TREASURY SERVICES



Fraud protection playbook

BOK FINANCIAL®

Contents

Check fraud

ACH fraud

Wire transfer fraud

Business Email Compromise (BEC)

Ransomware

Fraud protection

BOK Financial fraud protection services



A recent survey found that 79% of organizations were victims of attempted or actual payments fraud activity in 2025. Fraudsters often target businesses because they know there is an ongoing cash flow, and a fraud attempt may go unnoticed by untrained staff. Therefore, companies must take a proactive approach to prevent costly issues.

"For businesses, it's not a matter of 'if', but 'when' these days," said Linda Marcum, director of treasury sales enablement at BOK Financial®, adding that companies need to be prepared for the inevitable because, at some point, a fraudster will try to steal data, information or money from you.

The first step is to be aware of the types of fraud to look for.

> **"For businesses, it's not a matter of 'if', but 'when' these days.**
>
> Linda Marcum
> **Director of treasury sales enablement at BOK Financial**

Check fraud

Businesses that still use and process paper checks are highly susceptible to check fraud. Criminals can create compromised checks in multiple ways to change the payee or amount.

According to Nasdaq's 2025 Global Financial Crime Report check fraud resulted in $21 billion in losses in the Americas.

Examples of check fraud

Forged: Criminals steal checks, filling in the payee and amounts with a forged signature that appears legitimate. The check is then cashed.

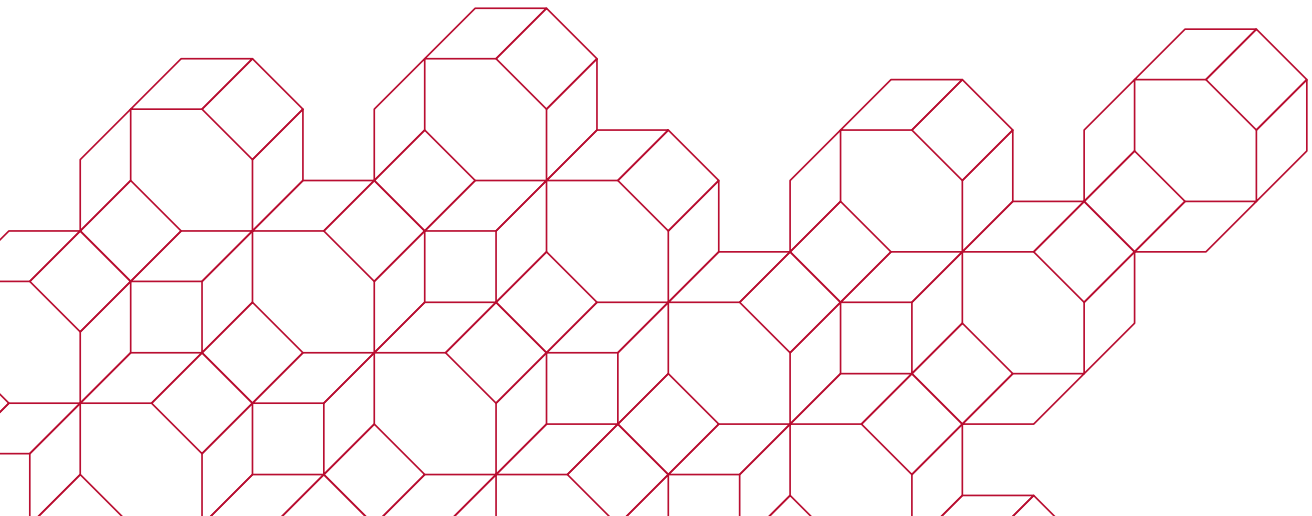
Counterfeit: Bank account information is stolen through security breaches, on the dark web or via a stolen check from the mail or pulled from the garbage. Information such as account numbers are then used to create fake checks using graphic design programs and printers. In some cases, stolen checks are scanned and then digitally manipulated to add/replace a payee and amount, known as "check cooking."

Altered: Also known as "check washing," this process uses chemical substances to remove payee and amount information on the check and leaving the signature intact. The check is then rewritten with a new payee and a higher amount benefiting the criminal, and deposited into their own or a controlled account.

Paperhanging: Fraudsters write or reorder checks on closed or overdrawn accounts. These accounts could be their own or those of other people. The check is used for a payment and the fraudster disappears before the recipient tries to cash it and discovers it won't clear, known as "float time."

Uniform Commercial Code

Not only is it good business practice to be educated on existing fraud schemes, the Uniform Commercial Code (UCC) dictates that businesses must follow clear guidelines for check transactions and determine who is responsible, how losses are allocated and how disputes are resolved. For example, if a bank offers security features that could have prevented a specific case of fraud and the business did not implement these features, the bank can claim the business customer was negligent and therefore partially liable for a fraud loss.





Preventing check fraud

To avoid check fraud, businesses can adhere to best practices.

- **Use secure checks:** Order checks from reputable sources and keep them in secure storage. Consider advanced security features, such as watermarks, chemical voids and microprinting that make counterfeiting or altering checks more difficult.
- **Use permanent ink:** Use indelible ink that is difficult for fraudsters to "wash" off with chemicals.
- **Mail within post offices:** Mail all checks inside the post office to avoid having them sit in an unattended mailbox. For receiving checks in the mail, don't let them sit in your mailbox or a basket in the office. Consider a locked mailbox and keep track of who has a key. According to the U.S. Postal Service Office of Inspector General, mail and package theft continues to rise nationwide, with at least 58 million mail and packages stolen in 2024, creating significant exposure for check fraud and financial loss.
- **Shred documents:** Destroy voided/canceled checks, deposit slips immediately after use with a cross-cut shredder. Do not throw them in the trash.
- **Verify payment:** Never release goods or services until funds supplied by check have fully cleared. Be suspicious of checks that are more than the agreed-upon amount as fraudsters use this to ask for money back on a counterfeit check.
- **Go digital:** Switch to more secure electronic payment methods instead of paper checks, such as Automated Clearing House (ACH) payments, wire transfers or online bill pay.

It's important to be vigilant on check fraud. "There's a low barrier to entry for a fraudster to set up a counterfeit check ring, which makes it a popular crime. It only takes about $400 to buy the equipment and stolen checks sold on fraud forums," said Scott Edwards, director of fraud risk management at BOK Financial.

Employee handling of checks

Establish a division of responsibility to make it difficult for employees to tamper with checks and payments. For instance, ensure that the person responsible for account reconciliation is not also authorized to issue checks, thereby preventing the ability to cover fraudulent activity.

ACH fraud

ACH (Automated Clearing House) transactions are electronic fund transfers (EFTs) commonly used for scheduled payments. Payments remain in the ACH network until cleared and deposited into the designated accounts. Because of this processing period, increased risk of exposure to fraudulent activities can happen when fraudsters exploit the time lag between initiation and settlement to redirect or withdraw money before detection.

Examples of ACH fraud

- The criminal gains access to a commercial customer's login credentials, creates a fraudulent ACH file in the originator's name and quickly withdraws funds before the fraud is detected.
- An employee of a company or bank modifies ACH files to steal money.
- A criminal sends funds back and forth between bank accounts at separate banks to take advantage of the time lag in transactions and withdraw funds that are not legitimate.
- An employee with authorization for ACH transactions falls victim to a phishing email that leads to an infected site, which installs keylogging software to obtain authentication credentials. This enables the criminal to impersonate the company's authorized representative and withdraw funds.



Preventing ACH fraud

Businesses can avoid falling victim to ACH fraud by following best practices, such as:

- Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Be suspicious of emails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack the computer.

Wire transfer fraud

Wire fraud typically occurs when a fraudster uses electronic communication to trick a business employee into sending money or sensitive information to a fraudulent account. Since transfers are immediate, they often can't be recovered, so the business will suffer a loss.

Examples of wire fraud

For example, a scammer might impersonate a company executive and instruct an employee to urgently wire funds to a fake vendor, or pose as a trusted supplier with changed payment details. In other cases, fraudsters may intercept legitimate invoices and alter the bank account information.



Preventing wire fraud

Businesses can put multiple safeguards in place to prevent wire fraud.

Verify wire instructions

- Always confirm wiring instructions by calling the requesting party directly, using a phone number you already have on file - not one provided in an email or message.
- Never wire funds to unknown recipients.

Be alert to Urgency Tactics

- Be wary of requests that pressure you to act immediately. Fraudsters often create a sense or urgency to prevent careful review.

Implement dual controls

- Require at least two authorized individuals to approve all wire transfers.
- Use standardized verification processes for each transaction.

Secure account information

- Never send account information via unencrypted email.
- Use encrypted email or secure drop boxes to share sensitive details.

Educate employees

- Provide regular training on fraud schemes and how to recognize red flags.

Set up bank account safeguards

- Enable alerts to detect suspicious activity.

Establish daily limits on wire transfer amounts.

Report suspicious activity promptly

- Contact your bank immediately if you notice suspicious transactions. Quick action is critical, as there may be a brief window to reverse fraudulent activity.

Business Email Compromise (BEC)

Businesses use email every day. Untrained employees are particularly vulnerable to BEC, as attackers use social engineering to impersonate trusted individuals, other employees, or vendors, requesting sensitive information to gain access to company systems, make fraudulent fund transfers, or steal confidential data. Fraudsters often use artificial intelligence to create spoof emails and even monitor and intercept existing emails to continue ongoing conversations, so the victim isn't suspicious of the request.

"We're seeing a significant rise in intelligent—and believable—AI-generated scams targeted at not only individuals, but also businesses and financial institutions to try and gain access to critical financial information," said Paul Tucker, chief information security and privacy officer at BOK Financial.

Red flags to watch for

- Attackers create a sense of urgency and encourage victims to bypass standard security procedures.
- Attackers may try to impersonate high-level executives who typically do not directly request fund transfers.
- An unexpected invoice may come through that is difficult to confirm, requesting payment for a product or service.
- Emails requesting payment information be changed.

Double-sided spoofing

This sophisticated type of financial scam involves a fraudster manipulating both the business customer and the bank by impersonating trusted parties on each side of a transaction. The process typically unfolds in two stages:

Stage 1: Impersonating the financial institution
The scammer contacts the business customer, pretending to be a representative from their bank or financial institution. During this call, the fraudster uses convincing tactics—sometimes creating a sense of urgency or referencing plausible account issues—to trick the customer into sharing sensitive information such as account numbers, passwords, or verification codes.

Stage 2: Impersonating the business customer
Armed with the stolen information, the fraudster then contacts the bank, this time posing as the business customer. Using the confidential details obtained earlier, they attempt to authorize fraudulent transactions, such as wire transfers, that appear legitimate to the bank.

Preventing double-sided spoofing
Train employees to be skeptical of unsolicited calls from a bank representative requesting sensitive information. Have them hang up and call the bank directly to verify the call and request. Banks will never ask for passwords or verification codes over the phone, so such requests should be treated as suspicious.

Implement Payee Positive Pay to prevent unauthorized transactions. This product requires businesses to provide their bank with a list of authorized payees for payments. When a check or an electronic debit comes in for payment, the automated system compares it to the list. Transactions that are not on the list are flagged for review.

> **"We're seeing a significant rise in intelligent—and believable—AI-generated scams targeted at not only individuals, but also businesses and financial institutions to try and gain access to critical financial information.**
>
> Paul Tucker
> **Chief information security and privacy officer at BOK Financial**

Ransomware

Ransomware is a form of malicious software, also referred to as "malware," that restricts access to computer files, systems or networks and requests payment for restoration of access. Ransomware attacks can cause business disruptions to operations and the loss of critical information and data.

Cybercriminals can distribute malware via links in emails, advertisements or websites. When these links are activated, malware can be installed onto computer systems, restricting access to devices and stored data. Certain types of malware include code that encrypts files and folders on local, attached and networked drives.

Detecting ransomware infection can be difficult until data access is lost. In many cases, a message is displayed requesting ransom payment. "The best defense against ransomware is preventing it—and it's more important than ever for companies and employees to work to prevent cyber incidents through training and good user behavior," said Paul Tucker, chief information security and privacy officer at BOK Financial.

Protection from ransomware

- Keep computer operating systems up to date with anti-virus and malware security installed and running regular scans.
- Back up all data will help prevent disruption to operations or lost data due to an infected computer or network.
- Keep all employees aware of not clicking on links that could be corrupt and hold regular training on cybersecurity.

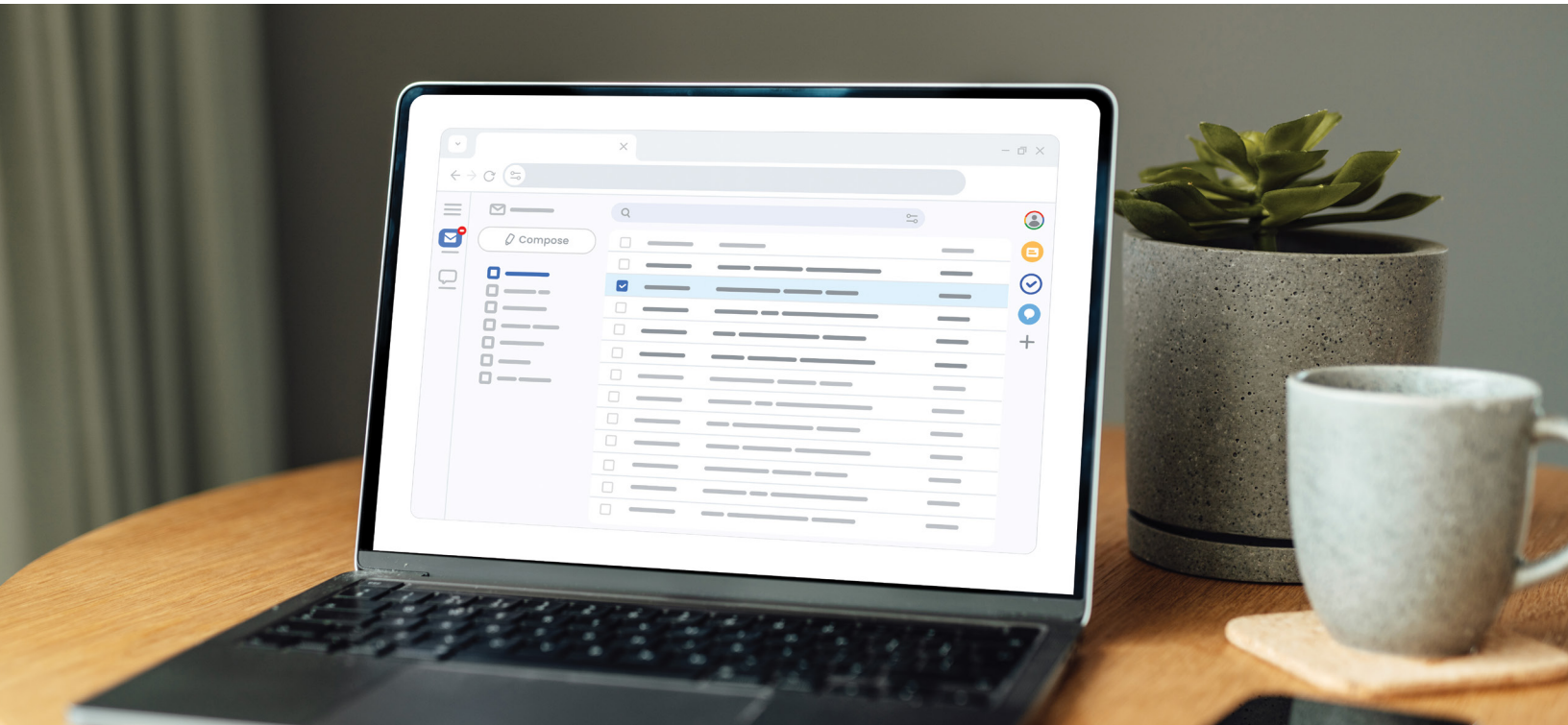
LEARN MORE

Take a byte out of fraud

5 ways fraudsters attempt to attack your company

Businesses brace for fraudulent payments

Ransomware on the rise is your business prepared



Fraud protection

Being aware of the types of fraud your business is susceptible to and having quick reaction times increases the likelihood of financial and data loss recovery. Accounts should be reconciled monthly or more frequently. Businesses that fail to identify discrepancies until months have passed may become liable for losses.

Having fraud protection measures in place can help stop fraud before it happens and allow for quick detection.

BOK Financial has a number of fraud protection services as well as business consultants who can provide guidance.

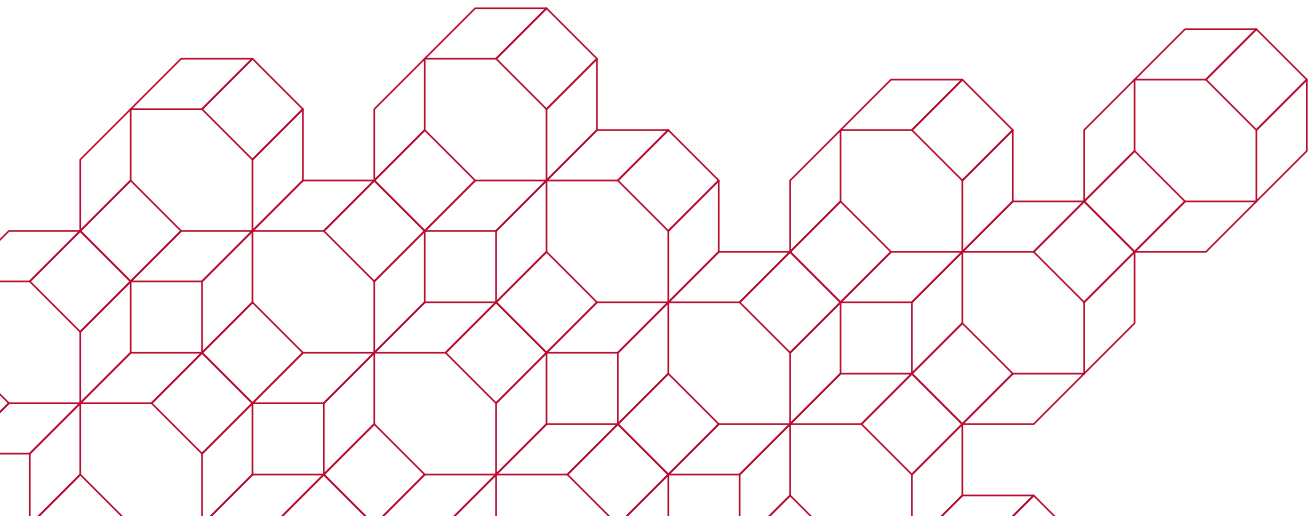
Precautions we take to protect you from fraud

Protecting your account information is one of our top priorities. We use advanced technology, data encryption and other security measures to help keep your account safe. As our client, you can enjoy peace of mind when performing key banking activity using our systems.

We are serious about safeguarding your business information online. As a security measure, you may access your account information online from our website only if you have signed up for our Exchange product.

Exchange uses Secure Socket Layer (SSL) technology to encrypt your personal information, such as user IDs, passwords and account information, over the internet. Any information provided to you is scrambled enroute and decoded once it reaches your browser. With Exchange, passwords are known only to the people entitled by them and require a change every 90 days.

Exchange also uses two-factor authentication with One-time Passcode, a security protocol that adds an extra level of protection for ACH and Wire transactions. Two-factor authentication requires a user to enter unique information to access the application and to complete ACH and Wire transactions. Additionally, online sessions automatically terminate after a period of inactivity.





Precautions you should take to protect your organization from fraud

When it comes to fraud, your business can never let its guard down. From computer systems and digital data to employee training and property security, it's important to look at fraud prevention from all angles.

- Validate all email requests for wire and ACH transactions, even when the email appears to be an internal email. Fraudsters can mimic internal emails to look like they are from company executives and still have them go to the authorized personnel for processing.
- Keep all software, including operating systems, browsers and applications updated with the latest security releases.
- Log off and lock your workstation whenever you leave your computer.
- Change your passwords often. Be sure to choose passwords that are hard for others to guess. Use special characters, capitalization and numbers when creating your password. Do not use words found in a dictionary but make changes to that word using special characters. For example: Instead of using 'Summer' as a password, consider '$ummer!'.
- Do not give your passwords to anyone. Do not record your passwords in an easy to find location.
- If you notice suspicious activity in your accounts, report it immediately to the appropriate parties.
- Install anti-virus, anti-spyware and other internet security software on your PC. Use it regularly and keep it up to date.
- Be leery of emails you receive from people you do not know, and do not open any attachments they may contain.
- When in doubt, delete the message without opening it.
- Take advantage of your PC's security features.
- Make sure your browser uses the strongest encryption available and be aware of the encryption levels of the sites and applications you use.
- Use only software from reliable vendors.

BOK Financial fraud protection services

Check fraud

One of the strongest defenses available to help prevent check fraud is **Positive Pay** services. Positive Pay helps detect check fraud by identifying payments the customer did not initiate. Daily, it compares check MICR line data to the company's issued check files for suspicious activity.

For an added level of fraud protection, add **Payee Positive Pay**, where payee information is verified in addition to standard MICR line data validation. Any discrepancies discovered in the payee line during this process are flagged as an exception item and sent to the customer through Exchange for decisioning.

PAYEE POSITIVE PAY FEATURES

- **Cashed check/teller verification** When someone cashes a check, the teller verifies it against the customer's check issued file.
- **Stale date and dollar amount exception processing** A customer can define stale dated checks or checks within a dollar range as exceptions.
- **Payee Positive Pay Payee** is verification of the Payee name.

BENEFITS TO YOU

- Protects checks from internal fraud and account impersonating.
- Error detection and correction occurs with redundant encoding.
- Increase protection around check distribution.
- Provides peace of mind.

Reverse Positive Pay is useful in situations in which a company wishes to prevent fraud and misuse of an account but cannot efficiently send the bank issued check files. The service allows the client to review all the previous day checks that were presented for payment. If any of the checks presented do not match the checks issued, the client can further investigate by viewing an image of the check. They can then elect to pay or return the check. All payment decisions are easily managed online via the Exchange Positive Pay module.



ACH fraud

ACH Fraud continues to be one of the leading causes of loss for companies and a growing concern for business owners everywhere. BOK Financial has several solutions available to help protect you from fraudulent ACH transactions.

TYPES OF ACH FRAUD PROTECTION

- **ACH Block** This is the simplest approach to protecting yourself from fraudulent ACH transactions. This service blocks any ACH debits and/or credits from posting to your account.
- **ACHAlert Positive Pay** This solution allows you to be in complete control of all ACH debit transactions on your account. The transactions are presented to you online for easy decisioning. With a simple click of a button, you can approve or return a transaction. Plus, authorized transactions are automatically approved for you. ACHAlert Positive Pay is accessed through Exchange.

BENEFITS TO YOU

- Helps to reduce fraud loss because potential items are identified within a 24-hour window.
- Provides an extra layer of protection against fraud.
- Saves time and money when you need to handle a potentially fraudulent situation.



I’ve been affected by fraud. What should I do?

REPORTING SUSPECTED FRAUD.

Please contact your local Treasury Client Services Professional (TCSP) at your specific market number below. They will engage the appropriate resources to assist with your specific situation.

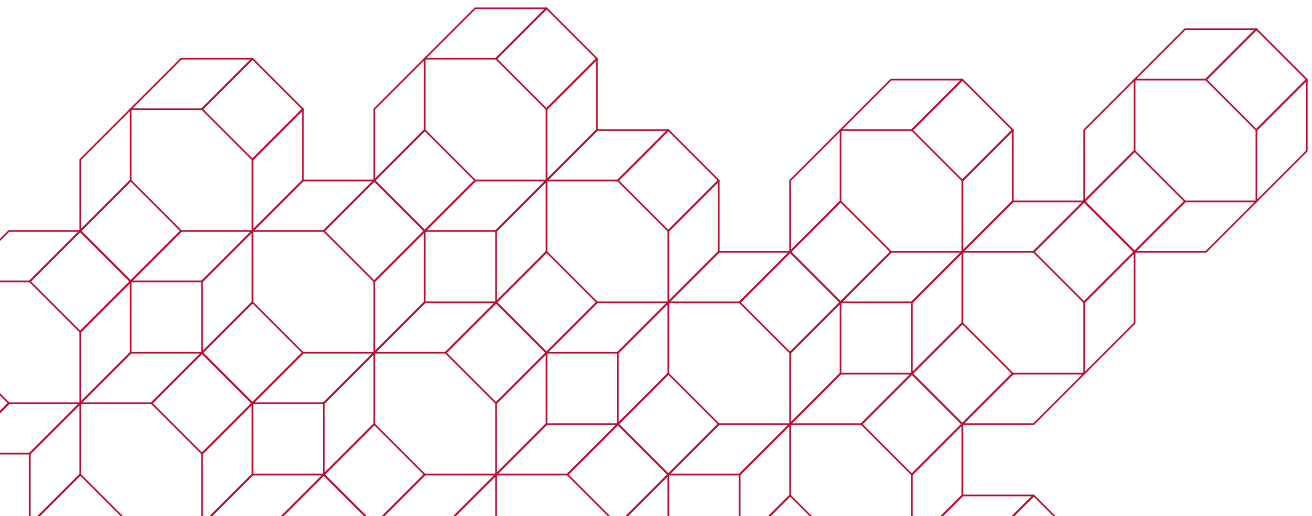
Market	Local Number Toll-Free
All Markets	800-878-7817
Arizona	602-808-5342
Arkansas	479-973-2611
Cash Management Consultants	855-709-3844
Colorado	303-863-4457
Dallas	214-987-8870
Fort Worth	817-255-2134
Healthcare	800-541-4844
Houston	713-289-5858
Kansas City	816-881-8270
New Mexico	505-855-0803
Oklahoma City	405-272-2496
San Antonio	210-568-7717
Tulsa	918-588-8655

See next page for Federal Trade Commission (FTC) and U.S. Department of Justice contact information.

Customer best practices

EMPLOYEE TRAINING

- Hold regular training on secure workflows, protocols and systems.
- Train staff to identify phishing attempts and recognize business email compromise.
- Establish dual-control procedures and vendor verification protocols.



WHEN PROCESSING PAYMENTS

- Follow predefined payment instructions and properly verify changes.
- Verify legitimacy and then validate changes to existing invoices, bank deposit info and contact info.
- Perform call back verification for fund transfer requests using phone numbers on file, NOT numbers in an email.
- Prohibit fund transfer requests received via email or other less secure messaging systems.
- Require authorization from senior management on payments over a specified threshold.
- Use dual control for outgoing payments such as ACH and wire transfers.
- Use voice confirmation for high-risk wire requests.
- Require multi-factor authentication for access to company networks and payment initiation.
- Strictly limit the number of employees who have the authority to approve and/or process payments.
- Segregate duties and limit employees who process collections, disbursements and reconciliation.
- Perform daily reconciliation of accounts.
- Review your insurance coverage to determine the appropriate levels needed for your organization.

ADDITIONAL CONTACTS

Report scams, deceptive business practices, identity theft and imposter fraud.

  - **Website:** ReportFraud.ftc.gov
- **Process:**
  - Visit the site and click “Report Now”.
  - Select the category of fraud (e.g., online shopping, payment services).
  - Provide detailed information including names, payment methods, and communications.
- **Phone Support:** 1.877.382.4357
- **Spanish Portal**: ReporteFraude.ftc.gov/cite/turn1search1/

U.S. DEPARTMENT OF JUSTICE

- **General Fraud:** Contact the FBI via tips.fbi.gov
- **Internet Fraud:** Report via IC3.gov
- **Mail Fraud:** U.S. Postal Inspection Service at postalinspectors.uspis.gov
- **Securities Fraud:** SEC Complaint Center

FRAUD RESPONSE CHECKLIST

- [ ] Notify internal stakeholders
- [ ] Contact bank fraud department
- [ ] File police report if necessary
- [ ] Document incident details
- [ ] Review and enhance controls
- [ ] Communicate with affected parties

BOK FINANCIAL®

BOK Financial® is a trademark of BOKF, NA. Member FDIC. Equal Housing Lender. © 2026 BOKF, NA. CM-14184 03-2026