Contracting with vendors to accept or process your payments

Best practices

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

September 2020

Intro

If you are looking 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
- Accept or process credit card payments (also known as a merchant card service provider)

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

When others handle your money, you need to manage the associated risks. For example, electronic payments might be lost in transit while going through the virtual channels to reach you. Here are some of the best practices we've observed during our audits of this area, which we often refer to as third-party receipting.

Before you sign a contract

1. **Put someone on point.** Assign a point person to help departments with these contracts. This employee can help with vendor selection as well as understanding and negotiating contract terms consistently across your organization.

2. **Select your vendor with care.** Discuss and agree on your scope and specifications in advance. A good selection process is important to make the best choice based on your needs. For a resource to help when selecting a vendor, see the Government Finance Officers Association (GFOA) best practices for "Accepting Payment Cards and Selection of Payment Card Service Providers."

3. **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 is complete. For example, it should spell out the details of how payments will be received and ultimately remitted to your government.

Monitor for compliance

4. **Double-check vendor compliance.** Any time credit-card payments are made online using a vendor, you need a process to verify the third-party provider is complying with Payment Card Industry (PCI) requirements.[1] These requirements are in place to protect cardholder data. There are two ways to accomplish this:
    - Make sure the vendor is a registered[2] provider through one of the three major credit card companies; or
    - Obtain other assurance from the vendor that it is in compliance, such as a PCI compliance audit.
5. **Monitor your own compliance.** Your government should have controls to monitor your own responsibilities for compliance with PCI requirements, under the contract. For example, this might take the form of a self-assessment or a report on compliance. However, refer to your contract for specific requirements you are expected to follow.

Maintain oversight of money

6. **Keep tabs on the money.** Have certain controls in place if money is deposited with the vendor first. Here are some things to look for:
    - Check the timeline for how long it takes funds to be remitted (from when the funds are settled to the vendor's account). This should happen within 24 hours, unless the treasurer has granted an exception of up to one week (RCW 43.09.240).
    - Make sure the bank account receiving the remitted funds from the vendor is owned by your government, located in the state of Washington, and is an approved qualified public depository, confirmed by the Public Deposit Protection Commission (PDPC).[3]
    - Ensure funds are remitted electronically so the transmission is faster and safer (not mailed).
    - Verify procedures are in place to monitor the remittance and to make sure it's 100 percent intact and accounted for.
    - All service fees should be clearly and separately identified on a report and reviewed regularly.

[1] A local government can have its own merchant ID number and avoid a vendor, in which case this would not apply.

[2] A registered payment facilitator has gone through a special registration process for controls that safeguard money and to demonstrate PCI compliance. These vendors can be verified online on each major credit card's websites.

[3] Can be checked at https://www.tre.wa.gov/pdpc/pdpc-info/qualified-public-depositaries/

7. **Be wary and watchful for reserves.** If the vendor holds back money, this is a reserve. State law requires that deposits be made intact (RCW 43.09). 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 shouldn't actually be holding back funds. If your contract has this language *and* your vendor is exercising this option, we would consider that a high-risk situation and potentially a compliance issue.

8. **Protect against losses.**[4] First, confirm your vendor's status as a registered payment facilitator, if applicable. If registered, these 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, online on each major credit card company's website. If your vendor is not a registered payment facilitator, then here are some other options:

    - Require a fiduciary bond or crime protection insurance policy. The goal here is to build in a mechanism that provides you a reasonable ability to recoup any losses incurred while the vendor controls the revenue.
    - Obtain and review a service organization control (SOC) report from your vendor. There are different types of reports and assurances, so understand what you want and are getting. To learn more: www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html

9. **Build in management oversight.** Internal controls over these contracts and revenue streams are important and might include:

    - Verifying that policies and procedures address how to reconcile financial records with bank deposits received from the third party
    - Ensuring revenues meet your expectations. Someone else is handling your payments – you want to be sure you are receiving what you expect.
    - Evaluating fees to make sure they follow your contract terms
    - Centrally tracking these contracts to ensure you know what departments have them, and that your risks are adequately covered

[4] This won't apply when you have a *"merchant agreement"* – the merchant agreement is with the bank card handling service. But it will apply to any vendor you are using for accepting credit cards, other than a bank of course.

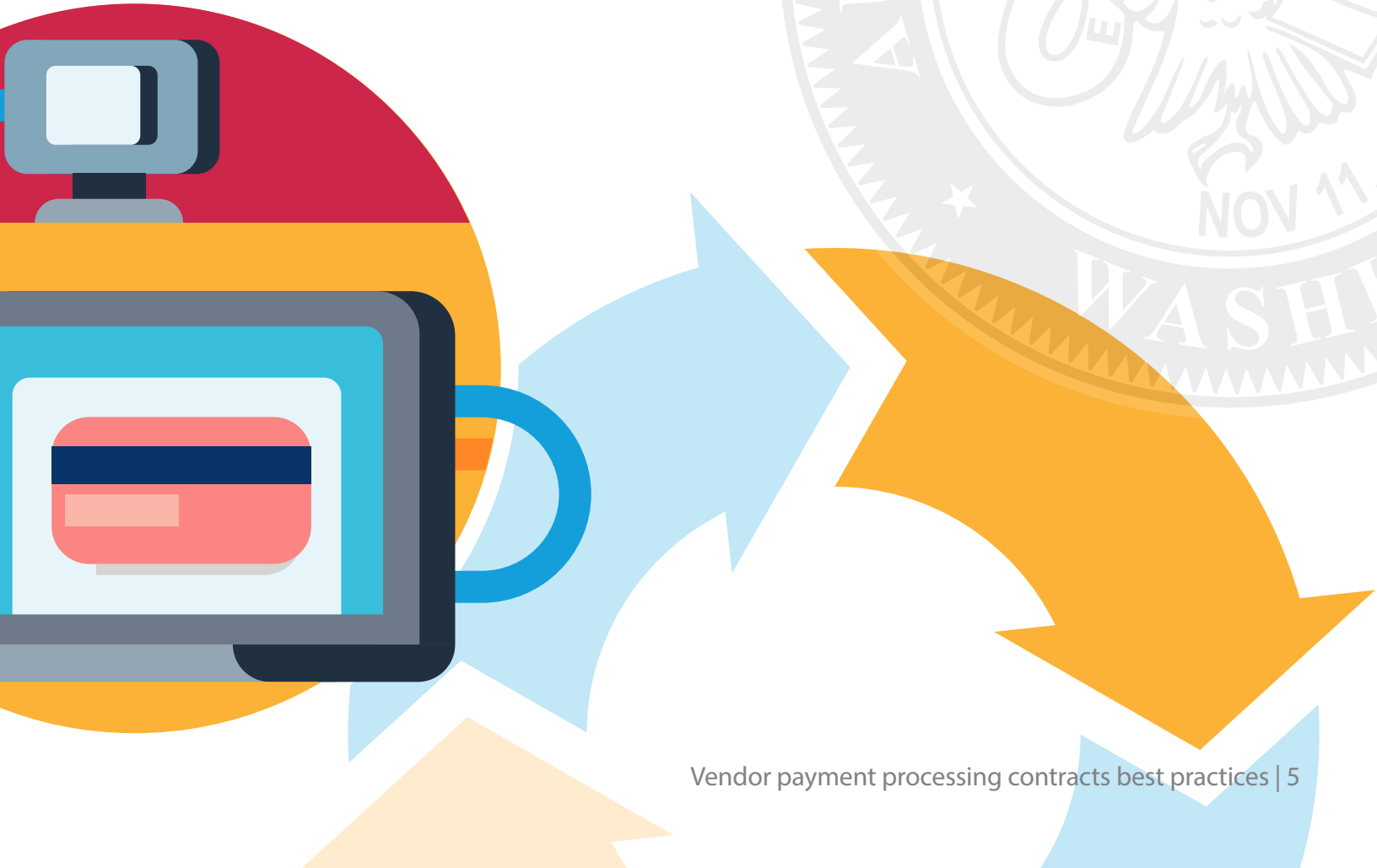
Additional information and resources

- Payment Card Industry (PCI) standards: www.pcisecuritystandards.org
- E-commerce requirements for state agencies: www.ofm.wa.gov/accounting/administrative-accounting-resources/e-commerce
- GFOA best practices for selecting a provider: www.gfoa.org/materials/accepting-payment-cards-and-selection-of-payment-card

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

1-866-902-3900

Center for Government Innovation

Office of the Washington State Auditor