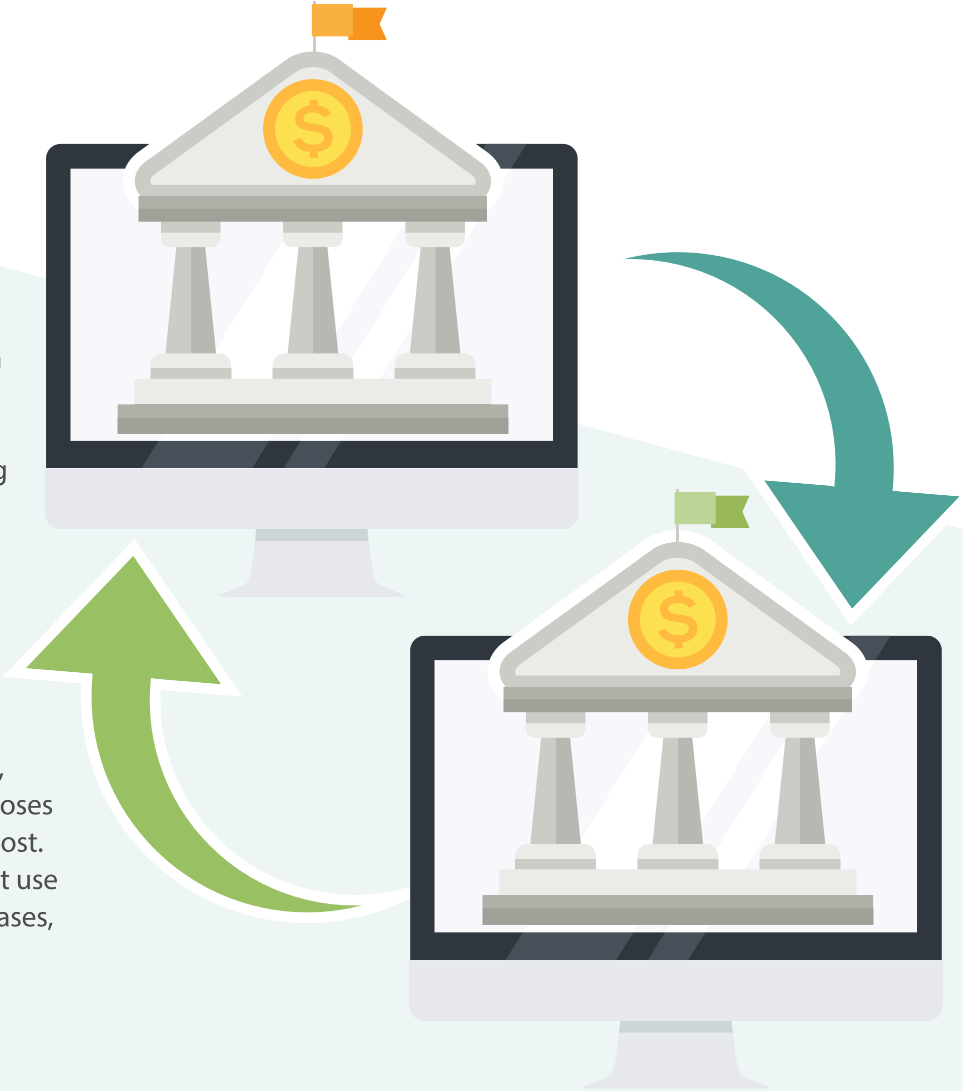
Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

Best Practices for Sending Wire Transfers



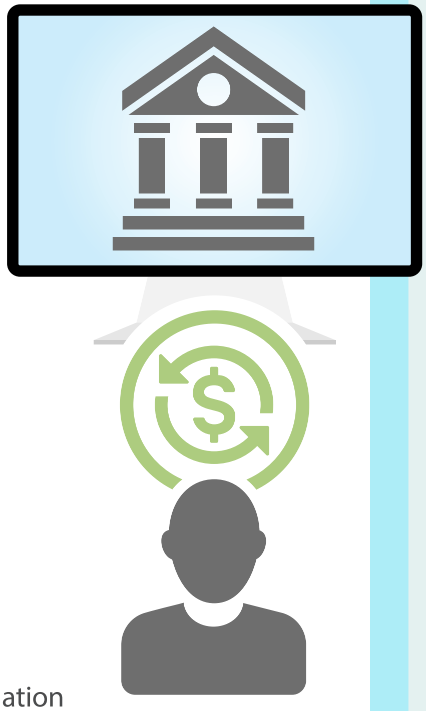
Wire transfers move money from one bank account to another almost instantaneously. They are generally considered safe as long as the sender is confident the transaction is valid, and the wiring instructions are accurate. In today's environment, those can be hefty assumptions.

Wire transfers are typically used to transfer larger sums of money, and usually only for limited purposes due to the higher transactional cost. For example, governments might use them to make investment purchases, debt payments, or potentially to purchase property.

August 2022

Fraudulent actors are attracted to wire transfers and purposely try to deceive accounting staff into wiring money to accounts they control. Employees can also perpetrate wire transfer fraud, or merely make a mistake and send money to the wrong place. A government may not be able to dispute or reverse a wire transfer once it has been sent, except in limited circumstances. Authorities can try to recover the funds, but often bad actors will move them quickly to other accounts, making it impossible.

It is critically important that governments design and implement a robust set of internal controls before sending wire transfers. To help you, we've developed the following best practices.



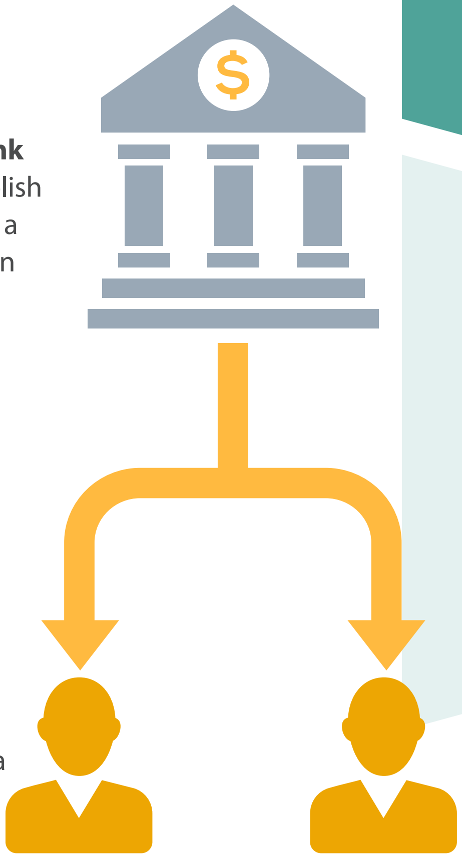
Take these important first steps

- **Develop a detailed wire transfer policy.** Your policy should include detailed procedures for initiating, approving and executing wire transfers. It should address segregation of duties and include steps employees should take when they are uncomfortable proceeding with any transaction. It should also require all transactions go through your regular internal control processes before staff initiate a wire transfer. For example, all disbursements should be supported, approved, and audited before payment. Your policy should incorporate as many of the best practices below into your procedures as you deem appropriate.

- **Educate and empower your finance staff to be responsibly suspicious.** Management should provide training to employees on social engineering and wire transfer fraud schemes during onboarding and annually thereafter. You want staff to be responsibly suspicious when asked to wire money, and to proceed with the utmost caution and diligence. Your training should also inform employees about your wire transfer policies and procedures, create a perception of fraud detection within the organization, and share knowledge of consequences for committing fraud among staff.

- **Understand your insurance coverage.** Read your policy, and work with your legal counsel if you need help understanding the terms and conditions for wire transfer payment losses. Obtain additional coverage if you need it, including potentially bonding certain employees.

Segregate duties to reduce your risk



- **Require two people to execute a wire transfer with the bank [an essential internal control].** Work with your bank to establish a protocol where one employee initiates the wire transfer and a second employee approves releasing the funds. No one person should ever be able to send a wire transfer on their own! Your policy should specify which positions may act as initiators and approvers.

- **Separate banking responsibilities from the payment processes.** Employees with the authority to add or edit wire blocks to bank accounts, or those who have responsibility to monitor or reconcile bank account activity, should not have the authority to send or approve wire transfers.

Prepare your bank accounts for wire transfers

- **Use a dedicated bank account for wire transfers.** Maintain a zero balance and restrict this designated wire transfer bank account from processing checks or other payment types.

- **Establish dollar limits with your bank.** You can establish dollar limits for an individual transaction, per day, or by employee. To determine this limit, you might consider the amount of insurance coverage you have to cover a loss.

- **Place international wire transfer blocks.** If you are not going to send money internationally, then put a block on your dedicated wire transfer account. Sending money internationally carries more risk—once money leaves the United States, it is likely gone forever.

- **Place wire transfer blocks on all other accounts.** Work with your bank to place blocks for any accounts not authorized for wire transfers.

- **Establish wire templates for repeat transactions.** To reduce manual keying errors, work with your bank to set up wire templates for repeat transactions.

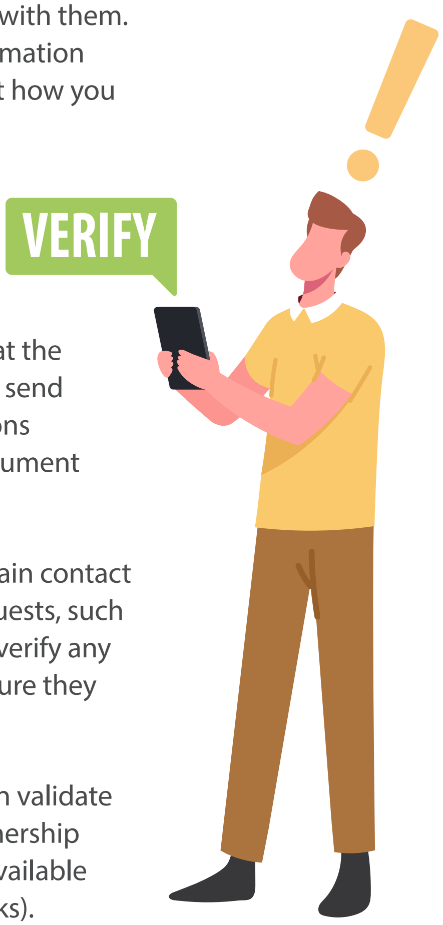
- **Sign up for a bank callback service.** Many banks will contact a designated official for final approval to release funds. This is especially important for high-dollar or non-repetitive wire transfers. The designated official provides a passcode or passphrase to the bank as further proof of their identity. It is important the designated official does not share this passcode or passphrase with others.

- **Use a bank that verifies account ownership.** Major banks are now required to confirm the payee for domestic wires. The bank will obtain the recipient's name from you and match it to the bank account's owner. You should check with your bank to see if it has adopted this important security measure.

Set up a verification process

VERY IMPORTANT TO DO

- **Verify the authenticity of the wire transfer request.** It is critical that employees verify a wire transfer request, especially if received by email. Staff should call **the authorizing employee** requesting the wire **by phone**, using contact information that is already on file and previously used. If you are a county receiving wire transfer requests from your taxing districts, make sure to verify directly with them. Your policy should direct staff not to use contact information provided in an email or wiring instructions. Document how you verified the wire transfer request.



- **Verify the wiring instructions are correct.** You should verify wiring instructions directly with the payee, preferably by phone, using contact information that is known and reliable. Staff should also verify the bank routing number is correct, and that the bank's location is consistent with where you intend to send the wire. Any subsequent changes to wiring instructions should go through the verification process again. Document how you verified the wiring instructions.

- **Verify changes to contact information.** If you maintain contact information for anyone that submits wire transfer requests, such as certain employees or taxing districts, make sure to verify any requested changes to that contact information to ensure they are valid.

- **Consider implementing account validation.** You can validate the accuracy of account information and account ownership before sending a wire transfer using a commercially available validation service (such as those offered by some banks).

- **Review verification documentation.** Management should review and approve verification documentation before the wire transfer is sent.

Require these steps to execute a wire transfer

- **Use a standardized form.** The form should include the following information: the wiring instructions, the reason a wire transfer is necessary, the requestor's and approver's signatures authorizing the wire transfer, and how the wire transfer and wiring instructions were verified.

- **Limit how you will submit wire transfer requests to your bank.** A person could communicate wiring instructions to a bank in person, by fax, by email, via telephone or the Internet. You should discuss the best option with your bank, understanding that each option carries different risks. Once you decide on the best option, limit wire transfer requests to that method.

- **Share wire instructions securely.** Managers within your organization, vendors, taxing districts or other affiliated organizations may need to send wire instructions to finance staff. Your policy should discourage the use of email for this purpose. If you decide to allow email, the information should be encrypted and directly verified with the payee.

- **Require special approval to send a wire transfer.** Certain officials may be able to approve an expenditure, but your policy should require special approval to send a wire transfer payment. For example, your policy might require the finance director to approve all wire transfers exceeding $25,000. This approver should verify a wire transfer is necessary, given the details of the situation.

Take steps to protect yourself when banking online

- **Use a dedicated, secure computer.** You should use a dedicated computer for any online banking activity, such as sending electronic wire transfers. This computer also needs to be up to date with security patches and antivirus protection. These steps help protect it from malware, which can lead to compromised login credentials. You can learn more about how to bank securely online by reading this resource from the United States Computer Emergency Readiness Team (US-CERT).

- **Use a bank that offers token keys.** A token is a physical device that provides a key code you enter when logging in to your online account. This form of multifactor authentication is more secure than an emailed or texted code. Governments should contract with banks that offer this security device, and use it for any employee that has entitlements to send wire transfers.

- **Keep up to date on your bank's security measures.** Check in with your bank every six months to identify new options or services that can help protect your government against wire transfer fraud.

Actively monitor

- **Check the bank's wire receipt.** As soon as possible, compare the bank's wire receipt to your original documentation to identify any errors or discrepancies.

- **Review your bank activity daily.** Wire transfers happen almost instantaneously, so you have a very small window in which to report concerns to your bank. It is best if you review your bank account at least daily, to identify issues promptly.

- **Use fraudulent incidents to inform your risk assessment process.** Analyze and quantify the extent to which your government has already suffered financial losses from fraudulent wire transfer payments to inform fraud risk assessments and prioritize and tailor countermeasures.

Additional resources

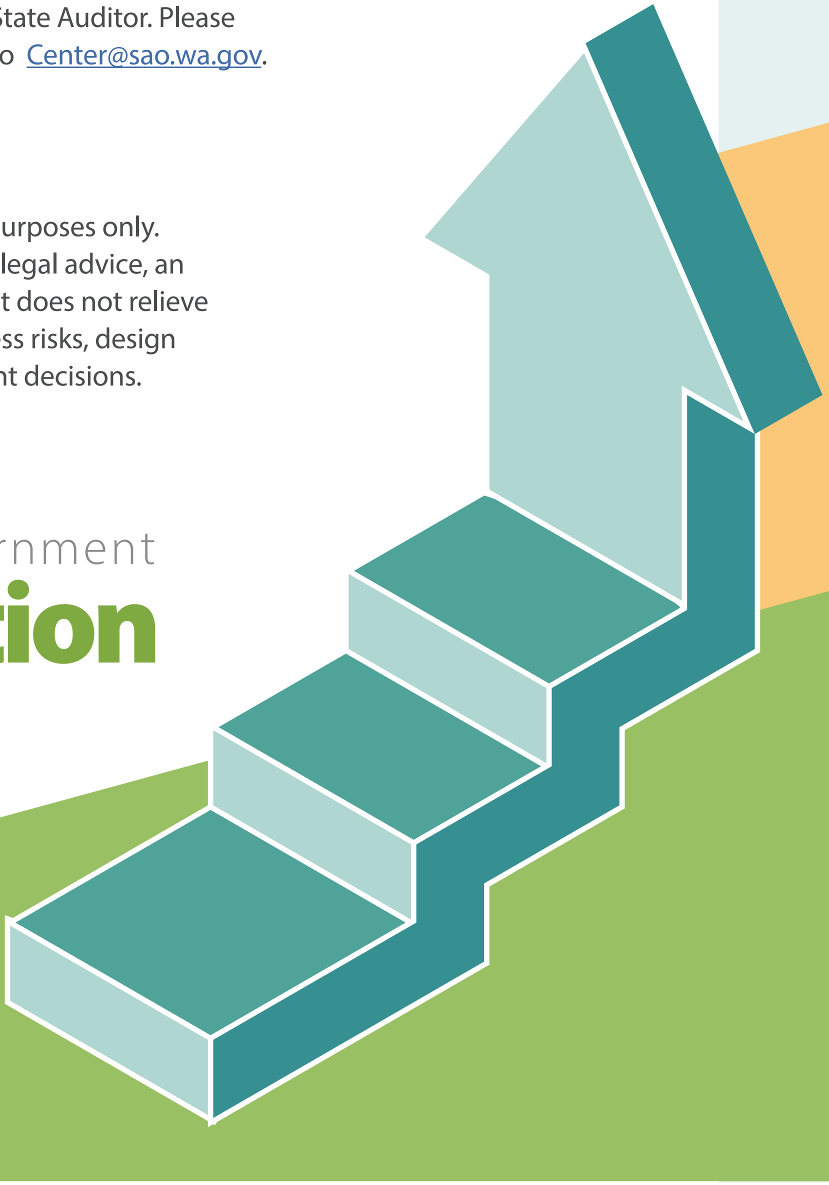
- Government Finance Officers Association's (GFOA) Advisory on Electronic Vendor Fraud
- United States Computer Emergency Readiness Team's (US-CERT) Banking Securely Online (cisa.gov)
- Office of the Washington State Auditor's Segregation of Duties guide

For assistance

This resource was developed by the Center for Government Innovation at the Office of the Washington State Auditor. Please send questions, comments, or suggestions to Center@sao.wa.gov.

Disclaimer

This resource is provided for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation, or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.



Center for Government
Innovation