DollarBank®
Wire Transfer

Best Practices for Wire Transfer Processing

Thank you for choosing Dollar Bank Wire Transfer. These best practices are to help protect and safeguard your confidential account information. Because wire transfer payments are typically irreversible, they are commonly targeted in fraud schemes. We recommend you put proper controls in place, provide education and conduct annual internal reviews of your processes.

Logical and Physical Security

- Protect all passwords and personal identification numbers.

- Secure all computers used to access Business Online Banking, both physical and logical.

- Store exported information securely, whether printed or electronic.

- Ensure logical security is in place which may include (but not limited to) firewalls, virus protection, anti-phishing software and keystroke logging prevention.

- Update computer operating system and software regularly.

Account Access Controls

- Establish and maintain internal procedures to reduce the risk of unauthorized/fraudulent activity:
    - New employee training
    - Outline access guidelines
    - Appropriate internal controls
    - Segregate duties

- Institute dual control procedures for verification prior to transmitting wires.

- Have different individuals process transactions from those who reconcile accounts.

- Apply role and account level security limiting users to only be able to transmit payments or research certain accounts.

- Review for inactive users and delete terminated employee access promptly.

Important Tips

- Verify wiring instructions and bank routing number prior to initiating a wire transfer via a phone call to a known number on file and not via email.

- Implement a call-back verification process when setting up payment instructions for a new vendor or making changes to payment instructions for an existing vendor.

- Understand email scams and educate your employees on wire transfer procedures.

- Don't be pressured or rushed. Requests for changes or immediate action, or a lack of availability by phone, should be met with intense scrutiny. Slow down and follow your company process.

- Notify the bank immediately if suspicious activity is detected.

- Review your business insurance policy to see if it covers financial losses due to cybersecurity fraud.

If you have any questions, please contact Dollar Bank Treasury Management at 1-855-282-3888, Monday - Friday, from 8:30 AM - 5:00 PM ET.