

# CREDIT CARD FRAUD, CHECK FRAUD, AND SCAMS IN THE US

**What do I need to know?**



A woman in a business suit is standing and presenting to a group of people seated at tables in a meeting room. The background wall features several business-related diagrams and icons, including a lightbulb, a pie chart, a target, a line graph, and a bar chart. The text is overlaid on this background.

# TODAY'S PRESENTER

**MICHAEL WILLIAMS**

**VICE PRESIDENT, UTA\* Presenter**

**Phone: 800-858-5256 x 7019**

**Direct: 786-264-7019**

**[mwilliams@unitedtranzactions.com](mailto:mwilliams@unitedtranzactions.com)**

**DISCLAIMER:** THIS COMMUNICATION, INCLUDING ANY CONTENT HEREIN AND/OR ATTACHMENTS HERETO, IS PROVIDED AS A CONVENIENCE ONLY, DOES NOT CONSTITUTE LEGAL ADVICE, DOES NOT CREATE AN ATTORNEY CLIENT RELATIONSHIP, AND DOES NOT ALTER YOUR CURRENT MERCHANT SERVICES AGREEMENT. BECAUSE OF THE GENERALITY OF THIS COMMUNICATION, THE INFORMATION PROVIDED HEREIN MAY NOT BE APPLICABLE IN ALL SITUATIONS AND DOES NOT CONSTITUTE A COMPREHENSIVE LIST OF ISSUES THAT COULD IMPACT YOUR BUSINESS. ALL MERCHANTS, INCLUDING UTA - WORLDPAY CLIENTS, ARE SUBJECT TO THE TERMS OF THEIR BANK CARD MERCHANT AGREEMENT, THE CARD NETWORKS' OPERATING REGULATIONS, AND APPLICABLE FEDERAL AND STATE LAWS.

**DISCLAIMER:**

THIS COMMUNICATION, INCLUDING ANY CONTENT HEREIN AND/OR ATTACHMENTS HERETO, IS PROVIDED AS A CONVENIENCE ONLY, DOES NOT CONSTITUTE LEGAL ADVICE, DOES NOT CREATE AN ATTORNEY CLIENT RELATIONSHIP, AND DOES NOT ALTER YOUR CURRENT MERCHANT SERVICES AGREEMENT. BECAUSE OF THE GENERALITY OF THIS COMMUNICATION, THE INFORMATION PROVIDED HEREIN MAY NOT BE APPLICABLE IN ALL SITUATIONS AND DOES NOT CONSTITUTE A COMPREHENSIVE LIST OF ISSUES THAT COULD IMPACT YOUR BUSINESS. ALL MERCHANTS, ARE SUBJECT TO THE TERMS OF THEIR BANK CARD MERCHANT AGREEMENT, THE CARD NETWORKS' OPERATING REGULATIONS, AND APPLICABLE FEDERAL AND STATE LAWS.

# CREDIT CARD FRAUD



# 2021 FRAUD STATISTICS

- Credit card fraud rose by **45%** over 2021
  - More than **400k** reported cases of Credit Card fraud in 2022
  - **1.4 MILLION** reports of identity theft in 2022
  - Those aged **30 to 39** reported the most cases of identity theft
  - **Kansas, Rhode Island,** and **Illinois** were the top three states for identity theft per capita
- 

# FRAUD CAN BE COSTLY

**THE COST TO BOTH BUSINESSES AND CONSUMERS FROM CREDIT CARD FRAUD ARE BILLIONS OF DOLLARS EVERY YEAR.**

- Fraudsters are continually finding new ways to commit their illegal activities.
  - It is essential to develop fraud prevention and detection techniques to counter the threat of fraudulent credit card transactions and identity theft and keep losses to a minimum.
  - A study conducted by Kount reported that 40% of all financial fraud was related to credit cards.
- 

# Personal Credit Card Fraud Prevention Tips



# THERE ARE TWO TYPES OF PERSONAL CREDIT CARD FRAUD

**NEW ACCOUNT:** AN IDENTITY THIEF USES YOUR INFORMATION TO OPEN A CREDIT CARD ACCOUNT IN YOUR NAME.

**EXISTING ACCOUNT:** AN IDENTITY THIEF USES AN EXISTING CREDIT CARD. THIS IS USUALLY DONE BY STEALING THE CREDIT CARD INFORMATION.



**NEW ACCOUNT FRAUD REPORTEDLY  
INCREASED BY 12% IN 2022 TO A  
TOTAL OF 363,029 CASES.**

<b>TYPE OF CREDIT CARD FRAUD</b>	<b>NUMBER OF REPORTS IN 2022</b>	<b>CHANGE FROM 2021</b>
<b>New account</b>	363,092	-1%
<b>Existing account</b>	32,204	-5%

# WHY THE SHIFT FROM STOLEN CARDS TO IDENTITY THEFT?

- EXISTING ACCOUNT FRAUD HAS BECOME MORE DIFFICULT I E CHIP CARDS AND EMV
  - DATA BREACHES CAPTURE PERSONAL DATA IN THE MILLIONS AT ONE TIME
  - EASIER TO STEAL FROM NEW ACCOUNTS
- 

IT'S IMPORTANT TO REMEMBER THAT YOU CAN DISPUTE CREDIT CARD CHARGES WITH YOUR CREDIT CARD ISSUER IF YOUR CARD OR INFORMATION HAS BEEN STOLEN.

TIME IS OF THE ESSENCE IN REPORTING FRAUD!

WHO YOU CHOOSE AS A PROCESSOR IS CRITICALLY IMPORTANT!

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

# BUSINESS CREDIT CARD FRAUD



# COMMON TYPES OF CREDIT CARD FRAUD

- Account Takeover
- Account Creation
- Brute Force Attacks
- Card Testing



# REDUCE SECURITY & DATA BREACH CONCERNS

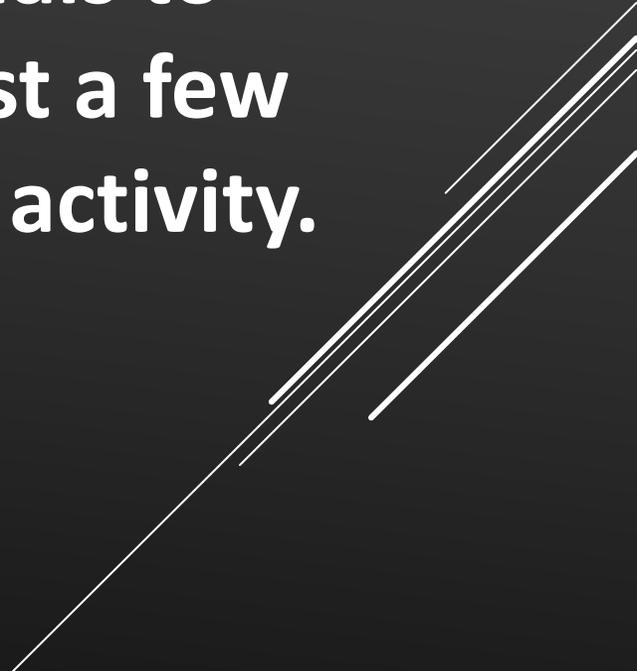
- Tokenization
- Point to Point encryption
- Secure sensitive data
- Employee Training
- In 2021, the average business cost of fraudulent attacks is \$4.24 million, and it takes more than 287 days to detect the breach.



**THERE ARE SEVERAL WAYS TO REDUCE YOUR EXPOSURE TO BUSINESS FRAUD. MANY INVOLVE DEVELOPING BETTER WAYS TO AUTHENTICATE CUSTOMERS AND ONLINE SHOPPERS.**



**Your ongoing challenge will be to make it as easy as possible for customers to complete their purchases without also inviting criminals to exploit your vulnerabilities. Here are just a few tips for deterring this type of fraudulent activity.**



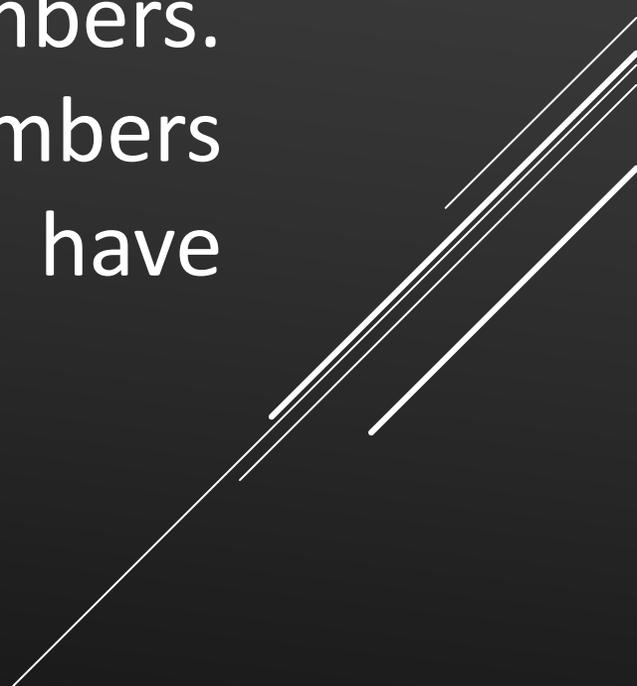
# 1. Don't expect credit card companies and processors to stop all fraud.

While they do take many precautions, you should plan to perform additional checks after a card processor approves an order. This is also why maintaining your PCI compliance should be a priority.

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

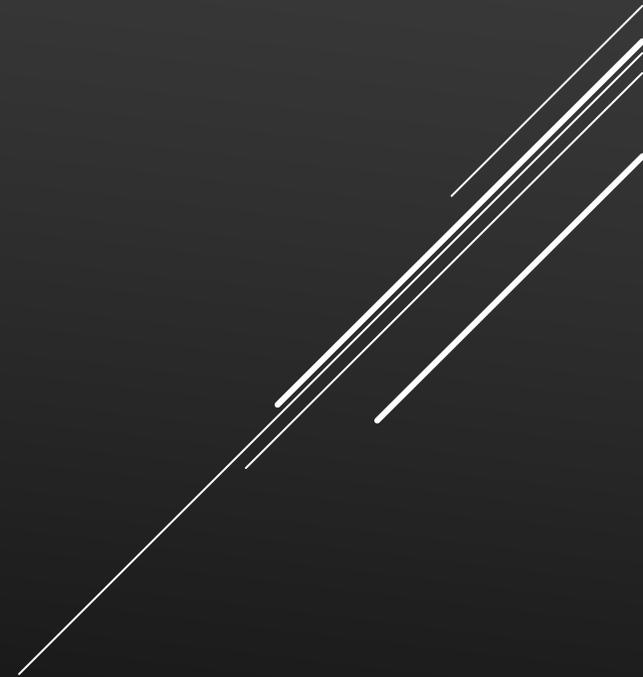
## **2. Watch for strange patterns.**

Watch for orders with an extra-large quantity of a single item or multiple orders to the same address using different credit card numbers. That's especially true if the credit card numbers are very similar, which suggests they may have been stolen from the online source.

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

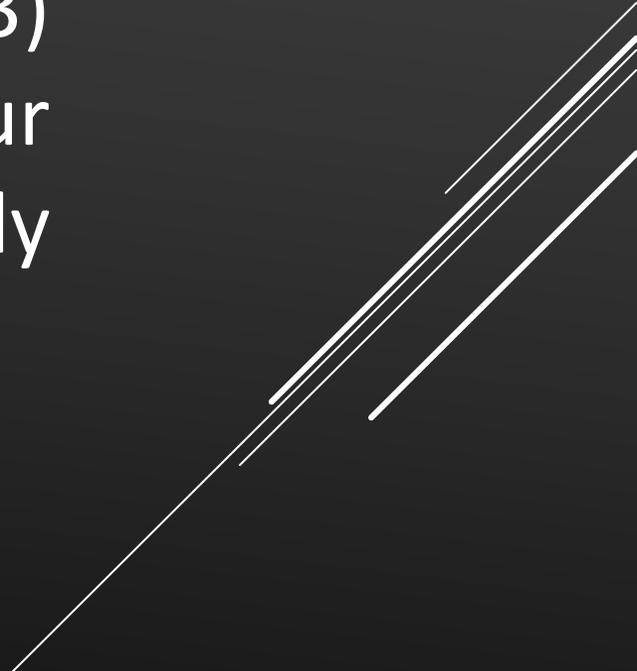
### **3. Consider flagging purchases with different billing and shipping addresses.**

Be wary of shipping to a re-mailing service that might automatically forward your packages. If the billing and shipping addresses differ, you might request phone numbers for both addresses, charge an extra fee to require a delivery signature, or require advance payment by cashier's check or money order.



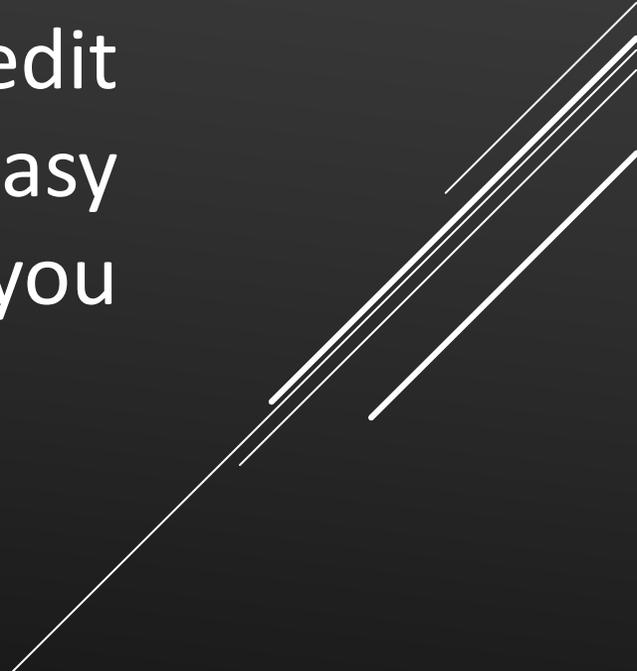
## **4. Address fraud on your website.**

Indicate on your website that you have anti-fraud safeguards in place and will report all fraud to the FBI Internet Crime Complaint Center (IC3) – and then follow through. Also, state on your website that you may contact customers directly if there are any problems with their order.



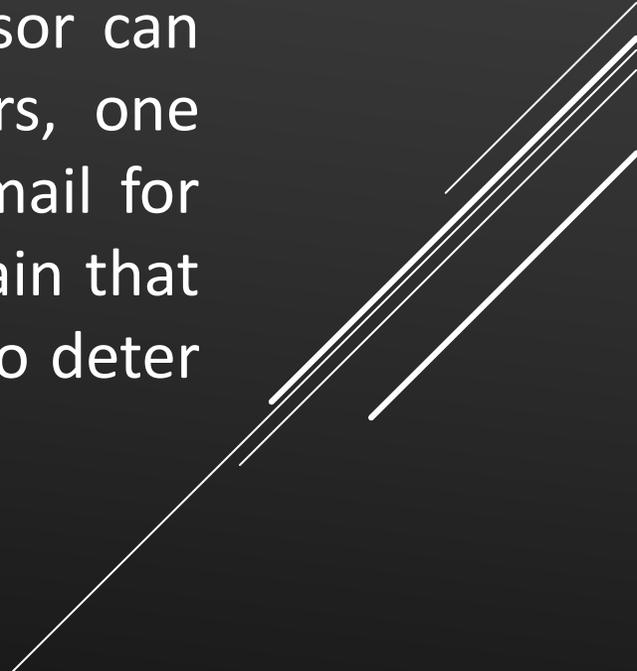
## 5. Call your customer.

Fraudsters rarely share their real telephone number. If you suspect fraud, you can call the cardholder to see if they authorized the charge. If they did not, you can suggest they call their credit card company to report a stolen card. It's an easy call to make and customers will appreciate you taking an extra step to ensure their security.



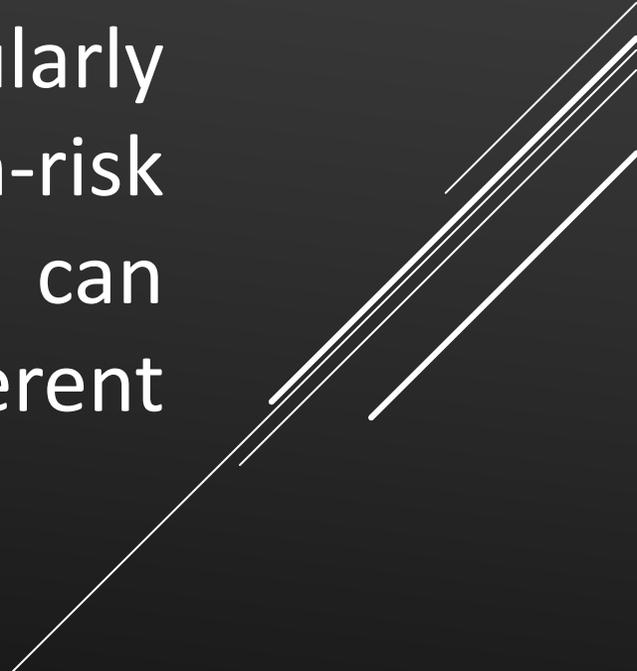
## 6. Develop alternate ordering procedures for international customers.

International sales can be an important part of your business. Because it is difficult to retrieve goods once they have left the country, it's important to have safeguards in place to identify fraud before orders are shipped. Your bank or credit card processor can provide lists of high-risk countries. For international orders, one strategy is to ask customers to contact you by phone or email for shipping costs. Alternately, your 'thank you' page might explain that the purchaser is required to take additional steps like these to deter scammers and safeguard the customers information.



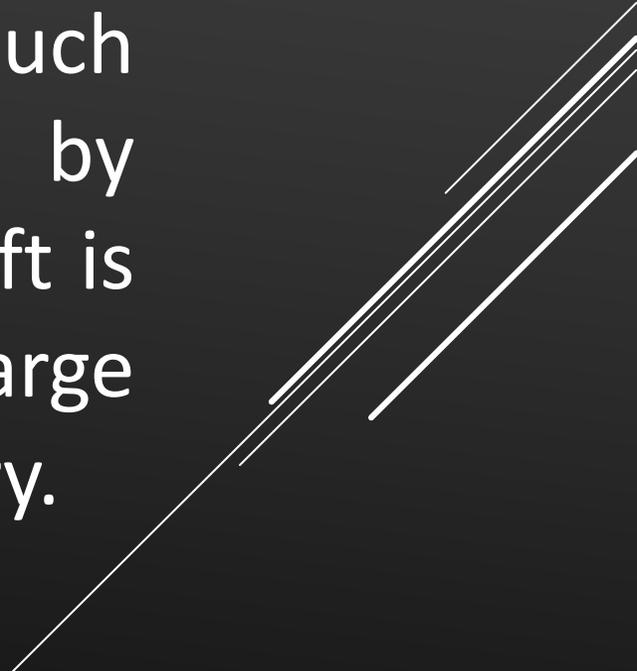
## 7. Develop a fraud-scoring system.

In the U.S., most fraudulent purchases are made between midnight and 2 A.M. Does this mean that a purchase made at 1 A.M. will be by a scammer? No. But if that purchase is also for a particularly high dollar amount or originates from a high-risk country, the chance of fraud increases. You can develop a system that assigns points for different parameters in a transaction.



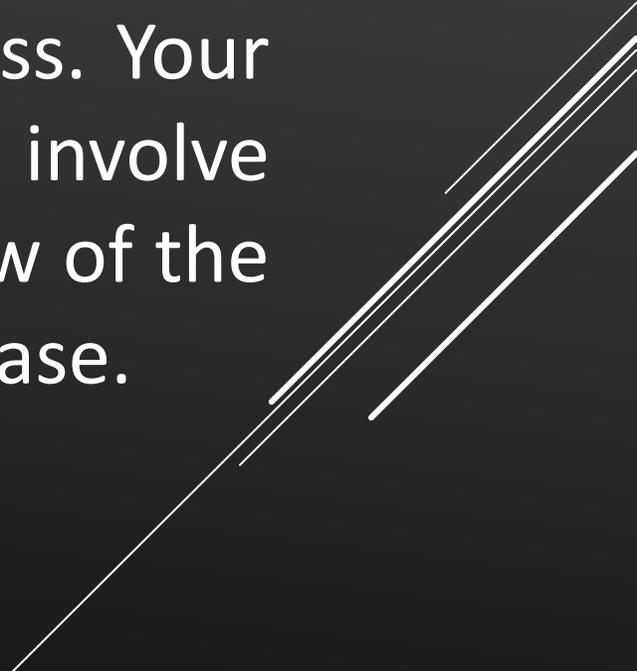
## **8. Implement a delayed shipping policy for suspicious orders.**

An order confirmation email can explain that additional checks or holdovers are sometimes necessary to reduce fraudulent offers. Such notifications may result in order cancelation by fraudsters who know that most credit card theft is reported within 24 hours. Be wary, too, of large orders requiring immediate or overnight delivery.



## 9. Watch for ship-to-store order fraud.

Many online retailers now give their customers the option of having orders shipped to a brick-and-mortar store for pickup. Be aware that fraudsters like this option, given that they don't have to provide a shipping address. Your in-store or curbside pickup process should involve confirming all order information, including a review of the credit card and CVV2 validation used for the purchase.



**THOSE WHO COMMIT CREDIT CARD FRAUD  
PREFER ANONYMITY AND SPEED SO THEY CAN  
GET AWAY WITH THEIR STOLEN GOODS BEFORE  
THEY ARE CAUGHT. YOUR JOB IS TO THWART  
THEIR EFFORTS WHILE NOT FRUSTRATING YOUR  
LEGITIMATE CUSTOMERS. IT'S A DELICATE  
BALANCE, BUT ABSOLUTELY CRITICAL TO YOUR  
SUCCESS.**



# REDUCE THE INHERENT RISK OF FRAUD

- ESTABLISH AND ADHERE TO A BEST PRACTICES CREDIT CARD ACCEPTANCE PROGRAM
- MAKE SURE THAT ALL EMPLOYEES ARE AWARE OF YOUR BEST PRACTICES PROGRAM



# CHECK FRAUD



**NO ONE USES  
CHECKS  
ANY MORE!**



# NO ONE USES CHECKS ANY MORE!

**IT IS TRUE THAT CONSUMERS HAVE MIGRATED TO EPAY AND CREDIT CARDS,  
HOWEVER....**

Businesses in the U.S. still pay half of their bills by check, according to a September survey by the Association for Financial Professionals.

"Businesses know the check system works. It's been around for a long time, and they feel very comfortable with it," said Magnus Carlsson, a manager at the trade group.



# HOW PREVALENT IS CHECK USE TODAY?

THE MOST RECENT FEDERAL RESERVE STATISTICS SHOW THAT PAPER CHECKS WERE AT 17.4 BILLION CHECKS FIVE YEARS AGO, INCREASED TO OVER 20 BILLION CHECKS, AND NOW HAS CONTINUED TO DECLINE TO less than 10 BILLION PAPER CHECKS.



# WHAT IS CHECK FRAUD?

“Check fraud is one of the largest challenges facing businesses and financial institutions. Technology has made it increasingly easy for criminals, either independently or in organized gangs, to create increasingly realistic counterfeit and fictitious checks as well as false id.”

\*Interagency Bank Fraud Working Group for FBI, DOJ, and FDIC



# WHAT IS CHECK FRAUD?

Check Fraud on the Rise Despite Anti-Scam Efforts, ABA Says in a survey of 151 banking institutions.

*"Sometimes, what's old is new again as we've seen criminals gravitate back toward check fraud," said Paul Benda, senior vice president for risk and cybersecurity policy at ABA. "Fortunately, banks are well-equipped to catch this type of fraud and do it successfully day in and day out."*

According to the American Bankers Association, check fraud makes up 60% of all attempted frauds against US deposit accounts, and makes up a full 47% of all successful bank fraud.

# IF I AM A VICTIM OF CHECK FRAUD, THE BANK IS RESPONSIBLE, RIGHT?

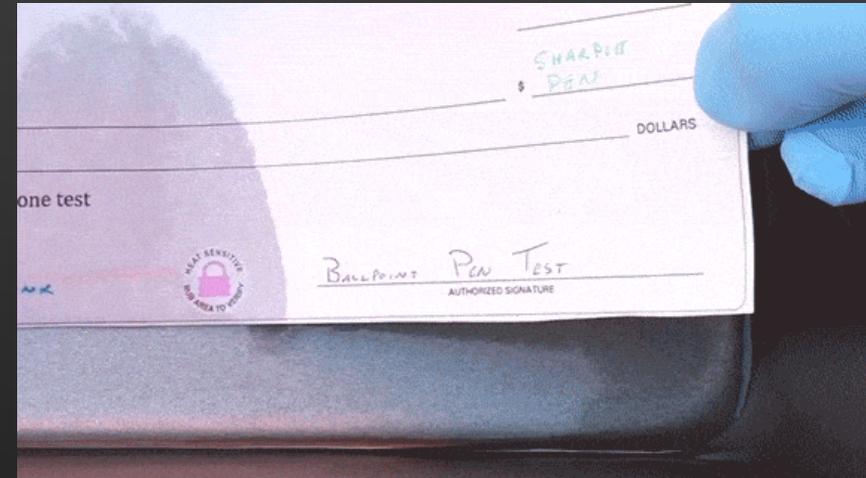
*“It’s important to remember that bank customers are protected against losses. When a customer reports an unauthorized transaction, the bank will take measures to recover the loss and protect the account.”*



# CORPORATE CHECK FRAUD

## CHECK WASHING

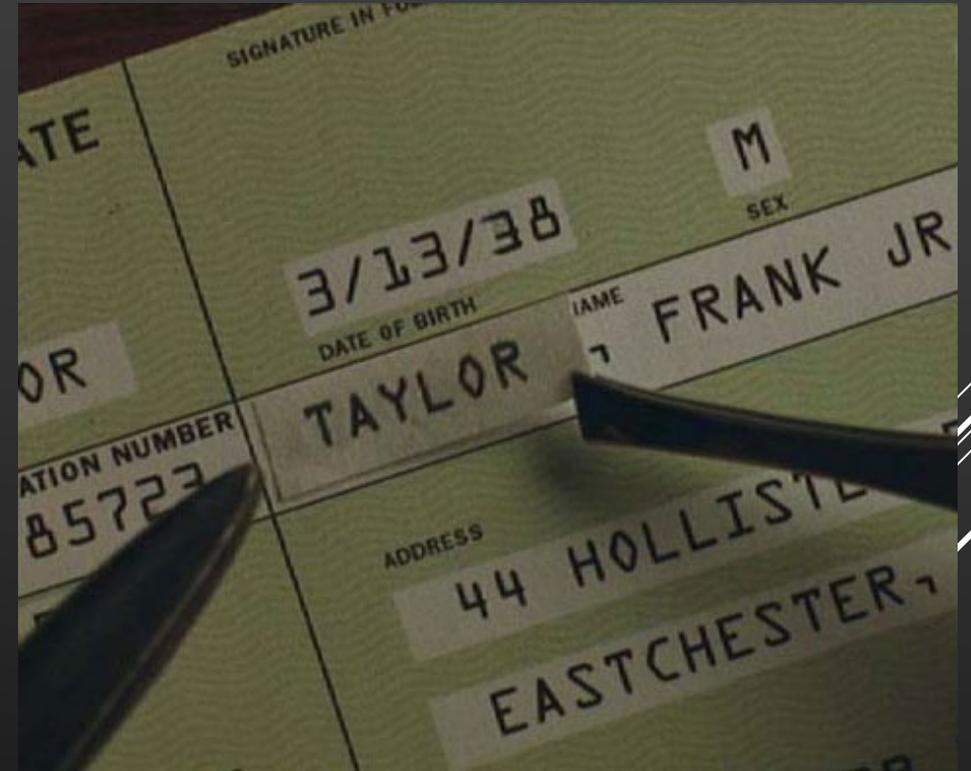
Using a process known as check washing, mail snatchers erase the ink on a check with chemicals found in common household cleaning products or on the shelves of your local Walmart and then rewrite the checks to themselves, increasing the amount payable by hundreds and even thousands of dollars.



# CHECK WASHING

Check washing scams involve changing the payee names and often the dollar amounts on checks and fraudulently depositing them.

According to Terry Barrett, Director of Collections at UTA, “We are seeing less and less check washing and increased printing fraud due to the development of more and more sophisticated equipment available to anyone. It is easier to simply print a fraudulent check and then populate and sign it.”



# PREVENTION METHODS

How do I prevent check washing of my company's checks?



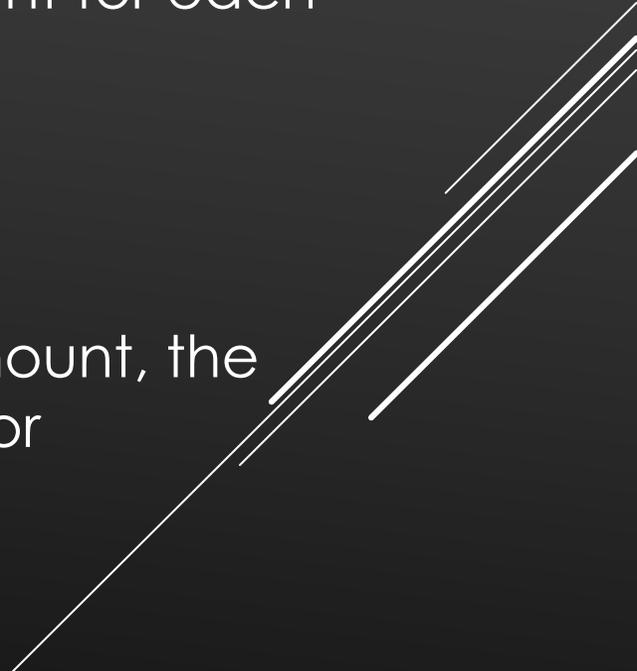
# PREVENTION METHODS

## POSITIVE PAY

For Positive Pay, the Check Issue File from the customer to the bank shall contain a check serial number and exact dollar amount for each check.

## PAYEE POSITIVE PAY

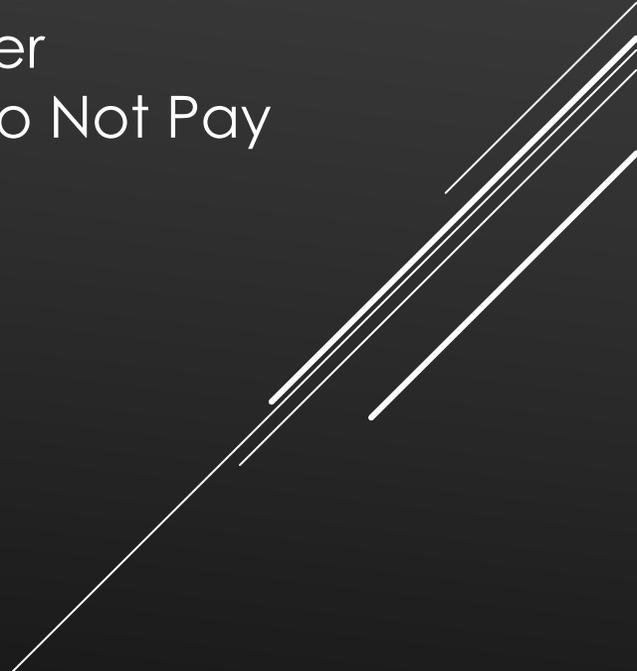
In addition to the check serial number and exact dollar amount, the Payee name will also be provided on the Check Issue File for verification.



# PREVENTION METHODS

## REVERSE POSITIVE PAY

Bank will send Customer a daily check presentment report file (“Presentment Report”). It is Customer’s responsibility to review the Presentment Report and communicate to Bank, in a manner acceptable to Bank, its decision on whether to “Pay” or “Do Not Pay and Return” such checks



# PREVENTION METHODS

Use a paper stock for your checks that cannot be bought in a store or online.

"If your check stock can be bought elsewhere, then your checks can be replicated, no matter how many security features they have. By using unique check stock, you're going a long way to prevent someone from duplicating your checks."

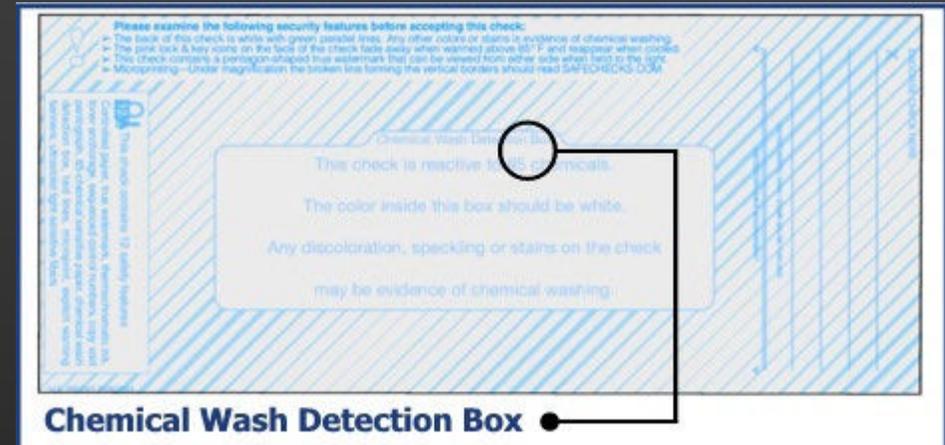
- **Frank Abagnale**, Secure Document Consultant



# PREVENTION METHODS

## Chemically Reactive Paper Protects Against Forgery

Uniquely treated paper, with primary and enhanced alteration indicators, creates stains, spots or discoloration if chemicals are used to alter or wash checks.



## Multi-colored Background Deters Check Copying

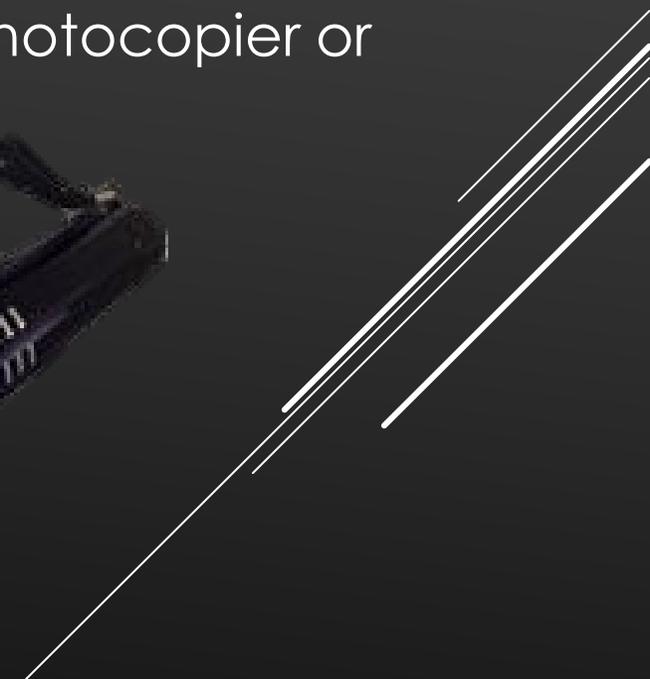
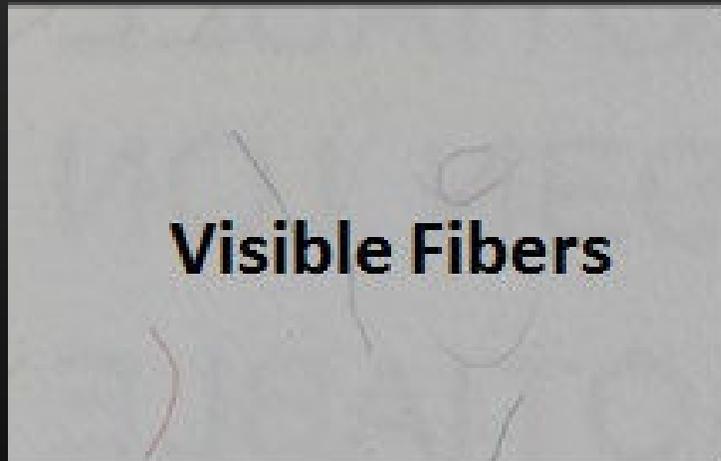
A composited, multi-colored background with subtle gradations that make it difficult to reproduce on a copier.

# PREVENTION METHODS

Use a permanent blue ink for both check writing and signatures

## Visible Fibers Make Counterfeiting Difficult

Arbitrarily placed red and blue fibers of various lengths are visible on both sides of the paper making it difficult to reproduce with a photocopier or scanner.



# PREVENTION METHODS

## **Microprint Makes Counterfeiting Extremely Difficult**

Microprint on front, back and signature lines contains small words in type too small to read with the naked eye and is extremely difficult to reproduce using a photocopier or scanner.

## **Fraud Sensitive Ink Exposes Forgery Attempts**

Ink disappears or turns pink when chemical alterations are attempted.

## **Void Indication Confirms Counterfeiting**

If the check is copied or scanned, the word "VOID" will appear in the warning box on the back.



# PREVENTION METHODS

## **Paper/UV Dull Allows for Check Authentication**

Reduce or eliminates brighteners from the paper, lowering its reflectance properties. Authentication is possible by comparing originals to ordinary copy bond paper.

## **Warning Bands and Boxes Help in Check Authentication**

Warning Bands and Boxes Help in Check Authentication Warning Band on the front and Warning Boxes on the back call out security features, helping the recipient authenticate the check.



# PREVENTION METHODS

## Security Screen Indicates Counterfeit Attempts

The words "Original Document" are printed lightly on back of checks making them difficult to duplicate on a photocopier or scanner. The absence of these words on the back is a red flag that the check is counterfeit.

## Security Weave Exposes Counterfeit Attempts

An intricate, patented background design on back of check in fugitive ink that deters counterfeiting, scanning and copying.



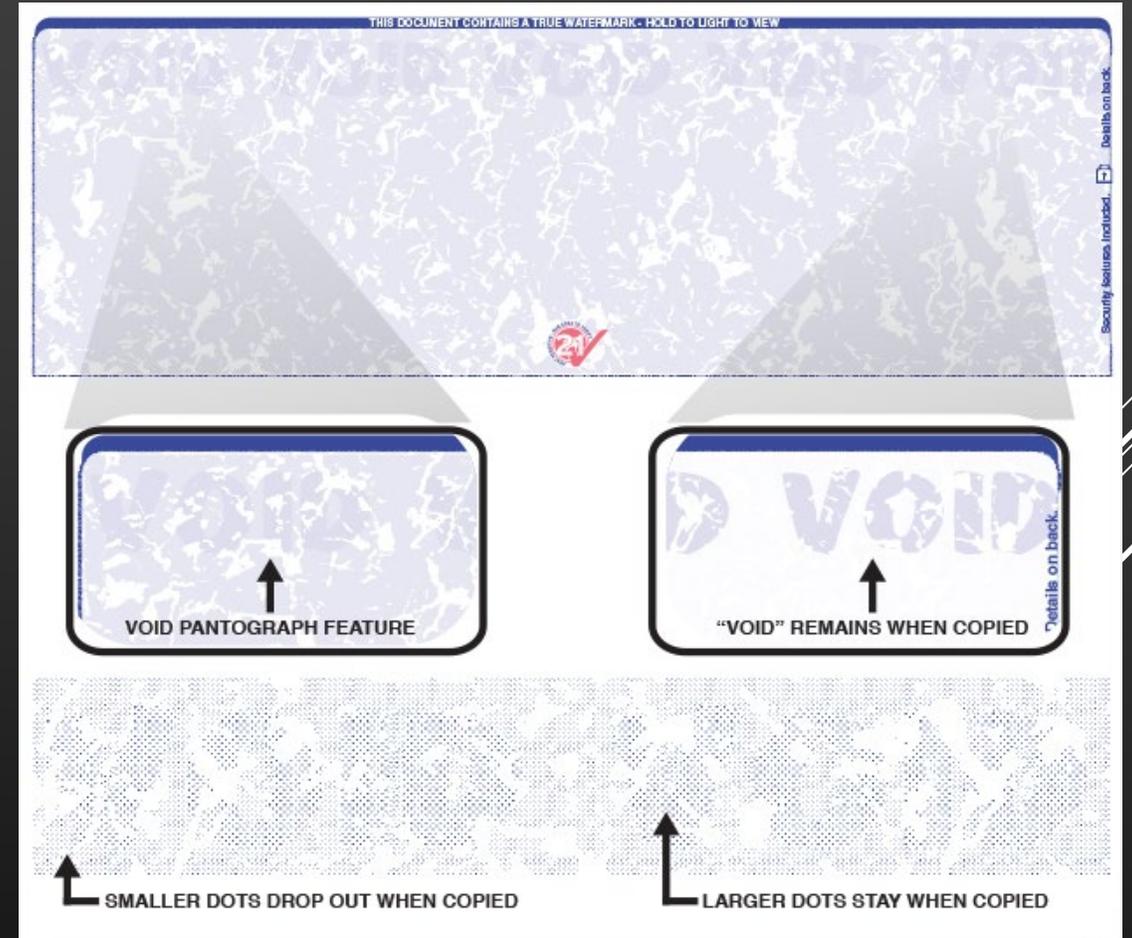
# PREVENTION METHODS

## Prismatic Multi-colored Background Deters Check Copying

A composited, multi-colored background with subtle gradations that make it difficult to reproduce on a copier.

## Void Indication Confirms Counterfeiting

If the check is copied or scanned, the word "VOID" will appear in the warning box on the back.



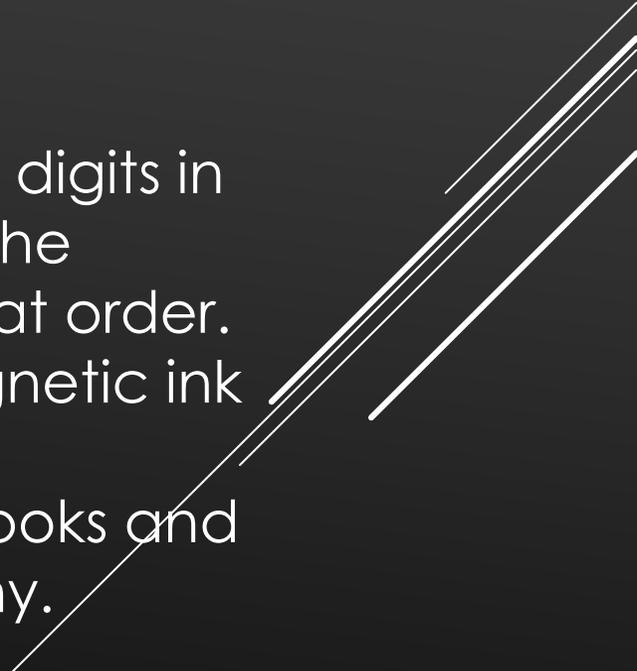
# HOW DOES MY TEAM IDENTIFY A FRAUDULENT CHECK?

1. **Edges:** Most legit checks have at least one perforated or rough edge. If all edges are smooth, the check may have been printed from a personal computer.
  2. **Bank logo:** A fake check often has no bank logo or one that's faded, suggesting it was copied from an online photo or software.
  3. **Bank address:** No street address, just a P.O. box or a wrong ZIP code — which you can check by contacting the issuing bank — indicate a fake check.
- 

# HOW DOES MY TEAM IDENTIFY A FRAUDULENT CHECK?

- 4. Check number:** If there's no check number at the upper right-hand corner, or the number doesn't match the check number in the MICR line, you've got a counterfeit.
  - 5. Amount:** Usually it's less than \$5,000 because federal rules require that deposits of that size be made available to you within five days. This can trick you into thinking that the check has cleared. Deposits of \$5,000 or more are subject to longer holding periods.
  - 6. Paper:** Fake checks are often lighter than the paper stock used for authentic checks. They also may feel slippery.
- 

# HOW DOES MY TEAM IDENTIFY A FRAUDULENT CHECK?

- 7. Signature:** Stains or gaps around signatures, a digitized appearance, or many up and down pen strokes indicate the payer's John Hancock was printed from a scanned original or was forged.
  - 8. MICR line:** The bottom of every real check has a series of digits in an unusual font, representing the bank routing number, the account number and the check number, generally in that order. That special font is known as MICR, which stands for magnetic ink character recognition. These numbers can be read by specialized check-sorting machines. Real magnetic ink looks and feels dull to the touch. Fake MICR numbers are often shiny.
- 

# HOW DOES MY TEAM IDENTIFY A FRAUDULENT CHECK?

9. **Routing number:** Typically, the first nine digits of the MICR line make up the routing number, which identifies which bank issued the check. A check with no routing number or with fewer — or more — than nine digits is clearly a fake. You can verify routing numbers by going to the Federal Reserve Financial Services website.
  10. **Misspellings**
  11. **Shiny MICR numbers** real MICR ink tends to look dull
  12. **Missing signatures**
  13. **Up and down pen strokes** associated with forged signatures
- 

# OUTSIDE SERVICES FOR YOUR PROTECTION

- Positive Pay
  - Specialty Check Printers
  - Ach Block/Positive Pay
  - Customer Facing Secure Environment
  - Check Guarantee
  - Ach With Guaranteed Settlement
- 

# PERSONAL CHECK FRAUD AND SCAM PROTECTION

It's estimated that as many as 500,000 Americans were burned by fake check scams last year, with the average victim losing about \$1,200, according to a new report from the Better Business Bureau.



# PERSONAL CHECK FRAUD PROTECTION FOR STUDENTS

## Scammers are targeting college students.

A scammer posing as a professor sends you an email. It uses a college domain name and a format like your.name@collegename.edu. The scammer offers you a part-time job, like personal assistant or dog walker. Then, the scammer sends you a check, asks you to deposit it, send some of the money to someone else, and keep the rest as payment.

A while later, the bank realizes the check was fake and deducts the original check amount from your account. So, if you deposited a \$1,000 check, they'll take that back. But if you sent \$400 to someone else, you're now out \$400 of your own money.

# PERSONAL CHECK FRAUD PROTECTION FOR ELDERLY

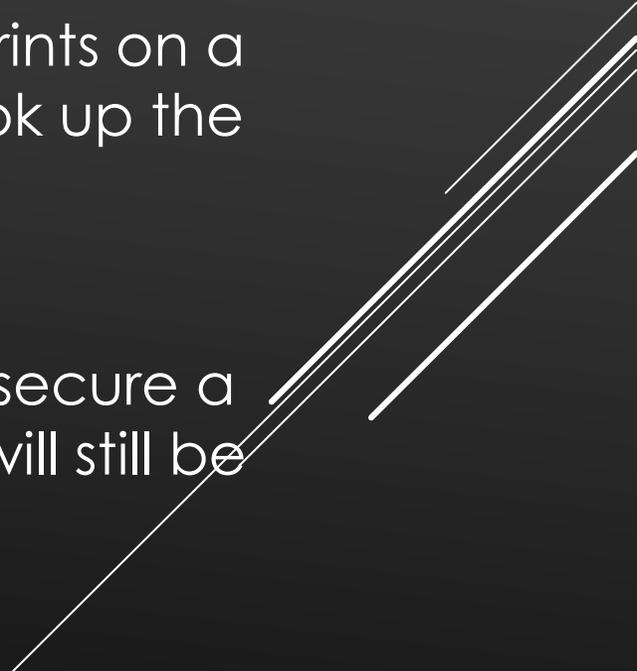
## Why do scammers target the elderly?

- They have money
- They are more trusting
- They have memory or health problems

## Top Three Elderly Scams

- SOCIAL SECURITY SCAM
  - MEDICARE SCAM
  - LOTTERY SCAM
- 

# HOW DO I PROTECT MY FAMILY FROM CHECK FRAUD AND SCAMS?

- Don't accept a check that's made out for more than the price of the item or service you're selling. Insist that the buyer make out a new one for the correct amount.
  - Don't rely on a phone number for a bank that a seller prints on a check. If you want to call to authenticate the payment, look up the bank's number on its official website.
  - Don't wire money to people you don't know.
  - Don't give in to pressure to move fast on a payment to secure a job or supposed financial windfall. If a deal is legitimate, it will still be available after the check clears.
- 

# CHECK GUARANTEE

THE ULTIMATE DEFENSE AGAINST FRAUD AND ANY RETURNED CHECK

## THE UTA BENEFIT PACKAGE

- No equipment required
  - No mandatory usage
  - No minimum monthly fees
  - Pay only for the checks you actually guarantee
  - No-deductible Stopped payment coverage for members
  - No contract term
  - No additional charge for multiple locations
  - Dedicated Customer Service Manager
- 