EXPECT THE UNEXPECTED

How to protect unanticipated revenue from fraud

September 2023

Not all revenue is predictable

Local governments rely on revenues from property and sales taxes, various charges and fees, and transfers from state and local governments. These revenues are predictable and stable. But not every revenue is predictable. Governments also receive revenues from rebates, donations, collection agency payments, agreements with annual payments, or one-time fees. These revenues are infrequent or unanticipated, making them a prime target for misappropriation.

According to the Association of Certified Fraud Examiners (ACFE), fraud of unanticipated revenue accounts for about 17 percent of all asset-misappropriation schemes, with a median loss ranging from $45,000 to $50,000. These schemes typically last for 14 to 16 months before being detected. Here in Washington, fraudsters continue to employ this age-old tactic while finding new unanticipated revenue streams to target, as well as new ways to conceal their schemes.

Governments should know what types of unanticipated revenues they may receive, and design and implement internal controls to protect them. To help you, we have developed best practices for you to consider as you evaluate your current controls.

What is an unanticipated revenue?

A revenue is considered "unanticipated" when government staff do not know that the revenue is coming (like an unexpected donation), the amount (like taxes calculated by local businesses), or when the revenue will come in (like cemetery plot fees, where a government may only sell a few per year at random times). Commonly referred to as miscellaneous revenue sources, they encompass payments like gifts and donations, rebates and permit fees.

Unanticipated revenues can also be commonly receipted revenues for which governments do not typically invoice. For example, many governments have business and occupation taxes (also known as B&O taxes) that rely on business owners to pay the correct amount of tax based on their quarterly gross income. Governments cannot bill amounts because they do not know the quarterly gross income of every business, so they instead rely on each business to calculate and pay the appropriate tax. Because governments do not typically invoice or bill the payers (creating a record of the amount due), it is easy for employees to divert the payments without anyone noticing.

One of the largest frauds of unanticipated revenue that SAO has investigated involved B&O tax payments. A city discovered that B&O tax checks from one of its vendors were missing in the accounting system. Ultimately, an investigation discovered that the city's deputy clerk-treasurer had been taking other cash received and substituting unanticipated checks received in their place. The unanticipated checks were from vendors and customers for B&O taxes, lease payments, and cemetery plots and related service fees. This scheme went undetected for nearly seven years, costing the city more than $300,000.

The level of fraud risk varies by source. For example, if firearm permits are issued on prenumbered permit forms and have a standard fee, it may be easier for someone to reconcile the number of permits issued to revenue recorded and determine if receipts are missing. In contrast, it may be difficult for someone to notice that an unexpected donation was taken.

Examples of unanticipated revenue

The types of unanticipated revenues vary among local governments, but some common ones are listed below. You can find a complete list of revenue sources in SAO's online Budgeting, Accounting and Reporting System (BARS Manual).

- Cemetery plot fees
- Title company payments
- Trash collection fees (transfer stations)
- Firearm permit fees
- Building permit fees
- Impact fees
- Passport service fees
- Seized property fees
- Donations
- License fees for businesses, animals, marriage, electrical
- Lease and/or rental space fees
- Pool-use fees
- B&O taxes
- Public records request copy fees
- Rebates
- Insurance payouts

Common ways this type of fraud happens

Employees can use numerous cash receipting schemes to take unanticipated revenue, depending on whether it comes in as cash or check. Here are the most common tactics.

Unanticipated revenue coming in as cash

Employees are likely to use skimming schemes for unanticipated cash. Skimming refers to schemes where cash is taken before it is recorded and deposited. The employee simply takes cash "off the top" of the money coming in that day, and never records the receipt of those funds in the accounting records. These schemes are more difficult to detect because no documentation exists. And with unanticipated revenue, it is likely no one would know it ever should have been receipted in the first place.

Unanticipated revenue coming in as check

With advances in banking such as remote deposit, it is easier to use skimming schemes for checks. In the past, employees likely would have had to visit the bank to deposit a check payable to the government into their personal account. This deterred many would-be fraudsters, as it increased the risk the banker would notice the check was payable to a government, not the depositor, and call the government to investigate. Remote banking removes that person-to-person interaction, allowing employees to simply deposit the government's check by taking a picture on their phone. Further, depending on the bank, it is possible no one ever compares the payee line to the account holder.

Check-for-cash substitution is the most common scheme

In Washington, check-for-cash substitution schemes are common for unanticipated checks. In this scheme, employees want to pocket cash, not the unanticipated check. To do this, they access cash received, such as a customer's utility payment. Employees take cash in the same dollar amount as the unanticipated check, then apply that check to the customer's account so it reflects an accurate balance.

In the B&O case discussed earlier, the fraudster was using a check-for-cash-substitution scheme. This kind of fraud is tricky to detect because it is so easy for the fraudster to simply pocket the cash and use someone else's check payment to make the register balance. And it is even harder to detect when the revenue is unanticipated.

Best practices for preventing this type of fraud

The key to preventing fraud or reducing your risk for it is having strong controls in place. However, when designing a system of internal controls over revenue, it is common for governments to focus the controls on significant and predictable revenue streams, which leaves control gaps over unanticipated revenue. Governments should be intentional in considering unanticipated revenue when building their control systems.

Here are some of best practices you should consider:

- **Require that two employees open mail together**

  Many unanticipated revenues – especially those in the form of checks – come in through the mail. A policy requiring that two employees (together) always open and receipt mail will reduce your staff's ability to take checks before they are receipted or substitute them for other cash.

- **Segregate duties**

  Segregating duties involves assigning responsibilities to employees in a way that reduces the risk of fraud or error occurring or going undetected. SAO's Segregation of Duties Guide provides in-depth strategies to help you segregate duties in accounts receivable, accounts payable, cash receipting, payroll, procurement and other areas, regardless of the size of your government.

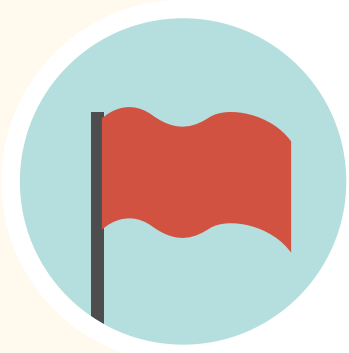
  When it comes to unanticipated revenues, governments should segregate these specific processes:

  > Receipting the actual payment

  > Reviewing the daily register/deposit for correct totals and payment methods

  > Depositing to the bank

  > Reconciling the bank account to the accounting system



- **Watch for behavioral red flags**

  Fraudsters typically exhibit warning signs if you know what to look for. According to the ACFE, the two most common red flags are living beyond one's means and financial difficulties. Other signs are unwillingness to share duties and complaints about inadequate pay.

- **Mandate vacations for staff and rotate assignments**

  Require staff to take vacations in blocks of time, such as one or two consecutive weeks, and remove system access temporarily, if possible, to prevent vacationing employees from performing tasks remotely. Ensure that other staff perform the work of the vacationing employees. By implementing mandatory vacations and having other staff fill in, you may uncover certain fraud schemes that require dedicated effort over time (such as lapping schemes) or even prevent a fraudster from executing a scheme in the first place.

- **Keep an eye open for potential unanticipated revenue sources**

  Start by developing a list of known revenue sources that come in at unexpected times or amounts, such as B&O taxes or cemetery plot fees. Add other potential unanticipated revenue, such as donations and rebates. Throughout the year, read your government's board and committee meeting minutes, as well as articles and other content from your local news outlets, blogs or community social media groups, which may tip off revenue coming your way, such as grants or donations.

- **Establish a written fraud policy**

  A well-crafted fraud policy is critical for communicating your government's anti-fraud stance, the expected process for reporting fraudulent actions, and what happens to those who commit fraud. Your policy should focus on deterrence, detection, and correction of misconduct and dishonesty. Consider requiring employees to sign a copy of the policy as an acknowledgement they have read and agree to abide by it.

- **Require annual fraud awareness training**

  A fraud awareness program trains employees to be mindful of fraud risks in their daily tasks. Your training should convey the importance of fraud prevention, train employees to spot red flags, and encourage them to verify details. According to the ACFE, providing fraud awareness training increases the likelihood that employees will identify and report fraud.

When a house is sold, the title company often adds any outstanding utility bills to the escrow payments. However, the homeowner might pay off the balance before the title company sends the check from escrow, resulting in two payments on the same balance. In one case we investigated, an employee responsible for receipting utility payments used several schemes to take these unexpected escrow payments.

Best practices for detecting this type of fraud

Despite a government's best efforts, it may not always be possible to prevent fraud involving unanticipated revenue. That's why it's imperative that governments have robust controls to detect these schemes.

Here are some best practices to consider:

- **Whenever possible, compare receipts to activity**

  Governments should use a prenumbered system to issue licenses and permits, such as building permits, firearm permits or dog licenses. Further, governments should accurately track assignment of land use, such as cemetery plots and airport hangar lots. Periodically, someone independent of receipting should reconcile the activity (list of assigned plots or number of sequential permits issued) to the receipts. For example, subtract the first permit number issued this month from the last to determine the number of permits your government issued. Then, multiply that number by the permit fee to determine expected revenue, and compare the dollar amount to the actual receipt activity in the accounting system.

- **Conduct proper reviews and reconciliations**

  Reviewing and reconciling receipted cash and check totals from daily receipts to deposits, the accounting system and bank accounts is a start, but governments should be looking at more during their reviews. Be sure to compare the payment method and amount to the actual accounts to which it was applied. If you see checks applied to more than one account, investigate it further to see if it makes sense. Also, make sure any voids and adjustments are supported and approved by a supervisor. A high volume of voids and adjustments, especially if unapproved and unsupported, is a red flag. And pay attention to any missing, incomplete, or altered documentation that can signal a fraudster is intentionally covering up something.

- **Consider randomly confirming business payments**

  Request various businesses provide you with a summary of the total amounts they have paid you. Compare their information to amounts recorded in your accounting system.

One case in Washington shows the increasingly negative effects of these schemes. After an employee used a check-for-cash substitution scheme to take cemetery plot fees, the city examined the plot map and registry and was unable to determine if the employee recorded plots sold, or simply took the cash from the sale and never recorded it. The city now worries it has sold the same lot to more than one person.

- **Conduct surprise cash counts**

  Surprise cash counts keep fraudsters on their toes and may deter them from executing their scheme. When conducting a surprise cash count, make sure to pay attention to the checks and what accounts they get applied to, as well as the cash on hand. Ask questions as necessary.

- **Pay attention to customer complaints**

  According to the ACFE, tips from customers or other employees are the most common method for detecting fraud. With unanticipated revenues, customers do not receive a bill for services or build an account balance with the government – common avenues for a customer to notice something is awry. However, customers can still pick up on important red flags because some unanticipated revenues schemes, such as check-for-cash substitution, may subtly affect their bills for other services. Pay attention and listen if you receive a complaint (e.g., a customer was not given a receipt for payment, or something just does not look right). Also, consider periodically reminding customers to closely review their bills for anomalies, such as check payments applied to their accounts when they typically pay cash.

- **Analyze and trend unanticipated revenues**

  Compare current unanticipated revenues to prior years to see if there are any anomalies. Consider drilling deeper into customer or vendor accounts, paying attention to any significant decreases in revenues. Follow up on any unexpected missing payment with the customer to verify if a payment was made. If the unanticipated revenue involves the sale of an asset (e.g., cemetery plots), compare the inventory to the revenue coming in and determine if it makes sense.

What to do if you suspect fraud

Washington state law (RCW 43.09.185) requires all state agencies and local governments to notify SAO immediately if staff suspects or knows that a loss of public resources or other illegal activity has occurred. When this happens, state agencies and local governments should take the following actions:

- Report the loss to SAO using the form on our website.
- Protect your accounting records. Secure all original records related to the loss in a safe place until we have completed our investigation.
- Notify others who need to know. This may include the governing body, agency head or deputies, chief financial officer, or internal auditor, depending upon the circumstances.
- Notify your legal counsel.
- File a police report with the appropriate local or state law enforcement agency when advised to do so by SAO.
- Read and follow SAO's guidance before entering into any restitution agreement with an employee.

Additional resources:

- SAO's Resource Library offers a variety of free guides, checklists, and best practices to help Washington's governments improve their internal controls to prevent fraud.

- SAO's Preventing Fraud webpage contains multiple internal control assessment tools, guidebooks, free training links, and additional resources to help combat fraud related to cash receipting.

For assistance

This resource was developed by the Office of the Washington State Auditor. Please send any comments, questions or suggestions to the Special Investigations Team at Fraud@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.