Transfers

Purchase a new computer that is dedicated to online banking only.

It connects into the bank, and nothing else.

Preventing Unauthorized Wire Transfers

Require two different computers and passwords to send money.

Multiple employees can initiate a wire or ACH transfer using their daily use computers.

ALL wires/ACH transfers MUST BE released using the dedicated banking computer.

Different user names, different passwords.

Preventing Unauthorized Wire Transfers

Update your bank's Electronic Funds Transfer (EFT) agreement to reflect your revised, two-computer policy.

Preventing Unauthorized Wire Transfers

To help shift liability for any cyber losses from you to the bank, follow your bank's internal controls and technology recommendations.

NOTE: Failure to implement the bank's recommends may result in your company being held liable for the losses.

2. Fraudsters infiltrate a company's network, **identify its customers**, and send BOGUS change-of-bank notices, diverting payments to a bank and P.O. Box the fraudster controls.

- ✓ **Hackers target Accounts Receivable List**
- ✓ **Send bogus change-of-bank notifications to customers**
- ✓ **New PO Box <u>controlled by hackers</u>**
- ✓ **New Bank R/T and account <u>controlled by hackers</u>**

Simple Solutions…

- ✓ <u>Banks</u>: Monitor bank changes on outgoing repetitive wires

  <u>Municipalities/Organizations</u>: Confirm ALL bank change notifications from vendors. <u>CALL</u>, don't email.

- ✓ Buy cyber crime and check fraud insurance

RESOURCES:

BEC BestPracticesVideo (YouTube), Guardian Analytics

BEC Scams: How Treasurers Can Recognize Them (YouTube), AFP

RESOURCES:

businessidtheft.org
Dun & Bradstreet
Bloomberg BusinessWeek,
The Council of State Governments

Also, review information and resources offered by your state and local government.

Check Fraud

Why talk about Check Fraud?

Check Fraud

Produces more $ Losses

than all other types of payment fraud!

AFP 2016 Payments Fraud Survey

"…checks continue to be the payment method most often exposed to fraud because they are still the most frequently used payment method….

AFP 2016 Payments Fraud Survey

…In addition, fraudsters are familiar with checks and so are able to commit check fraud with relative ease with the help of sophisticated equipment."

AFP 2016 Payments Fraud Survey

Check fraud still accounts for the largest dollar amount of financial loss due to fraud.

AFP 2016

Payments Fraud Survey

50% of organizations still issue checks.

Check fraud is not going away!

Today's generation:

What once was "old" is NEW

"...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**.

Wall Street Journal, March 8, 2016

9

"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

What has changed are the size and scale of the operations. **"The sums of money involved are staggering.** Even though it's a small minority...the potential amount of money involved and damage to people's financial accounts is greatly out of proportion to other gang crimes....

Check fraud has become especially popular..."

Wall Street Journal, March 8, 2016

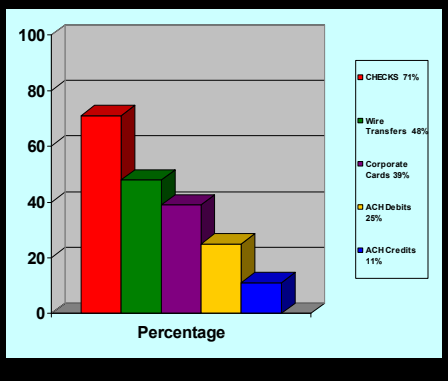
Twelve members of a group known as the Van Dyke Money Gang were accused last summer of bilking banks out of more than **$1.5 million**.

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.

Wall Street Journal, March 8, 2016

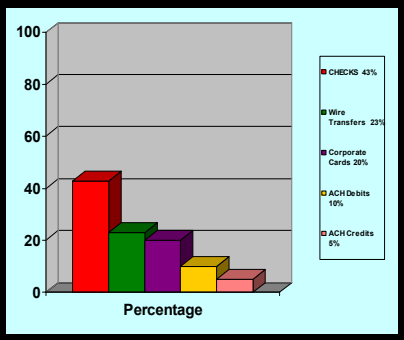
Fraudulent Payments by Method

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



Fraud Losses by Method

How Dollars were actually lost



Technology twists on Check Fraud....

Mobile Banking and Deposit Fraud:

Double Debits

Mobile Banking Deposit Fraud

Scenario: A check is mailed to Dishonest Don

- Don deposits the check using smart phone app
  - Digitized check is paid at drawer's bank
- 3 days later, Don cashes the same check at a check cashing store
  - ✓ 2nd check hits the drawer's bank account (check is presented for payment twice)

Who Takes The Loss?

The answer is found in the Rules governing **Check 21**

Under the § 229.56 Warranty…

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

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

§ 229.52 Substitute check warranties

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

§ 229.52 Substitute check warranties

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

§ 229.52 Substitute check warranties

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

§ 229.56 Liability

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

Under the § 229.56 Warranty…

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

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

Mobile Banking and Deposit Fraud:

Holder in Due Course

Scenario: A title insurance company gives John Doe a check at closing. John Doe deposits the check via a mobile app,

then comes back to office and returns the check, asking that it be made payable to John Doe or Jane Doe.

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

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

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

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

Don't Write Checks!

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

But, if you are going to write checks…

#1. Positive Pay

Positive Pay…

…a powerful tool!

PositivePay.net

#2. High Security Checks

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

High Security Checks

1. Deter the forger (psychological warfare)
2. Thwart forgers' attempts to replicate or alter the check
3. Provide legal protection from some Holder in Due Course claims (UCC § 3-302)

What makes a check secure?

10+ safety features

Important Security Features

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

www.safechecks.com

Controlled Check Stock

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

www.safechecks.com

Uncontrolled Check Stock

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

www.safechecks.com

How is Uncontrolled Check Stock a problem?

Counterfeit Cashiers Checks

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Home | Deposit Insurance | Consumer Protection | Industry Analysis | Regulations & Examinations | Ins

Press Releases | Online Press Room | Conferences & Events | Financial Institution Letters | Special Alerts | Letters to the Editor/Opin

Home > News & Events > Special Alerts

Printer Friendly

Special Alerts

SA-1-2011
January 3, 2011

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)
SUBJECT: Counterfeit Cashier's Checks
Summary: *Counterfeit cashier's checks bearing the name Delta Trust and Delta Bank & Trust, Little Rock, Arkansas, are reportedly in circulation.*

Delta Trust & Bank, Parkdale, Arkansas, has contacted the Federal Deposit Insurance Corporation (FDIC) to report that counterfeit cashier's checks bearing the institution's name are in circulation.

Counterfeit Cashiers Checks

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Home | Deposit Insurance | Consumer Protection | Industry Analysis | Regulations & Examinations | In

Press Releases | Online Press Room | Conferences & Events | Financial Institution Letters | Special Alerts | Letters to the Editor/Op

Home > News & Events > Special Alerts

Printer Friendly

Special Alerts

SA-12-2011
March 2, 2011

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)
SUBJECT: Counterfeit Cashier's Checks
Summary: *Counterfeit cashier's checks bearing the name CommunityAmerica Credit Union, Lenexa, Kansas, are reportedly in circulation.*

CommunityAmerica Credit Union, Lenexa, Kansas, has contacted the Federal Deposit Insurance Corporation (FDIC) to report that counterfeit cashier's checks bearing the institution's name are in circulation. CommunityAmerica Credit Union does not issue cashier's checks; however, it does issue

Counterfeit Cashiers Checks

FDIC Federal Deposit Insurance Corporation
Each depositor insured to at least $250,000 per insured bank

Home | Deposit Insurance | Consumer Protection | Industry Analysis | Regulations & Examinations | Ins

Press Releases | Online Press Room | Conferences & Events | Financial Institution Letters | Special Alerts | Letters to the Editor/Opi

Home > News & Events > Special Alerts

Printer Friendly

Special Alerts

SA-2-2011
January 3, 2011

TO: CHIEF EXECUTIVE OFFICER (also of interest to Security Officer)
SUBJECT: Counterfeit Cashier's Checks
Summary: *Counterfeit cashier's checks bearing the name South Georgia Banking Company are reportedly in circulation.*

South Georgia Banking Company, Omega, Georgia, has contacted the Federal Deposit Insurance Corporation (FDIC) to report that counterfeit cashier's checks bearing the institution's name are in circulation.

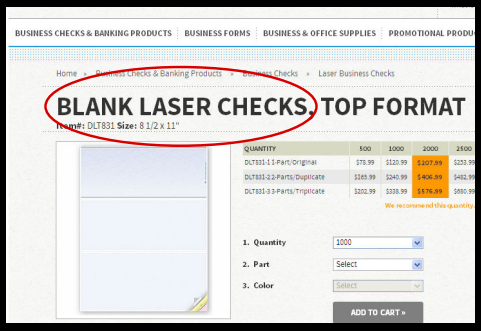
Who Sells Blank, Uncontrolled Checks?

- Virtually ALL accounting / check writing Software Vendors

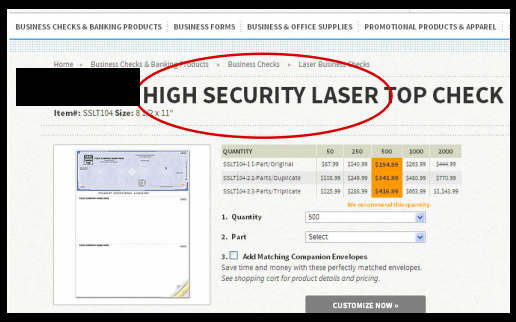
Who Sells Blank, Uncontrolled Checks?

- Virtually ALL accounting / check writing Software Vendors
- Virtually ALL check printers
  1. Large, national printers
  2. Small print brokers buy from wholesalers

Uncontrolled Checks

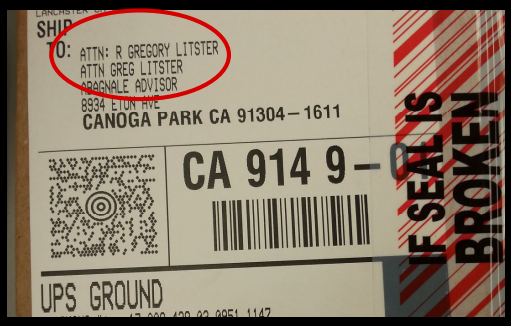


Uncontrolled Checks

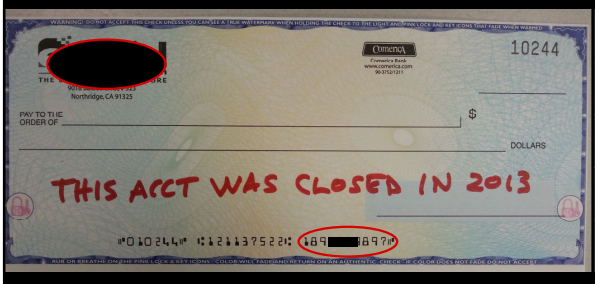


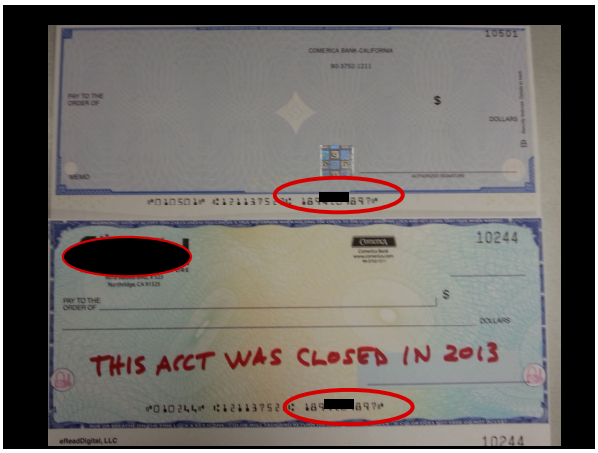
I bought high-security checks from XXXXX…

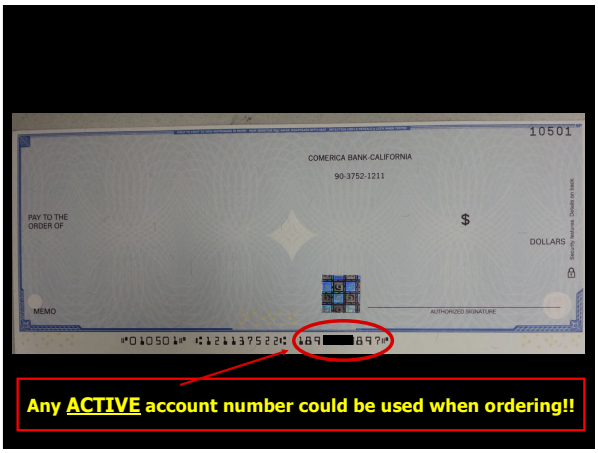
…using the account number of a closed account!

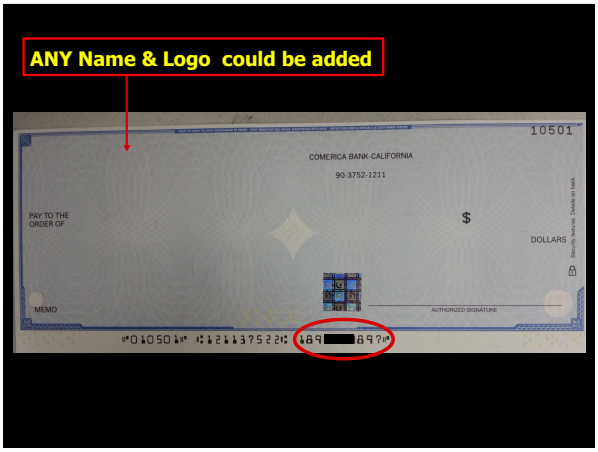


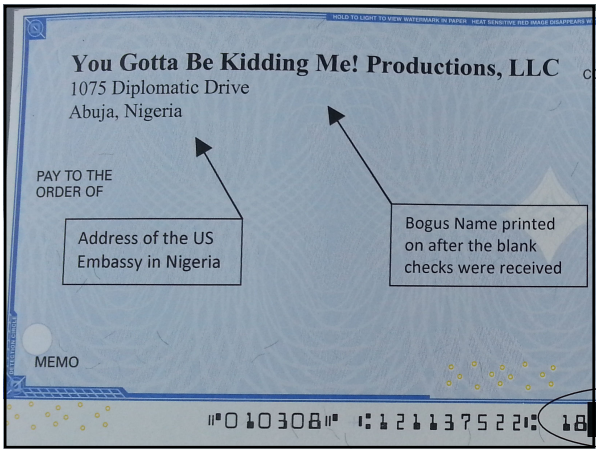
Failure to Verify Name/Account #/ Address



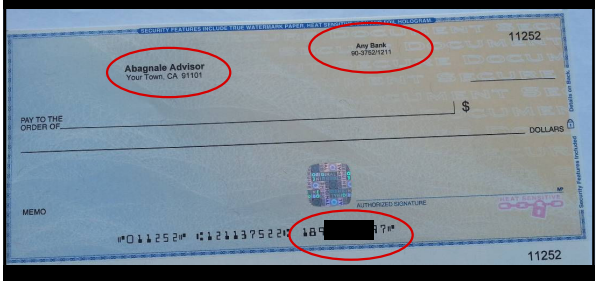






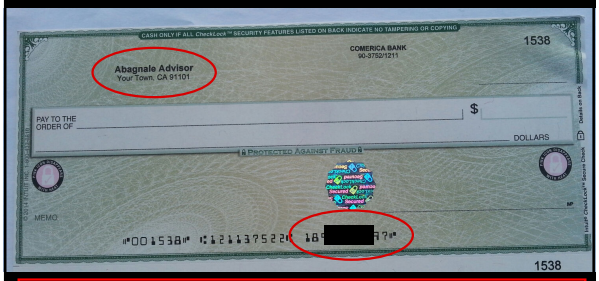


Costco



I ordered checks using a closed account number…
Costco didn't care! Forgers use good account numbers.

Intuit (Quickbooks)



I ordered checks using a closed account number…
Intuit didn't care! Forgers use good account numbers.

Holder in Due Course

and

Uncontrolled Check Stock

Web: FraudTips.net

HIDC & Uncontrolled Check Stock

Robert Triffin v.

Somerset Valley Bank and

Hauser Contracting Company

Obtaining Controlled Check Stock

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

SAFEChecks.com

Other Important Security Features

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

www.safechecks.com

HIDC & High Security Checks

Robert Triffin v.

Pomerantz Staffing Services

Preventing Altered Payees

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

Frank Abagnale's Fraud Bulletin on Laser Check Printing

Positive Pay Provides

NO PROTECTION

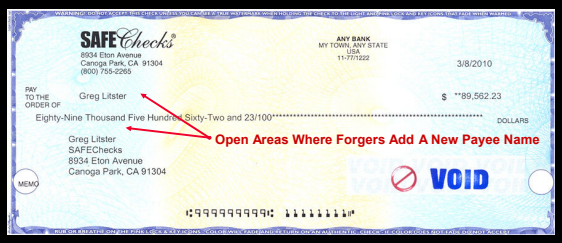
Against

Added Payee Names!

Secure Check Writing Software

To Prevent Added Payees

Typical Check Layout



Fix it: Use a Secure Name Font

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

Leaves No Room for Adding Bogus Payee

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

Deterrence: Add Info to the Check

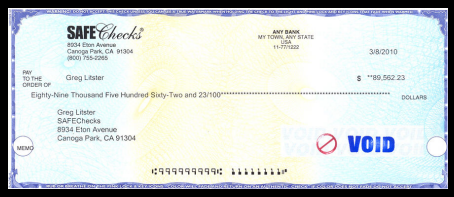
Deterrence: Encrypted barcode

Barcode contains:

1. Drawer
2. Payee Name
3. Dollar Amount
4. Issue Date
5. Check Number
6. Account Number
7. Routing/Transit Number
8. Date and Time Check was printed
9. Laser Printer used
10. The employee that printed the check

Barcode is created by a Printer Driver

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



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