



# Follow ☆☆☆ the ☆☆☆ money

A practical guide to reviewing  
government bank statements  
to stop fraud in its tracks



Office of the Washington State Auditor

September 2025



# Table of Contents


<a href="#">The monthly bank statement: An essential tool to monitor your government's financial activities</a>	3
<a href="#">Basics of banking and bank statements</a>	4
• <a href="#">Case study warnings</a>	
• <a href="#">Where to obtain statements</a>	5
• <a href="#">What a bank statement can tell you</a>	5
What your bank statement is telling you:	
• <a href="#">About deposits</a>	6
• <a href="#">About withdrawals</a>	9
<a href="#">What to do if you spot a red flag</a>	19
<a href="#">The 30-minute Follow the Money approach</a>	20

## Use FIT to check the fitness of your government's financial health

The State Auditor's Office has a free tool you and your community can use to monitor your government's financial condition. The Financial Intelligence Tool <https://portal.sao.wa.gov/FIT/explore> is based on the financial statement you are required to file with us annually; it is due 150 days after the government's fiscal year end. (In most cases, that means May 30.)







# The monthly bank statement: An essential tool to monitor your government's financial activities

A bank statement is one of the most valuable tools available to help you monitor your government's financial activity. This independent record of your financial transactions is an essential tool because of the depth of information it contains. Bank statements show all transactions affecting a government's flow of money, whether they are income or spending.

The Office of the Washington State Auditor has investigated many losses governments could have detected sooner – if only someone had looked at their bank statements. Whether you are a finance professional, a department head, or even an elected or appointed official, regularly reviewing your monthly statements can greatly increase the odds of deterring and detecting fraud.

A simple scan of banking transactions can reveal unusual transactions, especially if you review the statements every month and develop a baseline expectation of activity. Reviewing can be the difference between deterring loss and identifying it early, or having it go undetected for a long period of time.

To help you stop potential fraud, we have designed an approach to statement reviews that can take as little as 30 minutes a month. Our 30-Minute Follow the Money template outlines all the steps – print or save a copy each month to start protecting your government's money. Done regularly, it's an activity you can bank on!

## Other helpful resources

[Bank statement review is a top-notch fraud-fighting tool. Our Office shows you how to do it \(blog article\)](#)

[Best Practices for Bank Reconciliations \(PDF\)](#)

[Trust, but verify: A guide for elected officials and appointed boards to prevent and detect fraud \(PDF\)](#)





# Basics of banking and bank statements

## Who should have access to bank accounts, including debit or credit cards and statements

Access to a government's bank account (and other financial products, listed in the sidebar) should be carefully controlled and granted based on business need.

If you don't already have a master list of who is permitted access to your government's money, that's a good place to start. List everyone who has been issued a debit card or credit card, and who maintains online account access for creating and processing electronic bank account transactions.

Then, review this list periodically. Has someone changed to another job function or left the government through retirement or a new job elsewhere? If so, be sure to remove their access to your online banking accounts by telling the bank promptly. Don't forget to cancel credit or debit cards held in the employee's name or to which they had access.

## Case study warnings

We have investigated many losses where management or the board were unaware an employee obtained a debit card or credit card to use for making purchases, because no one reviewed who had bank account access. And because no one carefully reviewed the bank statements, unauthorized spending went undetected for months – or years – as the employee made multiple personal purchases.

We have also seen several cases where a government did not remove a former employee's bank access promptly, and the government suffered additional losses because the person still had the ability to make personal debit card or credit card purchases, log in online to the government's bank account to create and process electronic payments to their personal accounts, or even make cash withdrawals.

**Consider all these types of financial products when you think about "banking access"**

- Checking and savings accounts
- Online banking login credentials
- Existing physical debit or credit cards and their account numbers/PINs, including the ability to change billing or payment details
- Checkbooks and deposit/withdrawal slips
- The ability to open new credit cards
- Investment accounts connected to your day-to-day bank

### Case studies

Simple secondary reviews of bank statement activities could have identified these losses sooner.

- [Town of Cusick Fraud Investigation Report, issued April 18, 2024 \(PDF\)](#)
- [City of Morton Fraud Investigation Report, issued August 26, 2024 \(PDF\)](#)
- [Washington Counties Insurance Fund Fraud Investigation Report, issued April 7, 2025 \(PDF\)](#)



# Where to obtain statements

Bank statements are an independent record from the accounting system that can instantly reveal a potential misappropriation. Original bank statements are best for review. This way, your examination starts off right, and you have confidence no one could have altered the statements.

Ideally, you should download statements from the bank's website yourself. Opening the mail containing the printed statement yourself also minimizes any risk someone might have tampered with the statement the bank issued. If for some reason you couldn't obtain a statement firsthand, you'll need to look more carefully at electronic or print documents to ensure they are genuine and intact.

**Original bank statements are best for review**

Here are some typical red flags indicating someone may have altered a statement:

- Inconsistent formatting or alignment of rows, sections or columns
- Missing bank header, footer or page numbers
- Mathematical or date errors: for example, incorrect statement periods or a beginning balance that differs from the ending balance on the previous statement
- Nonsequential checks without notation. Banks often indicate a gap in check sequence with an asterisk or other symbol. Missing symbols could indicate someone altered the statement to remove a check they didn't want anyone to notice was missing.

## What a bank statement can tell you

Examining a government's bank statements may seem like a daunting task, but it isn't really much different from checking a bank or credit card statement at home. You're looking for something out of the ordinary: Hey, I wasn't in California in June, so why does my statement show the purchase of Disneyland tickets?

Once you know the basics of each common area on the statements, you can narrow your focus and shorten the amount of time it takes for review. This is made easier because all bank statements follow a consistent format. While the design may vary from bank to bank, all have three basic areas in common.

1. **Bank and account information.** At the top of the first page, you should see the bank's name and logo, the statement beginning and ending period, and account information and numbers.
2. **Summary section.** Also on the first page: a summary showing the account's beginning balance, total deposits, total withdrawals and an ending balance.
3. **Transaction activity.** Transactions are typically broken into categories, such as deposits, electronic transactions and checks. Each category will display information in a standardized format that includes the date, transaction description and amount.

Now that you know the basics about your government's bank statement, you can think about asking it some tough questions – the kind fraudsters really hope you won't bother asking.





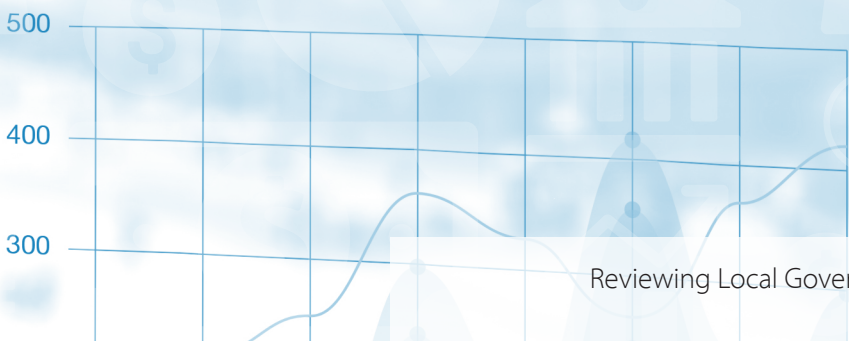
# What your bank statement is telling you: About deposits

Governments should have sufficient cash in the bank to cover expenses. Bank statement deposit activity demonstrates the flow of money into a government's accounts. By familiarizing yourself with typical monthly income shown in the statements, you'll be prepared to notice if there's less cash than typical for any given month. This can be a red flag that a fraudster is diverting cash receipts or authorizing inappropriate bank account transfers to personal accounts.

**Table 1**, which starts on the following page, lists the most common types of deposits you might see on a bank statement with a short description of each. The last column of the table offers some questions you might ask yourself to decide if a deposit seems unusual to you. For auditors, they might raise a red flag. Here are a few examples to get you started as you review deposit activity on every month's statement.

- Evaluate the frequency of deposits and whether it meets your government's policies and expectations. Possible red flag: Weekly or inconsistent deposits at a government that requires daily deposits.
- Examine the dollar amounts deposited and whether they are whole-dollar amounts or include change. Possible red flag: A string of deposits in whole-dollar amounts at a government that bills dollars and cents would be unusual, and possibly a red flag.
- Consider spot-checking the month's total deposit amount on the statement to an accounting system report of total deposits recorded. Possible red flag: Deposits missing from the bank statement that appear in the accounting system.

	\$ (1,161)	\$ (193)
	<u>          </u>	<u>          </u>
	3,077	1,450
	(852)	(291)
	\$ 2,225	\$ 1,159
	<u>          </u>	<u>          </u>





## Table 1: Types of deposits on a bank statement

The notation [4-digit account number] refers to the last four numbers of whatever bank account or credit card statement you're reviewing.

Transaction label	Description	What to know	Ask yourself...
Deposit	Deposit of cash and checks	Deposits made physically at the bank for deposit, by handing it to a bank teller, dropping it in a night box or putting it into an ATM deposit terminal.	<ul style="list-style-type: none"><li>• Do the total amounts match the expected accounting system total receipt records for that day's deposit?</li><li>• Does the bank cash deposit amount match the total cash receipt records for that day's deposit?</li></ul>
Remote Capture Deposit	Deposits of checks made somewhere other than at the bank	Typically, someone at your government scans individual checks using a check scanning device. The device takes a photo of the check to support an electronic deposit. Note: You should physically retain the original checks on file at your offices to support the electronic deposit transaction.	<ul style="list-style-type: none"><li>• Do the total amounts match total check amounts recorded in the accounting system for that day's deposit?</li><li>• Does the original check payee information match what is recorded in the accounting system?</li><li>• Are original checks properly retained to support the remote deposit in case there is a discrepancy with the bank?</li></ul>
ACH Credit Settlement Bankcard	Automated Clearing House credit card payments to you	Typically customer credit card payments for various services, such as utility payments.	<ul style="list-style-type: none"><li>• Were these amounts properly recorded in the accounting system?</li><li>• Do the amounts received agree to customer accounts?</li></ul>

*Continued on page 8*

**Table 1: Types of deposits on a bank statement**

The notation [4-digit account number] refers to the last four numbers of whatever bank account or credit card statement you're reviewing.

Transaction label	Description	What to know	Ask yourself...
ACH Credit (Vendor Name)	Automated Clearing House payment received from a vendor	Payments received from a vendor for various revenue or funding purposes. They can include grant funds received or business and occupation tax revenues.	<ul style="list-style-type: none"> <li>Do you recognize all the vendor names as companies you do business with?</li> <li>Was the deposit properly recorded in the accounting system, and are there supporting records on file?</li> </ul>
Transfer from [4-digit account number]	Deposit from a different bank account	Electronic transfer of funds to your government from a different bank account. The last four digits identify the originating bank account number.	<ul style="list-style-type: none"> <li>Is the listed four-digit account number associated with an account known to the government?</li> <li>Is this transfer recorded in the accounting system, and are there records on file to support the purpose of the transfer transaction?</li> <li>Who has access to make this transfer and was it authorized?</li> </ul>
Automatic Transfer from [4-digit account number]	Automated transfer of funds	Transfer deposits from one account to another that do not require individual action or approval. Typically set up to occur routinely, on an expected date, and typically for a set amount. They might include payroll sweeps to cover payroll amounts processed or to a loan account number to pay off a loan. Automated sweep transfers should all be received from account numbers known to the government.	<ul style="list-style-type: none"> <li>Is the listed four-digit account number associated with an account known to the government?</li> <li>Is this transfer recorded in the accounting system, and are there records on file to support the purpose of the transfer deposit?</li> <li>Who has access to set up automatic transfers, was the transfer set up properly, and was it authorized?</li> </ul>



# What your bank statement is telling you: About withdrawals

Government expenses should be for a valid business purpose, properly approved, recorded in the accounting system, and supported by records on file at the government. By examining typical expenditure transactions in the monthly bank statement, you'll be better prepared to recognize expenditures that are out of the ordinary – possible red flags that money is flowing out of your accounts and into the wrong hands.

Three types of withdrawal transactions appear on most monthly statements:

1. Electronic withdrawals (a category that includes debit cards and wire transfers)
2. Check payments clearing the bank
3. Bank fees or corrections

In this chapter, we look at them one by one, highlighting what you can consider normal and what questions to ask about those transactions you should consider less common and therefore riskier.

## 1. Electronic withdrawals, including debit cards and wire transfers

For more than a decade, state and local governments have been moving away from traditional paper checks to more efficient and lower-cost digital payments. These electronic payment methods include Automated Clearing House (ACH) payments, electronic funds transfers (EFT), electronic withdrawals and wire payments. Many governmental associations (including the National Association of Counties and the Government Finance Officers Association) say that the benefits of electronic banking are clear: you can pay a variety of vendors seamlessly, process employee payroll faster and easily transfer money between multiple bank accounts.

Nonetheless, government leaders should be aware that digital payments can also create new opportunities for employees to conceal their misappropriation. For example, employees with access to the payment system can simply change a vendor's banking information to divert payments to their personal bank account.

It is important to put compensating protections in place for this type of banking activity. One protection that is directly related to reviewing electronic withdrawal activity on your monthly bank statements is to maintain a list of known bank accounts – yours and the vendors you regularly do business with. Use the list to spot-check against electronic transfer accounts listed on the statement: it will help you verify these accounts are appropriate to pay.

ent

Account No.:

Amount

54.00

16.00

32.00

21.00

21.00

44.00

28.00

34.00

22.00

### A special note about debit cards

Debit cards are a particularly risky digital payment method for governments, because the money is withdrawn immediately from your account balance, unlike a credit card which allows dispute resolution before you pay the card balance. In fact, the [Municipal Research and Services Center](#) advises local governments in Washington that they are not authorized to use debit cards because the immediate withdrawal of public funds would be inconsistent with the state's requirements for voucher review payment procedures. If you see debit card activity during a bank statement review, first double-check whether your government's policy allows a debit card to be set up and if someone did so with proper approval. If your policies do allow staff to use debit cards, review debit card transactions in the bank statement especially carefully. And remember, any debit card use at an ATM is a red flag you should follow up on.

**Table 2** lists the most common types of electronic withdrawals you might see on a bank statement with a short description of each. The last column of the table provides some questions you might ask yourself to decide if a withdrawal seems unusual to you. For auditors, they might raise a red flag.

**Table 2: Types of electronic withdrawal transactions on a bank statement**

The notation [4-digit account number] refers to the last four numbers of whatever bank account or credit card statement you're reviewing.

Transaction label	Description	What to know	Ask yourself...
ACH Debit (Vendor Name)	Automated Clearing House payment made electronically to a vendor account directly from your bank account	A common method of paying vendors for services provided or to purchase business operational items without writing a check. Because it only shows the vendor name and not the account number paid, there is a risk that while the name on the statement appears to be a legitimate vendor, the underlying transmittal receipt record could show the payment was diverted to a personal bank account by the employee responsible for disbursing the payment.	<ul style="list-style-type: none"><li>• Do you recognize the vendor name as a company you do business with?</li><li>• Does the bank account listed on the transmittal receipt where the funds were paid to agree to the bank account record the vendor requested funds be paid to for services provided?</li><li>• Is the vendor name "Visa payment"? If so, confirm this was a payment properly applied to your government's credit card company.</li></ul>

*Continued on page 11*



**Table 2: Types of electronic withdrawal transactions on a bank statement**

The notation [4-digit account number] refers to the last four numbers of whatever bank account or credit card statement you're reviewing.

Transaction label	Description	What to know	Ask yourself...
ACH Debit [4-digit account number] Funds Transfer to Dep [4-digit account number]	Automated Clearing House electronic transfers, from the account you are examining to another bank account	The destination account where the funds transferred to should be a known bank account held in the government's name.	<ul style="list-style-type: none"> <li>Do you recognize the destination four-digit account number?</li> </ul>
EFT Automatic Transfer to [4-digit account number]	Electronic Funds Transfer: Automatic transfer within the bank, from the account you are examining to another account	Typically, these automatic transfers are set up to occur routinely, on an expected date, and typically for a set amount. The destination account number should be a known account held in the government's name.	<ul style="list-style-type: none"> <li>Do you recognize the destination four-digit account number?</li> </ul>
PreAuthorized WD [Vendor name]	A withdrawal authorized to pay a vendor	Payments set up and preauthorized by your government with your bank, using its online bill pay system. The vendor name should be for a known vendor.	<ul style="list-style-type: none"> <li>Do you recognize the vendor name as one you do business with?</li> <li>Who has access to set up vendors through your bank, and was this an authorized payment?</li> <li>Are there supporting records on file to verify this was a legitimate expense to pay?</li> </ul>

Continued on page 12



## Table 2: Types of electronic withdrawal transactions on a bank statement

The notation [4-digit account number] refers to the last four numbers of whatever bank account or credit card statement you're reviewing.

Transaction label	Description	What to know	Ask yourself...
Debit purchase  (Business name) [4-digit account number]	A debit card was used to make a purchase at a physical or online business	The transaction description shows the business name and the last four digits of the debit card used to make the purchase. In general, debit cards are a risky method of payment for governments, because payments from them are immediately deducted from your bank account. Carefully examine this activity.	<ul style="list-style-type: none"> <li>• Who made the purchase?</li> <li>• Do you recognize the shop or business name?</li> <li>• Where was the purchase made, and is it reasonable for your government's location?</li> <li>• Does the transaction date reflect a weekend or holiday?</li> <li>• Is there a receipt on file to support the purchase?</li> <li>• Was the amount properly recorded in the accounting system?</li> </ul>
ATM or OTC	<p>Cash withdrawal</p> <p>ATM = a debit card or cash card was used to access the account and withdraw cash at an automated teller machine</p> <p>OTC = over the counter cash withdrawal processed physically at the bank</p>	Government staff should never need to withdraw cash from ATMs or use debit cards at the bank, and state law prohibits cash withdrawals from credit cards. If a government needs cash (for example to stock an event cashbox), staff should write an accounts-payable check and cash it at the bank so there is a traceable record of the transaction. Examine any ATM cash withdrawals very carefully.	<ul style="list-style-type: none"> <li>• Who withdrew the cash?</li> <li>• Why did they do so?</li> <li>• What happened to the cash once withdrawn from the account?</li> <li>• What supporting records are on file to demonstrate how the cash was used?</li> </ul>

Continued on page 13



## Table 2: Types of electronic withdrawal transactions on a bank statement

The notation [4-digit account number] refers to the last four numbers of whatever bank account or credit card statement you're reviewing.

Transaction label	Description	What to know	Ask yourself...
Debit Memo	Bank deposit correction indicates the bank made a change to a deposit that it already processed, either to add or subtract funds. It can happen for several reasons, such as an error in the original deposit or a failed electronic transaction.	When a “bank deposit correction” is shown as a debit on the statement, it means the amount your deposit slip listed as being physically or remotely deposited was more than the amount the bank calculated for deposit.	<ul style="list-style-type: none"> <li>• Can you determine why a deposit required correction?</li> <li>• Who was responsible for the deposit that the bank corrected?</li> <li>• What amount was recorded in the accounting system related to the correction?</li> <li>• Are there supporting records on file to explain the correction, and does the support make sense?</li> </ul>
Wire Withdrawal	Wire transfer of cash from your bank account and deposited into another bank account.	The transaction description should list the payee’s name and four-digit destination account number. This is an uncommon method for a government to use to pay a bill. The risk: wire transactions can be easily used to send funds out of state and out of country. Scrutinize any wire withdrawals thoroughly.	<ul style="list-style-type: none"> <li>• Did you expect this transaction?</li> <li>• Is the payee’s name that of an employee or an employee’s relative?</li> <li>• Does the four-digit number identify an account known to the government?</li> <li>• Are there supporting records on file for review?</li> </ul>

### A warning about digital payment platform transactions

In today's digital world, where convenience and speed are highly desirable, digital payment platforms are a quick, convenient way to send, receive and request money from individuals and businesses. For governments, however, they can be particularly risky for a variety of reasons. Key among them: the funds held in digital payment apps are unlikely to be federally insured, as bank funds are. User agreements for digital payment apps often lack information on where funds are being held or invested, and what would happen if the company or the entity holding the funds were to fail.

When it comes to government banking, digital payment apps should not be an expected way to pay vendors. That means that if you see this type of transaction activity on a bank statement, you should consider it **an immediate red flag**. Any cash transactions made through digital payment apps should be thoroughly scrutinized.

**Table 3** lists a few examples of digital payment app names that might appear on your government's bank statements.

Table 3: Types of digital payment app transactions on a bank statement		
Digital payment app name	Transaction label	What to know
Square Inc.	SQ*	Transaction will start with SQ* and then typically include a shortened business name or individual's name
Western Union wire payment	WU*	Transactions will include a WU* somewhere within it and include numbers, which is the receipting transaction information.
PayPal Inc.	Paypal *	Transactions will include the transaction label and then a shortened business name or individual's name.
Zelle Inc.	Zelle Instant	
Apple Inc.	Apple pay	
Instacart	IC*	



## 2. Check payments clearing the bank

A check has “cleared” when the bank has transferred the money to the payee shown on the check. Bank statements typically group checks in one section. This section will list all checks paid from your government’s checking account for the statement period. Your review of this section should help confirm that all cleared checks were written for legitimate business purposes.

If your monthly bank statements do not include copies of cleared checks, consider asking your bank to include check images with each statement. This can help streamline your review of cleared checks, because you can readily identify the name of the payee who received the check as well as who authorized it – making it easier to compare check details with information recorded in the accounting system.

Another option to discuss with your bank is setting up “positive pay” for your government’s checking account, which is a service banks offer that allow them to match checks issued by the government with those presented for payment. The bank will return suspicious checks to the issuer for examination, helping you protect against unauthorized checks.

**Table 4**, which begins on the following page, lists the most common types of check payments might see on a bank statement with a short description of each. The last column of the table offers some questions you might ask yourself to decide if that check seems unusual to you. For auditors, they might raise a red flag.



**Table 4: Types of check payment transactions on a bank statement**

Transaction label	Description	What to know	Ask yourself...
Check numbers, 4 or 5 digits	Typically listed in order from smallest to largest dollar amount. Gaps in the numerical sequence of check numbers are marked by an asterisk (*) or other symbol.	<p>Whether handwritten or printed by the accounting system, numbered checks are the most common type issued by a government. Typically, they are payments to vendors or reimbursements paid to employees.</p> <p>Checks listed in your accounting system as voided but listed on the bank statement as having been cashed are not expected and should be examined.</p>	<ul style="list-style-type: none"><li>• Do any dollar amounts stand out as unexpected, for example are any even-dollar amounts?</li><li>• Does the volume of checks make sense given current operations?</li><li>• Is there a gap in check sequence (shown by an asterisk or other symbol)?</li><li>• Do any check numbers voided in the accounting system appear as having cleared the bank?</li></ul>
Check numbers longer than 5 digits	Typically an electronic check created by your bank and then paid out either by physical check or electronically by the bank	<p>The bank will only process this kind of check if someone with online banking access requested and set up the payment to be processed. This would require them to enter the payee's name, address information, the amount to be paid, and the date the bank should prepare to send out the payment. These payments are completed using the bank's online bill payment system. These can be set as a one-time payment option or on a regular payment schedule with a specified date and amount.</p>	<ul style="list-style-type: none"><li>• Who has access to set up bill payments through your bank?</li><li>• Was this an authorized payment?</li><li>• What supporting records are on file to verify this was a legitimate expense?</li></ul>

### 3. Bank fees or corrections

Most often banks will assess monthly bank fees for basic maintenance or services based on the type of account. Other fees could be considered red flag indicators for fraud. Below are some types of fees you may commonly see on the bank statements and others to be on the lookout for.

**Table 5** lists the most common types of fees you might see on a bank statement with a short description of each. The last column of the table offers some questions you might ask yourself to decide if fee charged seems unusual to you. For auditors, they might raise a red flag.

**Table 5: Types of service fees on a bank statement**

Transaction label	Description	What to know	Ask yourself...
Service fees or monthly maintenance fees	Common fees charged by the bank for the account services it provided	Service fees vary by bank and account type and are usually the same amount every month.	<ul style="list-style-type: none"><li>• Is the fee standard month-to-month? If not, why has it changed?</li><li>• Does the amount match expected service fees set out in the banking contract agreement?</li></ul>
Fees: - Overdraft - Returned check - Insufficient funds	Penalty fees assessed by the bank to cover shortfalls or other checking account problems	Such fees should be very uncommon as they indicate the government's account lacked sufficient cash when a check was paid out.	<ul style="list-style-type: none"><li>• Such fees on the bank statement always warrant further research into the purpose of the fee, and why it was incurred, to better understand the reason behind the unexpected expense.</li></ul>

*Continued on page 18*





**Table 5: Types of service fees on a bank statement**

Transaction label	Description	What to know	Ask yourself...
ATM fees	Fee associated with an ATM cash withdrawal transaction	As already noted, government staff should not withdraw cash using an ATM, especially at one that is not connected to the bank. The fee date indicates an ATM cash withdrawal transaction close to the date the fee was applied.	<ul style="list-style-type: none"> <li>• Is the related cash withdrawal transaction also listed on the statement?</li> <li>• Then ask the same questions as for any ATM withdrawal: <ul style="list-style-type: none"> <li>◦ Who withdrew the cash?</li> <li>◦ Why did they do so?</li> <li>◦ What happened to the cash once withdrawn from the account?</li> <li>◦ What supporting records are on file to demonstrate how the cash was used?</li> </ul> </li> </ul>



# What to do if you spot a red flag

## 1. Research the transaction further by taking one or more of these steps:

- Review the statement for similar transactions, and **make a list** of dates, amounts and any other transaction details that might be important to note. Then review several previous statements – do similar transactions appear in the past?
- **Discuss the transaction with the employee** who handled the transaction. If the employee can only provide a verbal description of its purpose, consider that the information may not be true. If you're concerned, take another step to verify what they described by reviewing supporting documentation.
- **Pull the original invoice** or other records that should be on file to support the transaction and its business purpose. If there is no support on file, this is an issue that will need to be resolved.
- **Call the bank directly** to learn more about the transaction. Bank staff are independent of anyone from your government and will not attempt to conceal the purpose of a transaction.



## 2. Notify our Office

Washington state law (**RCW 43.09.185**) requires all state agencies and local governments to notify the State Auditor's Office immediately if staff suspects or knows that a loss of public resources or other illegal activity has occurred. In the unfortunate event that your government appears to be the victim of a fraud or loss, we recommend you take the following actions:

- **Protect your agency's accounting records.** Secure all original records related to the loss in a safe place until our auditors have completed their investigation. For example, you should secure backup copies of computer records and original paper records related to the situation in a vault, safe or locked cabinet until the investigation is complete.
- **Notify others who need to know.** This might include other governing board members, department managers or financial officers, depending on the circumstances.
- If you suspect a particular person of involvement in the loss, notify the bank immediately to **remove the employee's access** to your government's bank account. If necessary, cancel credit or debit cards issued in that person's name.
- **Report the loss to our Office** using [the fraud reporting form on our website](#). Even if you do not have all the information yet, report the loss as soon as you can. You can always update a loss report when you have more information to share.
- **Notify your legal counsel** and file a police report with the local or state law enforcement agency, if appropriate.
- If you decide to confront the employee suspected of misappropriation, **do not enter into a restitution agreement** with that person before an investigation has established the amount of loss. Under state law (RCW 43.09.260), local governments must obtain written approval from our Office and the Attorney General's office before they make any compromise or settlement of loss claims covered by RCW 43.09.185.

# The 30-minute Follow the Money approach

## Set your timer and get ready to improve your government's banking health!

If this is a relatively new practice for you, review the "What your bank statement is telling you" sections earlier in this handbook to refresh your memory about what kinds of questions you should ask yourself if a transaction looks a little – or a lot – unusual.

Time	Monitoring task	Notes from review
2 mins	Know the source of records, check the box that applies: <input type="checkbox"/> Used online bank access to print own copy <input type="checkbox"/> Received in mail and opened myself <input type="checkbox"/> Someone other than the bank emailed me a copy <input type="checkbox"/> Someone other than the bank provided me a hard copy	
0-5 mins  *Skip if original bank statements obtained.	Assess risk for alterations by reviewing for:  1. Inconsistent formatting or alignment of rows, sections or columns  2. Missing or blank pages  3. Mathematical errors: Last month's ending balance statement should be the same as the beginning balance of the new month's statement	
8 mins  (2 mins each check mark)	Scan deposits section  ✓ Assess the overall bank account balance and your current financial condition. Possible red flag: Missing deposits if the account balance at any point during the statement period appears lower than expected.  ✓ Evaluate the frequency of deposits and whether it meets your government's policies and expectations.  ✓ Examine the dollar amounts deposited and whether they are whole-dollar amounts or include change.  ✓ Consider spot-checking the month's total deposit amount on the statement to an accounting system report of total deposits recorded. Are any deposits missing from the bank but present in the system? Does the bank cash deposit amount of the deposit match the total cash receipt records for that day's deposit?	



Time	Monitoring task	Notes from review
10 mins  (~ 2 mins each check mark)	<p>Scan typical withdrawal activity</p> <ul style="list-style-type: none"> <li>✓ Scan electronic transfer activity. Focus on account numbers where money has been transferred to. Verify that these are known bank accounts for your government.</li> <li>✓ Examine ACH payment activity for reasonableness. Scan the vendor names listed: only expected vendors should receive ACH payments.</li> <li>✓ Spot check ACH group (known as a batch) transactions by examining supporting bank transmittal receipts to see which vendors or employee payments were included in the batch. Double-check vendor bank account numbers on the transmittal receipt agree with the vendor bank account listed on file.</li> <li>✓ Review debit card activity. Look at date, location, amount and vendor name. Examine supporting receipt records to determine what was purchased and the business purpose, and confirm they have been recorded in the accounting system.</li> </ul>	
4-5 mins	<p>Scan cash withdrawals, digital payment app transactions and fees</p> <ul style="list-style-type: none"> <li>✓ (2 mins) Scrutinize any cash withdrawal transactions. Review underlying support to determine the purpose or need for this type of activity, which should be rare.</li> <li>✓ (1 min) Scrutinize any digital payment app transactions. Review underlying support to determine the purpose or need for this type of activity, which should be rare.</li> <li>✓ (1 min) Look for any fees or charges applied on the account and whether they appear reasonable. Late fees or penalties should be rare.</li> </ul>	
3-4 mins	<p>Scan check withdrawals</p> <ul style="list-style-type: none"> <li>✓ (2 mins) Review list of cleared checks, scanning the dollar amount of the checks. Question whole-dollar amounts, volume of checks and reason for nonsequential checks. Examine supporting records to determine the purpose of the payment and whether it was properly authorized.</li> <li>✓ (1 min) Review list of voided checks and ensure none of the check numbers listed show as having cleared. Research any discrepancies.</li> </ul>	



"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

[www.sao.wa.gov](http://www.sao.wa.gov)

1-564-999-0950



Office of the Washington State Auditor