Treasury Services

Fraud Prevention Frequently Asked Questions

Q: What precautions do you take to protect me from fraud?

A: 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.

Q: Regarding online fraud, what precautions do you take to protect me?

A: 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 en route and decoded once it reaches your browser.

With Exchange, passwords are known only to the persons 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.

Q: What precautions should I take to protect my organization from fraud?

A:

- Validate all email requests for wire and ACH transactions, even when the email appears to be an internal email.Fraudsters are able to mimic internal emails to look like they're 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.
- Do what you can to prevent unauthorized people from using your personal computer (PC).
- 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.

Q: What options do you provide to guard against check fraud?

A: One of the strongest defenses available to help prevent check fraud is our Positive Pay services.* These services enable the bank to match checks presented for payment against your account to your data file. Checks that do not match can be returned unpaid before a pre-established return deadline. We also have Payee Positive Pay*, which goes one step further and validates that the payee was not altered during the check collection process. Through the use of both of these services, checks are also validated at the teller line before cashing.

Another fraud prevention tool is Reverse Positive Pay*. With this service, you receive a daily paid report you can use to match against your issued checks. You simply determine which checks to return and notify us of those instructions through the Exchange Positive Pay module.

BOK FINANCIAL

Treasury Services

Fraud Prevention Frequently Asked Questions

Q: **How do I protect myself from ACH fraud?**

A: We recommend that you use separate ACH and check disbursement accounts to allow for easier monitoring. You can also guard your ACH accounts by applying ACH Debit Blocks and Filters and ACHAlert Positive Pay.*

Q: **What are ACH Debit Blocks and Filters?**

A: ACH Debit Block* is a service which guards commercial accounts against unauthorized ACH debit transactions by comparing incoming debits against account numbers, transaction codes, amounts, effective dates and sending company identification numbers. ACH Debit Filters* block debits using pre-selected criteria such as a dollar amount and transaction originator.

Q: **Can I use an ACH Debit Block and still allow select ACH payments to be paid?**

A: Yes. All you need to do is provide us with the ACH ID numbers of clients or vendors you want to designate as exceptions to the ACH debit block service. These "exception" companies should be able to provide you with their ACH ID numbers.

Q: **What is ACHAlert Positive Pay?**

A: ACHAlert Positive Pay is a service that allows you to control the ACH debit &/or credit transactions that post to your account. Options are:

Return All-all incoming ACH debits &/or credits will be returned if no action is taken. You can decision certain items to post by reviewing the activity in ACHALert or you can authorize certain transactions to always post.

Pay All-all incoming ACH debits &/or credits will post if no action is taken. You can decision certain items to return and you can also Block certain items to always return.

Q: **What should I do to report suspected fraud or provide information regarding fraud?**

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

Market	Local Number	Toll-Free	Market	Local Number	Toll-Free
Albuquerque	505.855.0803	866.535.2082	Houston	713.289.5858	866.827.3710
Arkansas	479.973.2611	800.878.7817	Kansas City	913.234.6601	877.265.4069
Dallas	214.987.8870	866.407.4147	Oklahoma City	405.272.2496	800.541.4844
Denver	303.863.4457	866.434.2084	Phoenix	602.808.5342	866.802.5506
Fort Worth	817.255.2134	866.407.4147	Tulsa	918.588.8655	800.878.7817

BOK FINANCIAL