Fraud Mitigation Best Practices

ALL EMPLOYEES

- Download the security software Rapport by Trusteer. Bankers Trust offers this to all customers for free. Visit http://landing2.trusteer.com/landing/bankerstrust
- Never share usernames, passwords, or token PIN information.
- Where applicable, create strong passwords
  - » At least 12 characters.
  - » Combination of mixed letter cases, numbers, and special characters (at least 2 of each).
  - » Avoid letter or number sequences, names of relatives or pets, or common dictionary words.
- Check last login date and time at every log in.
- Logout from online systems, do not just close the browser window.
- ALWAYS lock your workstation every time you step away, even for a minute.
- Never conduct banking transactions while multiple browser windows are open on your computer.
- Do not use public or other unsecured computers for accessing Internet banking.
- Be aware of other people nearby who may try to look at information on your screen.
- Sign up for automated email and text alerts.
- Review account balances and transaction detail regularly and notify Bankers Trust immediately of any suspicious transactions.
- Never share account numbers with unknown parties.
- Sign up for electronic bank account statements to reduce the chances of misrouted, lost or stolen mail.
- When originating ACH transactions, consider sending prenotes to verify account information.
- Do not open email from unknown sources.
- Do not open file attachments or click on web links in suspicious emails.
- If anything looks suspicious in an email or on a web page, call the sender or company to verify AND contact your IT department for assistance.
- Follow procedures to validate payment approvals and instructions. If payment requests seem odd or payment information has changed, verify with the source before remitting.
- Always verify that any visitors are authorized to be in your area.

MANAGERS AND SYSTEM ADMINISTRATORS

- Only assign the services a user needs and assign dollar limits to the permitted transaction types.
- Limit administrative rights on users' workstations to reduce the possibilities of inadvertent malware downloads.
- Force periodic password changes.
- Assign dual system administrators for Internet banking services.
- Use multiple approvals and dollar limits for money transfers such as ACH and wire transfer. Also require separate entry and approval users.
- Maintain information technology and privacy policies and procedures. Train employees regularly on the policies and in security principles. Be sure all employees understand their responsibilities.
- Ensure that all computers have the latest security software, web browser, and operating system to protect against viruses and malware. Download and apply patches and updates daily or weekly.
- Back up data regularly and ensure backups are secure.
- Ensure a firewall is enabled on work computers and also on personal computers for any employees working from home.
- Ensure Wi-Fi networks are secured using WPA2 with a minimum of 12 characters for pre-shared passphrase. WEP is not a secure method.
- Delete Internet banking user IDs as part of the exit procedure when employees change positions or leave your company.
- When possible, use separate transaction accounts for electronic and paper transactions to simplify monitoring and identifying discrepancies.
- Reduce risk of financial loss by using ACH Positive Pay and Check Positive Pay with Payee Validation services.
- Implement Check Block on electronic-only accounts to block fraudulent checks.
- Utilize ACH Origination services to automate payments while reducing the number of checks with your bank information floating through the system.
- Restrict physical and electronic access to banking, customer, vendor and other protected information to those who need-to-know.

Call Bankers Trust to learn more

1-800-362-1688

BankersTrust.com

Customer Service:

7:30 a.m. – 8:00 p.m. Central	Monday – Friday
8:00 a.m. – 12:00 p.m. Central	Saturday

BankersTrust®
Member FDIC