Detect and Prevent Fraud

Presented by:

Barry Jeide
VP, Relationship Manager
Phone: (406) 624-4476 / email: barry.Jeide@usbank.com

Jason Euell
VP, Relationship Manager
Phone: (406) 657-8088 / email: Jason.Euell@usbank.com

Amanda Caillouet
VP, Treasury and Payments Consultant
Phone: (503) 367-7069 / email: Amanda.Caillouet@usbank.com

A look at the cost of fraud and payment exceptions

Business email compromise

21,489 BEC/EAC complaints were made to the FBI IC3 in 2023 with adjusted losses over $2.9 billion.[1]

Identity theft

There were 19,778 victims tracked by the IC3 in 2023 with over $126 million in losses reported.[1]

80% of organizations surveyed

experienced attempted and/or actual payments fraud in 2023.[2]

Sources:
1. FBI Internet Crime Complaint Center – Internet Crime Report 2023: 2023_IC3Report.pdf
2. 2024 AFP Payments Fraud and Control Survey Report: https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud/
See end disclosures.

How fraud impacts us

Check continues to be the payment method most impacted by fraud at 66%.

Restitution is unlikely

Recovery may be possible

Prevention is the best option

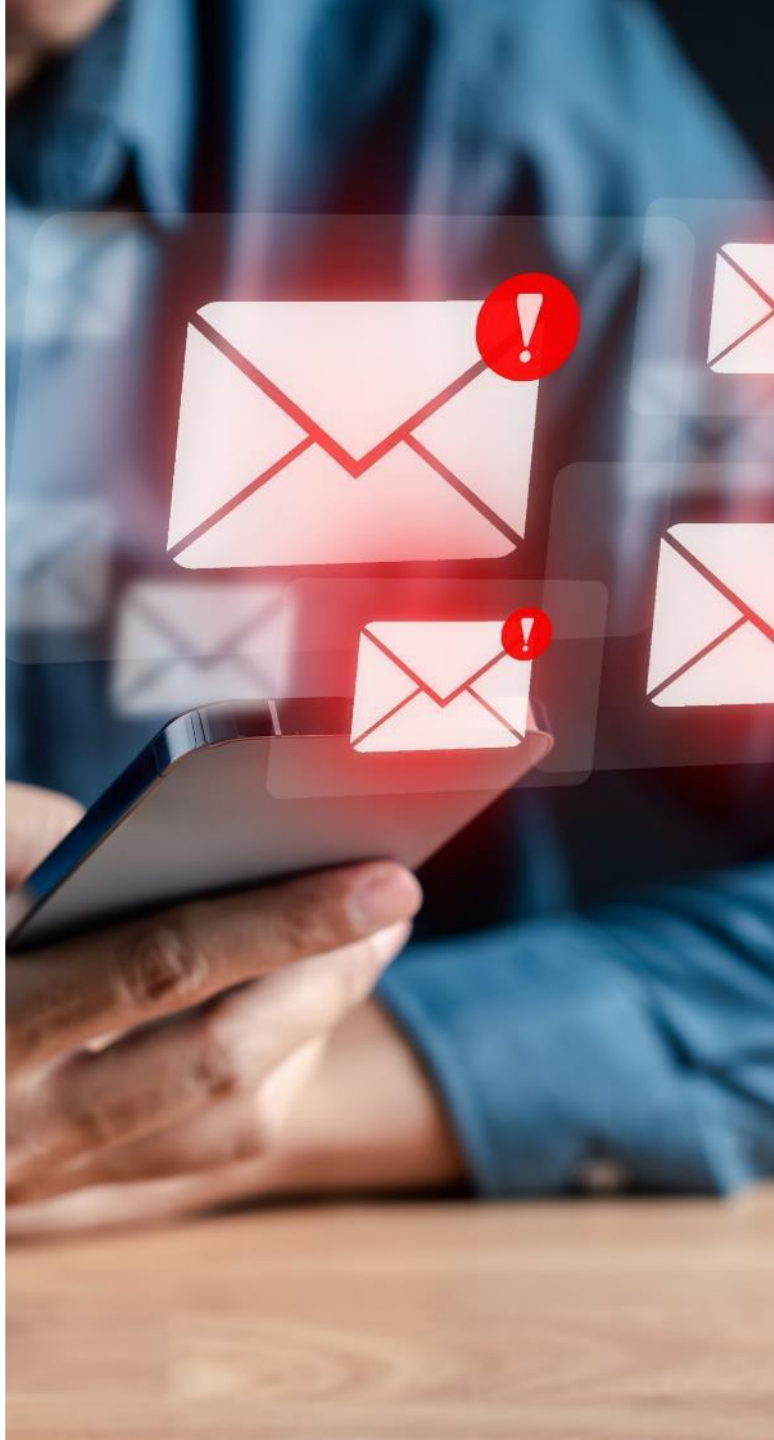
See end disclosures.

Top sources of attempted/actual fraud

Percent of organizations

Business Email Compromise (BEC)	62%
Individual external to the organization using tactics other than email	49%
Vendor imposter	45%
Invoice fraud	24%
U.S. Postal Service office interference	23%
Imposter to a client posing as representative from your company	14%
Third-party or outsourcer (i.e., vendor, professional services provider, etc.)	12%
Account takeover (i.e., hacking a system, malicious code, etc.)	12%
Compromised mobile device due to spoof/spam text or call	8%
Organized crime ring (i.e., crime spree that targets multiple organizations)	7%
Deep-fake attempt (i.e., voice, vishing, etc.)	5%

Source: 2025 AFP® Payments Fraud and Control Survey Report
https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud



Payment fraud

What is it?

Movement of funds initiated under fraudulent pretenses (i.e., ACH, wire transfer, Real Time Payments (RTP).

How is it perpetrated?

Most often, corporate customers are asked to process payments or change existing payment instructions due to social engineering, business email compromise (BEC), vendor email compromise (VEC, or email account takeover (ATO)

U.S. Postal Service

Stolen check transaction lifecycle

1. Client creates and mails check.
2. Check is stolen from the mail.
3. Check is posted for sale online.
4. Check is purchased by threat actor.
5. Threat actor attempts to obtain funds.

Types of check fraud

Check signature and endorsement forgery	Check alteration	Check counterfeiting	Embezzlement
• Fraudsters forge either the authorized signature on the face of the check or the endorsement on the back	• Fraudsters obtain and alter checks and negotiate them for personal gain • Methods include: – Check washing, scraping and erasure – Inserting new payee – Adding letters, words or numbers	• Fraudsters create a completely bogus check • Often resembles the actual check, but sometimes not at all (except for the account, routing and transit numbers) • Payee options – Shell company – Cash – Accomplice – Vendor (for personal purchases)	• Maker will exploit lack of controls, prepare check, sign it and convert it for personal gain • Payee options: – Maker – Shell company – Cash – Accomplice – Vendor (for personal purchases)

See end disclosures.

Vendor Email Compromise

The difference between BEC and VEC

While traditional BEC attacks usually claim to be from a trusted individual within the organization, VEC goes one step further: it impersonates vendors (or other trusted third parties) to trick the target into paying fraudulent invoices, disclosing sensitive data or granting access to corporate networks and systems.

Research

Cyber actor conducts open-source research on awarded and ongoing projects and companies.

Domain registration

Cyber actor creates a spoofed domain like the legitimate company.

Vendor Email Compromise (VEC)

Cyber actor sends an email to a customer of the legitimate company requesting a change to the ACH payment or direct deposit information.

Information change

Customer believes the email is legitimate and changes banking information.

Transfer

Customer transfers money to new account and the cyber actor receives the money.

See end disclosures.

Ransomware event

What is ransomware?

Ransomware is a type of malware, or software used to disrupt computer operation, gather information, or gain private access. It restricts access to a system or encrypts sensitive data preventing organizations from conducting business. Often, the system can be unlocked after a ransom is paid.

How does U.S. Bank become aware?

- Dark web monitoring
- News review
- Customer notification

What to do next?

- Work with your financial institution
- Report event to the FBI
- Employ reputable cyber-forensic firm

What is Artificial Intelligence (AI)?

What is AI?

The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

What can it be used for?

From self-driving cars to generative AI tools like ChatGPT, AI is transforming the way we live and work.

AI can be used as:

1. AI generated text
2. AI generated images
3. AI generated audio (aka voice cloning)
4. AI generated videos (aka deepfakes)

AI-based threats are growing, especially in their speed, volume and sophistication.

See end disclosures.

AI and Deepfakes

Be aware and use protective best practices

Use a secret word	Never share sensitive information	Do not send money or gifts	Listen closely to voices
Create a secret word or phrase with your family to verify their identity.	Never share sensitive information with people you have met only online or over the phone.	Do not send money, gift cards, cryptocurrency, or other assets to people you do not know.	Listen closely to the tone and word choice to distinguish between a legitimate caller and an AI-generated one.

Subtle imperfections	Limit online content	Verify caller's identity
Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic teeth or eyes, indistinct or irregular faces.	If possible, limit online content of your image or voice, make social media accounts private, and limit followers to people you know.	Verify the identity of the person calling you by hanging up the phone, researching the contact of the bank or organization purporting to call you, and call the phone number directly.

See end disclosures.

What you can do to protect your organization from fraud

Bolster your internal controls

- Ensure separation of duties
  - Check writers should not reconcile the accounts
  - Delegate separate individuals for invoicing, collecting and posting funds to accounts receivable
- Establish and document policies for all accounting functions
- Update and review procedures with your employees
- Conduct periodic reviews of procedures
- Reconcile your accounts in a timely manner
  - Notify the bank immediately if fraud is suspected
    - Normally a bank gives a time limit of 15 or 30 days
  - Use online information reporting prior to the arrival of your statement(s)
- Check background references when hiring
- Use appropriate bank solutions
- Add payee verification to your positive pay service

See end disclosures.

Use electronic payment alternatives

- Transition your employees to direct deposit or pay cards
- Use ACH credits to replace checks for your primary vendors
  - Use dual controls for payment initiation and payment approval
- Consider using card-based payments
  - Purchasing, T&E and fleet expenses
- Review outsourced services
  - Check Payables (check outsourcing)

See end disclosures.

Control check stock

- Control the storage and distribution of your check stock
  - Keep in locked quarters
  - Seal boxes
  - Maintain an inventory list
  - Conduct audits
- Secure mechanical signature plates separate from check stock
- Keep check stock consistent
- Consider outsourcing your check payments process to eliminate in-house paper check storage and printing

See end disclosures.

Use bank fraud prevention services

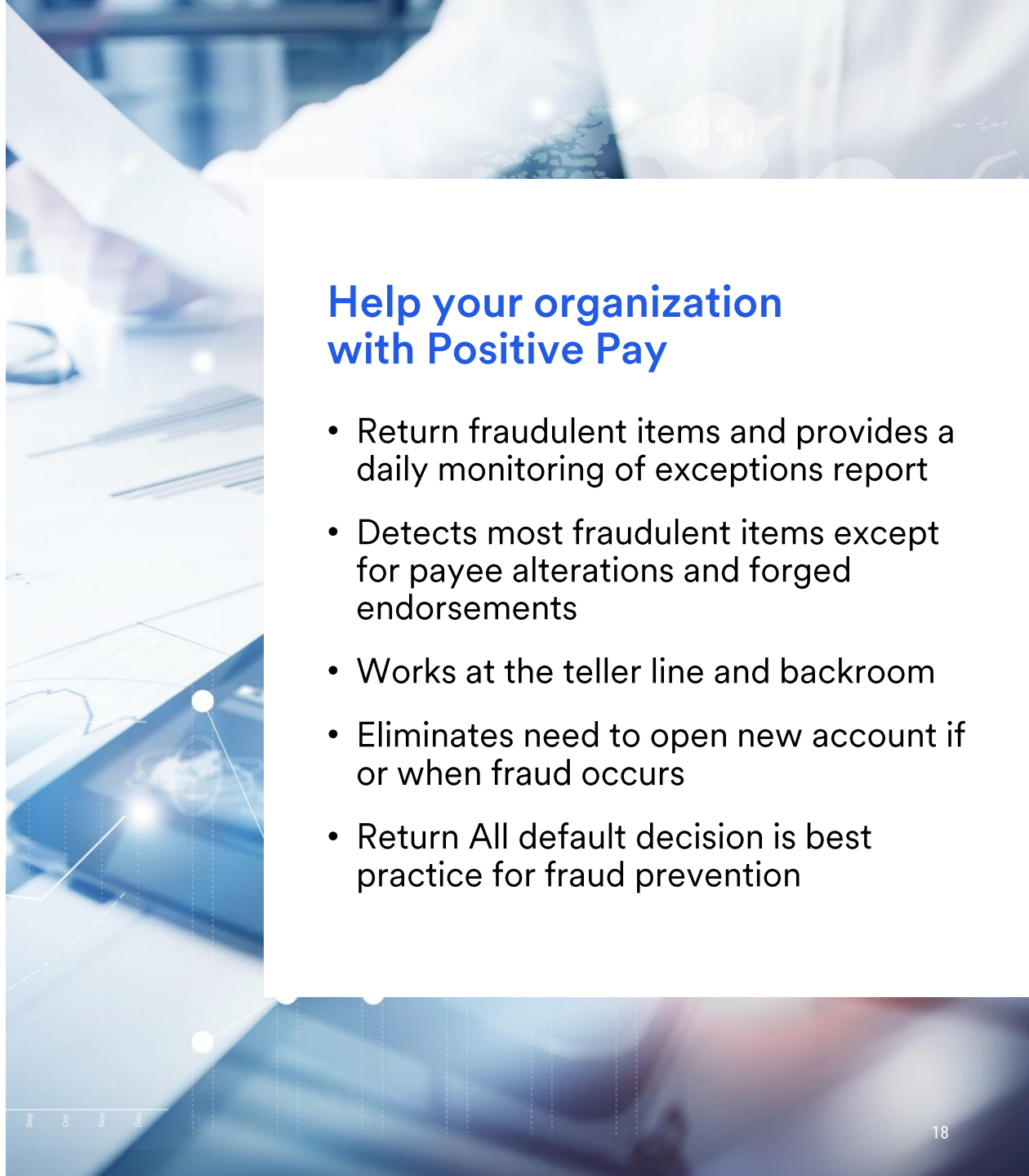
- Positive pay
  - Payee verification
- Check blocks and filters
- ACH positive pay
- ACH blocks and filters
- Universal Payment Identification Codes (UPIC)
- Electronic alternatives
- Account Validation Services

Key Takeaways

- **Identify adversaries and understand their motivations**
- **Think like a threat actor**
  - What makes your organization attractive to adversaries?
  - What are your high, medium, and low value targets?
  - Have you defined your attack surface and mapped controls to it?
- **Approach disruption by shifting from an organization-centric (inside out) to industry-wide (outside in) view**
  - Cultivate relationships and collaborate fully with industry peers and other partners
  - Lean on your bank
- **Build your own blueprint**
  - Develop and maintain a view of your ever-evolving threat landscape
  - Formulate your defense strategy based on a comprehensive view of your threats

Use Positive Pay

- The best tool to detect counterfeits, forgeries and dollar amount alterations on your account
- How it works
  - Send issued check file to bank each time you disburse checks
  - If a check clears that isn't on the file, we report the exception via positive pay
  - You review exceptions and make payment decisions



Help your organization with Positive Pay

- Return fraudulent items and provides a daily monitoring of exceptions report
- Detects most fraudulent items except for payee alterations and forged endorsements
- Works at the teller line and backroom
- Eliminates need to open new account if or when fraud occurs
- Return All default decision is best practice for fraud prevention

See end disclosures.

Add Payee Verification to your Positive Pay

- An enhancement to positive pay that detects alterations to payee names on the check
- May require checks are printed according to specific bank guidelines
- May require changes to the issue file

Discover the benefits

- Allows you to return fraudulent items, provided you monitor your exceptions report daily
- Works at the teller line and backroom
- Helps stop payee alterations and counterfeit checks with bogus payees

See end disclosures.

How Account Validation helps prevent fraud

Verify account information before sending payments.

Get real-time responses for any account-based transaction, including ACH, wire, RTP® payments and checks.

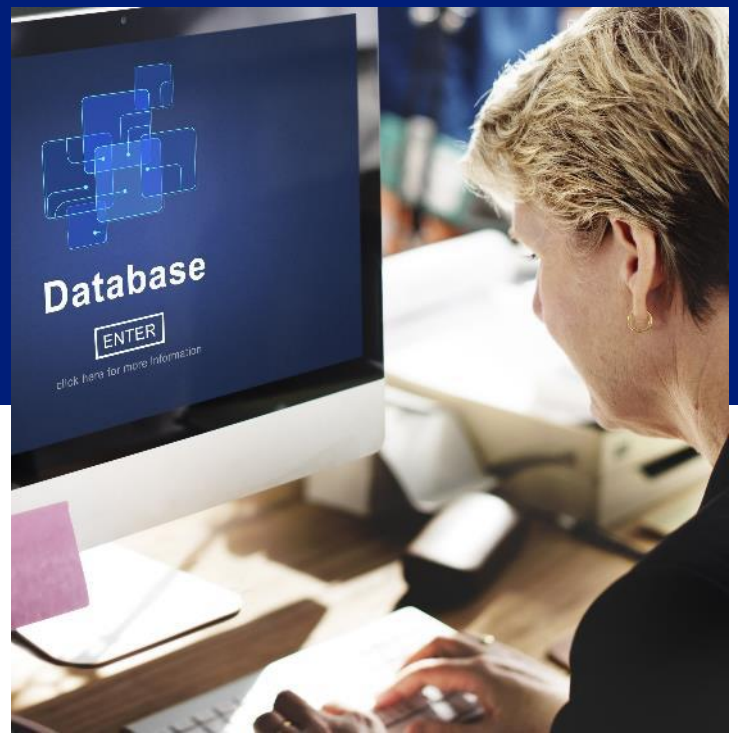
Avoid the hassle and cost of rejected transactions.

Mitigate risk

Reduce financial loss

Minimize cost of exceptions

See end disclosures.



Get the data needed to make educated decisions

Before you pay

Confirm account status and registered account owner.

Rely on a trusted source

Account validation connects you to a secure national shared database of checking and savings accounts formed by thousands of trusted financial institutions as your source for verification.

Use account validation with:

- ACH
- Check deposits
- Wire
- RTP® transactions

See end disclosures.

ACH fraud prevention services

ACH Block	ACH Filter	ACH Positive Pay	Universal Payment Identification Code
• Block all ACH debits and/or credits to an account	• Designate authorized ACH transactions and block the rest	• Create authorizations for automated posting of received transactions in SinglePoint • Review and decide to pay or return new transactions (exceptions) • Receive notification receipt of new transactions	• Receive ACH credit payments without revealing your bank account number • Give a unique remittance number that maps to your account

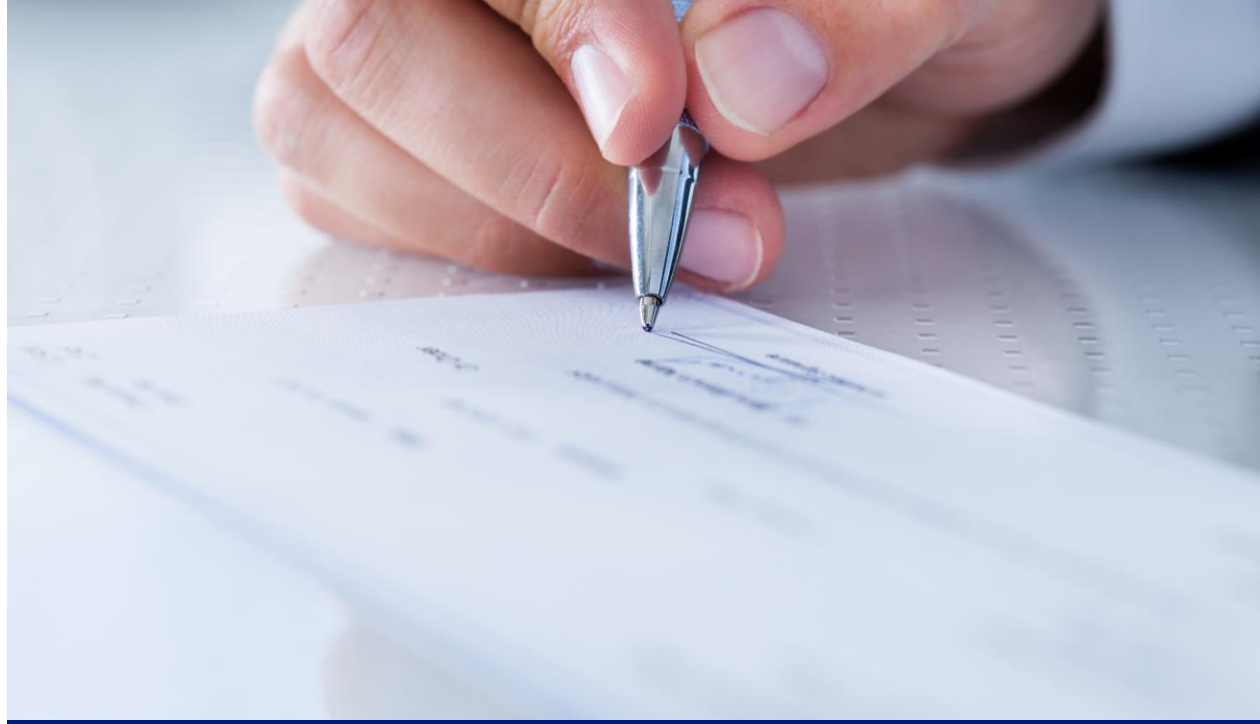
See end disclosures.

Case study: File 1

A newly hired bookkeeper was given authority to sign checks and originate payroll through ACH.

No one approved her work or reconciled bank statements.

The employee was a convicted check forger who transferred $2 million to her account over several years.



Solution:

Conduct a criminal background check for employees handling payroll. Internal controls and timely reconciliation of accounts would have detected fraud earlier.

See end disclosures.

Case study: File 2

An organization experienced check and ACH fraud and quickly closed accounts.

The bank recommended separate accounts for check writing and ACH.

Positive pay was placed on the check writing accounts.

Check and ACH filters were placed on the electronic-only accounts.

Within 30 days, losses were avoided.

Solution:

Separate payments by account and apply the appropriate bank solution.

See end disclosures.

Case study: File 3

After experiencing check fraud, an organization adopted positive pay.

After a time with no losses, they discontinued positive pay believing their internal controls would detect fraud.

Soon, check fraud attempts were detected by bank tellers.

Before positive pay was fully reinstated, check losses of $100,000 were experienced.

Solution:

Consistently maintain positive pay on accounts issuing checks.

See end disclosures.

Case study: File 4

On a positive pay account, large numbers of checks suddenly appeared as exceptions.

From viewing check images, they discovered their account was used in a bogus lottery scheme.

The timely return of exception items avoided losses of $1 million.

Solution:

Positive pay and timely reconciliation prevented a loss of $1 million.

See end disclosures.

Disclosures

Deposit products offered by U.S. Bank National Association. Member FDIC. Products and services may be subject to credit approval. Eligibility requirements, restrictions and fees may apply.

U.S. Bank and SinglePoint are registered trademarks of U.S. Bank National Association.

This information has been obtained from sources believed to be reliable but is not guaranteed as to accuracy or completeness. It is not intended to be a forecast of future events or a guarantee of future results, nor is it intended to serve as a recommendation or solicitation for the purchase or sale of any particular product or service. It does not constitute advice and is issued without regard to any particular objective or the financial situation of any particular individual.