Contracting with vendors to accept or process your payments

(Also known as third-party receipting)

Best practices

Brought to you by the Center for Government Innovation, a service of the Office of the Washington State Auditor

5/2025

Introduction

If you would like to contract with a vendor to accept or process payments, we have some helpful information for you. Perhaps you want to contract with a vendor to:

- Use a vendor receipting system, online or otherwise, where the vendor helps with handling or processing payments
- Use a payment and receipting "app" (also known as peer-to-peer payment applications)
- Accept or process credit card payments (vendors are referred to as a merchant account processor or a payment service provider)

Whichever type of contracting you choose, keep in mind you are still responsible and should have controls in place to protect your money.

When you contract out and allow third parties to handle your money, you also should have controls in place to protect it and manage any associated risks. For example, electronic payments might be lost in transit while going through the virtual channels to reach you. Or, you may not take steps to ensure you and your vendor protect cardholder data, or otherwise comply with Payment Card Industry (PCI) requirements. Here are some of the best practices we have observed during our audits of this area, which we often refer to as third-party receipting.

Before you sign a contract

- **Put someone on point.** Assign a point person to help departments with these contracts. This employee can help departments with vendor selection as well as negotiating contract terms consistently across your organization.
- **Ensure any vendor is state-approved, if you are a state agency.** The state of Washington evaluates two and approves any vendors that can access state bank accounts. State agencies should refer to the *State Administrative & Accounting Manual* section 85.20.20, as well as these resources from the Washington State Treasurer: Banking and Merchant Card Services and Payment Disbursement and Collection Options. Local governments are not subject to these restrictions.
- **Select your vendor with care.** Discuss and agree on your scope and specifications in advance. Use a robust selection process so that you make the best choice, based on your needs.

- For a resource to help when selecting a payment card service provider, see the Government Finance Officers Association best practices here. This document recommends governments us a "Request for Proposal" competitive process when selecting the type of vendor.
- For a resource to help evaluate peer-to-peer payment apps, consider Consumer Report information here. Consumer reports plans to expand its evaluation in the future.

  (Note: The State Auditor's Office does not evaluate third- party vendors, peer-to-peer payment apps or payment card service providers. If you decide to use a third party to handle or process your money, you must determine whether you may use them and understand and address all associated risks.)

- **Read the fine print.** A written contract should establish the responsibilities of the local government and any third-party provider. As with any contract, you should review it carefully to understand the terms and ensure it includes all appropriate provisions. For example, it should spell out the details of how the vendor will receive and remit payments to your government (settlement/remittance terms), as well as address payment card industry requirements. Consider involving your legal counsel before you enter into such contracts.

  If you plan to use a peer-to-peer payment application, make sure you understand the agreement terms and all related disclosures.

- **Be aware of Washington receipting requirements.** We suggest you familiarize yourself with your governing statutes, any other relevant statutes for banking, deposits or electronic transactions, and the *Budgeting, Accounting and Reporting System* (BARS) Manual requirements. Some key requirements include:

  - Expect an online receipting service to deposit money collected on your behalf within 24 hours of receipt, unless you have written authorization from your treasurer granting an exception of up to one week, in accordance with (RCW 43.09.240). We generally consider the start time for the 24-hour rule to begin when the card processing system remits the funds to the initial bank account –- whether owned by the local government or vendor.
  - The third party must not retain any withholding or reserve accounts. State law requires deposits to be made intact (RCW 43.09), which means that you cannot allow the receipting vendor to hold or maintain a pool of money as it violates qualified depository requirements. (Your contract might include some language for reserves related to returns or chargebacks/ disputed charges. However, that typically applies only in a retail setting, so the vendor should not hold back funds. If your contract has this language and your vendor exercises this option, we will consider that a high-risk situation and potentially a compliance issue.)
  - You must only deposit public funds with qualified public depositories as established by the Public Deposit Protection Commission, as per RCW 39.58.080. You can find them listed here. (Your vendor should only briefly have the funds, so if that is the case, then these requirements apply to only the final bank.)

Add additional safeguards if using peer-to peer payment applications

- **Use multi factor authentication** (MFA) to secure account information and protect yourself against compromised credentials. MFA requires more than just a password to access your systems and information. For example, the application might require a password and a code texted to your phone.
- **Limit access to your funds.** Only link the payment application to a zero-balance bank account, that you reserve for this special use. Avoid allowing a third party to access your main bank account, or any significant sum of money.
- **Implement procedures for how you will verify and process refunds.** A payee may use a compromised credit card to pay you and then seek a refund from you. If you process the refund using another method and the original transaction reverses, then you will lose double the original transaction amount.
- **Implement procedures for how you will verify payments.** If someone claims they paid you, your employees should not rely on a customer's phone data to confirm a payment. They might use a fake screen shot. Use your own records, such as by logging into the application to view payment data, to verify someone has paid you.

Complying with PCI requirements

- **Ensure your contract addresses all applicable PCI requirements.** All governments and vendors who handle credit card data must comply with PCI requirements, which focus solely on protecting cardholder data from theft or loss. This includes peer-to-peer payment application providers handling credit card data as well. For a quick reference guide about PCI requirements, click here.

- **Practice oversight over vendor compliance.** When you use a vendor to help you accept credit card payments, including use of a peer-to-peer payment app, you need a process to verify the third-party provider adheres to PCI compliance requirements. There are two ways to accomplish this:
  - Periodically make sure the vendor qualifies as a registered provider through one of the three major credit card companies; a registered payment facilitator has gone through a special registration process for controls that safeguard money and to demonstrate PCI compliance. You can verify vendors on each major credit card company's website, or by obtaining a written confirmation of registration from the vendor.
  - Obtain other assurance from the vendor that it has met compliance requirements, such as a PCI compliance audit.
- **Monitor your own PCI compliance.** Your government should have controls to monitor your own compliance with PCI requirements. At a minimum, local governments must complete a Self-Assessment Questionnaire appropriate to their level of responsibility, but depending on various factors, you may have to do more (such as obtain a report on compliance). Read your contract with your third-party receipting vendor for specific requirements you must follow.

Maintaining oversight of money

- **Keep tabs of the money.** If your funds go to your vendor before you, then you must have controls in place. Here are some things to look for:
  - Monitor to ensure the vendor remits funds to you in the required time frame, as per your contract settlement terms and state law requirements (RCW 43.09.240).
  - When your vendor remits funds to you, - make sure that you own the bank account receiving the remitted funds. State law also requires you to use an approved qualified public depository located in the state of Washington, as confirmed by the Public Deposit Protection Commission. You can verify this here.
  - Ensure the vendor remits funds to you electronically (not via mail).
  - Verify that you have procedures in place to monitor the remittance; you should verify the vendor sent you 100% of the funds they owed you. You must account for all of it.
  - Regularly review all service fees to ensure they comply with your contract's terms. Your vendor should provide a report that clearly and separately identifies them.

- Make sure that the vendor does not hold back money, which is often called a reserve.
- If you use peer-to-peer payment apps, monitor activity within the app. In some cases, apps will permit disbursements from the account, as well as accept payments. You should monitor that all activity meets your expectations.

- **Protect against losses.** Local governments should have a reasonable ability to recoup any loss that may occur during the vendor's control and custody of the funds. Consider taking these steps:
  - Confirm your vendor's status as a registered payment facilitator, if applicable. Registered vendors have undergone a special process that confirms they have controls and safeguards in place to protect your payments. You can search for a receipting service provider, and whether they are a registered payment facilitator, on each major credit card company's website.
  - Procure a fiduciary bond or crime protection insurance policy so you may recoup any losses incurred while the vendor controls your money
  - Obtain and review a service organization control (SOC) 2 report from your vendor; you might have to sign a non-disclosure agreement to view it due to the sensitivity of the information. To learn more about SOC reports, consider this information provided by Infosec.
- **Practice management oversight.** Internal controls over these contracts and revenue streams are important and might include:
  - Centrally track and inventory contracts with third party receipting vendors
  - Follow up before contracts expire and avoid conducting business with a third-party vendor when you have an expired contract with them (a common audit issue)
  - Verify policies and procedures address how to reconcile financial records with bank deposits received from the third party
  - Ensure revenues meet your expectations

Additional information and resources

- Washington State Treasurer, Banking and Merchant Card Services and Payment Disbursement and Collection Options.
- Government Finance Officers Association, Best Practices for Selecting a Provider
- Consumer reports, Potential Consumer Risks for Users of Apple Cash, Cash App, Venmo, and Zelle
- Washington State Treasurer, Qualified Public Depositories
- Payment Card Industry (PCI) standards, Quick Reference Guide
- Infosec, Understanding SOC Compliance: SOC 1 vs. SOC 2 vs. SOC 3

Municipal Research Services Center, Credit Card Acceptance

Questions? Concerns?

Contact the Center for Government Innovation at the Office of the Washington State Auditor at: 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

"Our vision is to increase **trust** in government. We are the public's window into how tax money is spent."

– Pat McCarthy, State Auditor

Washington State Auditor's Office P.O. Box 40031 Olympia WA 98504

http://www.sao.wa.gov

564-999-0818

Center for Government Innovation

Office of the Washington State Auditor