Payment-Fraud Prevention and Internal Controls

A Practical Guide for Small Government Finance Offices

IntelliPay®

Two high-consequence risks for small government finance offices are external payment-redirection fraud and internal fraud enabled by weak independent review.

Five habits close most of that gap:

1. Verify every vendor or payroll bank change by calling a number you already had on file.
2. Adopt a written "no bank changes by email" policy.
3. Keep a vendor and payroll change log that a second person reviews.
4. Have someone who never touches the money review bank statements every month.
5. Reconcile processor settlements to the bank to the general ledger on a fixed schedule.

None of this requires new staff or new software.

IntelliPay®

Why This Is a Small Government Problem

Business email compromise (BEC) caused $3,046,598,558 in reported losses in 2025, from 24,768 complaints, according to the FBI's Internet Crime Complaint Center. Local governments are regular victims:

- Baltimore, MD lost more than $800,000 after a fraudster tricked accounts-payable staff into changing a vendor's bank account information
- In May 2026, Harpswell, ME reported sending $189,999 to a scammer posing as a legitimate vendor.
- Arlington, MA lost $445,945.73 when criminals impersonated a school-project vendor and redirected four monthly municipal EFT payments
- Eagle Mountain, UT , lost nearly $1.13 million after criminals impersonated a road-project contractor and redirected an ACH payment

Insiders are a second, quieter risk. In 2025, the Washington State Auditor reported an increase in fraud investigations at small local governments where employees have access to public funds without appropriate reviews. One case was a town of fewer than 100 residents that lost more than $79,000 to its own clerk-treasurer.

That figure is not an outlier. The Association of Certified Fraud Examiners (ACFE), the global body that certifies fraud examiners and publishes the largest study of occupational fraud, analyzed 2,402 real cases from 143 countries for its 2026 Report to the Nations.

Government and public administration cases carried a median loss of $100,000, close to the $104,000 median across all industries. Broken out by level of government, local governments came in at a $79,000 median almost exactly what that one small town lost.

Municipalities of all sizes are subject to cyberattack and must be aware of the risks and understand what to do to mitigate them.

Broken out by level of government, local governments came in at a $79,000 median almost exactly what that one small town lost.

One set of controls covers both risks. GFOA advises that whoever enters or approves a vendor change should not also verify it, and that a supervisor should review vendor changes.

A second set of eyes stops an employee from acting alone, and it gives a fake bank-change request one more place to fail.

Small organizations are often less likely to maintain a formal fraud-reporting mechanism, such as a hotline, even though employee and third-party reporting can be critical. In the Association of Certified Fraud Examiners' Occupational Fraud 2026: A Report to the Nations, tips were the initial detection method in 43% of occupational-fraud cases—the most common detection method identified.

Only one-quarter of organizations with fewer than 100 employees had a reporting hotline, versus 85% of organizations with 100 or more employees. Yet tips were the initial detection method in 43% of cases in the ACFE's Occupational Fraud 2026: A Report to the Nations. (pp. 24 and 29; Figures 10 and 14).

In the Association of Certified Fraud Examiners' Occupational Fraud 2026: A Report to the Nations, organizations without a reporting hotline had a median occupational-fraud loss of $200,000, compared with $100,000 for organizations with a reporting hotline. (p. 29, Figure 14).

For a small agency, that can be an outside hotline vendor, or a designated elected official or outside CPA who sits outside the finance office. Part 4 covers how.

Part 1: Vendor Payment Fraud and BEC

How it works:

1. **Research.** The attacker finds a real vendor from your public contracts, board packets, or a compromised email account.
2. **The request.** You receive a polite email, a "voided check" or a change form asking to update the vendor's bank account.
3. **The payment.** Your office pays the fraudster on the next ACH or wire run. The real vendor calls weeks later asking why they haven't been paid.

What it looks like in practice

In Baltimore, the fraudster submitted a fake supplier contact form using a real vendor employee's name and a personal email address. An employee approved it without verifying the identity, because policy didn't require that at the time.

Fake voided checks and bank change requests followed, and the vendor's account was switched to the fraudsters by Feb. 19. The city sent $803,384.44 on Feb. 21 and $721,236.60 on March 10. The scheme diverted $1.52 million, and about $721,000 was recovered.

The inspector general noted that policies did not require phone verification of vendor contacts or bank changes.

That's the lesson. The staff weren't careless. The process had no verification step.

That's the lesson. The staff weren't careless. The process had no verification step.

Control 1: Call-back verification checklist

Use this for every request to add or change bank details, mailing addresses, or payee names.

- Do not reply to the email or use any phone number, link or contact in the request.
- Look up the vendor's number from your original contract, W-9 file, or a vendor record created before the request.
- Call and speak to a person you have dealt with before. Ask them to confirm the change, the new bank name, and the last four digits of the new account.
- Confirm the caller has authority. Compare against the vendor's signatory list on file.
- Record who you called, at what number, when, and who confirmed it.
- A second employee reviews the record before the change goes live.
- Where practical, send a small test payment or hold the first payment 24 hours after a change—without bypassing controls.

The Government Finance Officers Association recommends requiring vendors to provide both the old and new bank routing and account numbers when requesting a banking change. GFOA also recommends independently calling the vendor, using contact information already on file, to verify the existing and revised payment details.

Control 2: A "no bank changes by email" policy

Adopt it in writing, adopt it by board or council action if you can, and send it to your vendors. Sample language for your attorney to review:

"The [Agency] will not approve or process a vendor bank-account or remittance-information change based on an email, text message, or phone request alone. A vendor may initiate a request through these channels, but all changes require a signed change form, submission through [portal/mail], independent verbal verification by [Agency] staff using contact information already on file, and approval under the [Agency]'s documented vendor-change process. Requests that do not follow this procedure will be declined, regardless of urgency or the requester's claimed identity."

Two rules make it work:

- No exceptions for urgency or seniority. Fraudsters impersonate department heads and council members to create pressure. The policy protects staff who say no.
- Tell vendors in advance. Add a line to purchase orders and contracts, so honest vendors expect the call.

Control 3: Vendor master file change log

Every change to a vendor record should leave a trail someone else reviews. At a minimum capture these fields in your change log.

- **Vendor name and ID** - Ties change to the record
- **Date and time of request** -Spots after-hours or rushed requests
- **Who requested it, and how (email, phone, form) -** Shows whether policy was followed
- **Old and new bank info (last four digits only)** - Shows what changed
- **Call-back date, number called, person confirmed -** Proof of verification
- **Who made the change** - Accountability
- **Who reviewed it, and when** - Independent check

Three rules:

- The person who edits the vendor master file should not be the person who approves or releases payments.
- Someone independent runs a monthly change report and compares it to the log.
- Review any vendor whose bank account changed within 30 days of a payment.

Control 4: Treat a Familiar Voice as One More Thing to Verify

Call-back verification assumes the voice on the other end proves who they are. In 2026, that assumption is weaker than it used to be.

AI voice-cloning tools can recreate a real person's voice from a few seconds of audio pulled from a public meeting recording, a council video, or a voicemail. Video deep-fakes have been used to impersonate executives on live calls well enough to move tens of millions of dollars at a private company. A department head's voice, or even their face on a video call, is no longer proof by itself that a request is genuine.

The good news: the call-back method in Control 1 still works, for one specific reason. A cloned voice can sound like anyone, but it cannot make your outbound call ring on the fraudster's line. As long as you dial a number you already had on file, rather than answering an incoming call or dialing a number supplied in the request, you are reaching the real person or the real vendor, whoever answers.

- Never approve a bank change, wire, or urgent payment based on a phone or video call alone, however convincing the voice or face. The call confirms; it does not replace the change log and second-person review in Control 3.

- For your highest-value or most frequent payments, agree on a shared verification phrase with key vendors and department heads in advance, something never said over email or in a public meeting.

- Treat a request to skip the normal process because a caller is "too busy" for the change log as a red flag on its own, regardless of whose voice is asking.

- If something feels off during a call, hang up and call back on the number you already had, rather than continuing the conversation.

How to Recognize the Phishing Email

Every scheme in this guide starts the same way: a fraudulent email or text message built to look genuine. Phishing just means sending fake messages designed to trick the recipient into revealing information, clicking a malicious link, or acting on a fake instruction, and BEC is phishing aimed specifically at a payment.

Cybercriminals often build the message using information they found online: a vendor’s name from a public bid document, a department head’s title from your website, an employee’s name from a board packet or LinkedIn.

None of that requires hacking your systems, only reading what’s already public.

Train staff to look for the same handful of signs on every payment-related email, not just ones that look obviously suspicious:

- A sender address that is slightly off from the real one, or a free personal email account instead of a company domain

- Urgency, secrecy, or pressure to bypass normal approval steps

- A generic greeting instead of your name or your agency's name
- A request to click a link, open an attachment, or change payment or bank information
- Wording or formatting that is close to a real vendor's but not quite right

Red flags for finance staff

- A new "urgent" request from a vendor you haven't heard from in months
- A sender address that is a lookalike domain or a free email account
- A request to keep the change "confidential" or to skip normal approvals
- A new account at a different bank, in a different state, or in a different name
- Refusal to take a phone call

Secure the Devices Used for Payments

The email is the trick. The device is where it lands. A computer or phone that is out of date, unlocked, or used for both payments and everyday browsing gives a phishing attempt more room to succeed.

- Keep software current. Software updates patch real, documented weaknesses, including the ones phishing links are built to exploit. Turn on automatic updates for every computer and phone used to send or approve payments, and check the device's settings, usually under "System," for any update that was missed.
- Lock every device. Require a PIN, password or biometric lock on any phone, laptop or tablet used for finance work, never a default or shared code such as 1234. A lost or stolen device with no lock hands a stranger everything on it.
- Separate payment devices from everyday browsing where you can. A computer used to enter or approve vendor payments is a poor choice for checking personal email or browsing the web; that mix is exactly how a phishing link reaches a payment system.

These habits protect the device a phishing email is trying to reach. Part 5 covers the equivalent controls for payroll and HR portals specifically.

Check Fraud Hasn't Gone Away

Paper checks remain a frequent fraud target. In the Association for Financial Professionals' 2026 Payments Fraud and Control Survey, 58% of responding organizations reported attempted or actual fraud involving paper checks in 2025—the highest share among payment methods measured. This statistic reflects incidents reported by survey respondents; it does not measure nationwide dollar losses or mean every attempt succeeded.

Check fraud can involve check washing, counterfeiting, forgery, and unauthorized use of legitimate check information. Check washing occurs when criminals alter a genuine check's payee name, amount, or both—sometimes using chemicals or other methods to remove or cover the original information. Fraudsters may also use a stolen check as a template to produce counterfeit checks or fraudulently endorse and deposit the original.

Mail theft is a major driver of check fraud. From February through August 2023, FinCEN received 15,417 reports of mail-theft-related check fraud involving more than $688 million in suspicious activity. Criminals may alter stolen checks, create counterfeits, or fraudulently endorse and deposit them. These figures may include attempted as well as actual transactions.

What Your Insurance Will and Won't Cover

Even strong controls cannot eliminate payment-fraud risk. Recovery and insurance coverage may not fully reimburse a loss.

Business email compromise, vendor impersonation, and other social-engineering schemes can create significant exposure. Coverage may include a separate social-engineering or funds-transfer-fraud sublimit that is lower than the policy's overall limit.

Some policies require documented verification steps as a condition of coverage. Confirm requirements in writing with your broker or carrier. That is one reason to document and follow the controls in this guide.

- Ask your insurance agent or broker:
- Is a fraudulent vendor or payroll transfer covered under our crime policy, cyber policy, or neither?
- What is our specific social-engineering or funds-transfer-fraud sublimit?
- Does the policy require documented verification steps, and does our procedure meet that standard?

If a Payment Goes to the Wrong Account

Speed is critical. Your bank's available options and reporting deadlines depend on the payment type, timing, receiving institution, and whether funds remain in the recipient account. Do not delete, alter, or "clean up" any records before they are preserved. Do these in order:

- Call your bank immediately. Ask whether it can recall, reverse, hold, or freeze the payment. Get a case number and confirm in writing.
- File at IC3.gov and contact your local FBI field office.
- Notify your insurer. Policies may have notice deadlines.
- Preserve emails, headers, forms, bank records, and logs.
- Contact the real vendor using known contact information and check whether your systems were compromised.

Part 2: A Nacha Rule Your ACH Payments May Fall Under

What ACH and Nacha are.

ACH is the electronic network used for direct deposit and many vendor payments. If your agency sends ACH payments, Nacha considers it a non-consumer "Originator" subject to applicable ACH Rules.

What Changed

Nacha requires risk-based processes to identify ACH payments that may be unauthorized or induced by deception, including vendor, payroll, and business-email-compromise impersonation scams. Review your process with your bank or ACH provider to confirm how the rule applies.

What It Requires—and What It Does Not

- Maintain an ACH-fraud process suited to your risks and review it at least annually.
- Document who verifies high-risk payments, what triggers added review, and where records are kept.
- Identify high-risk activity, including bank-account changes, new payment destinations, urgent requests, unusual amounts, and out-of-pattern payments.
- The rule does not require checking every payment, reviewing every payment before release, or buying specific software.
- It does not automatically determine who bears a fraud loss; ACH Rules, contracts, applicable law, bank controls, timing, and transaction facts may affect responsibility.

Who Does What

Your bank: May offer fraud monitoring, ACH filters, blocks, callbacks, limits, alerts, or payment-review tools, depending on your agreement and services.

Your payment processor or ACH software vendor: May monitor payment volume, timing, dollar amounts, or other activity, depending on the services it provides.

Your agency: Must address the risks only you can evaluate: Is a vendor or employee bank-account change genuine? Does the payment match the invoice, contract, approval, and normal payment pattern?

Receiving banks also have ACH-fraud-monitoring responsibilities. That does not reduce your agency's duties as the sender.

What's Left for Your Agency

- Write a short procedure covering callback verification, change logs, and second-person review. Nacha does not require a specific written format, but documentation helps show that a process exists.
- Identify higher-risk payments. Vendor and payroll bank-account changes belong on that list.
- Put an annual review on the calendar.
- Ask your bank or processor in writing what it monitors, what tools it offers, and what it expects from your agency.
- Ask whether payroll files use the description "PAYROLL." Nacha has required that descriptor for PPD credits paying wages, salaries, and similar compensation since March 20, 2026.
- If your agency sends vendor ACH payments or direct-deposit payroll, this rule likely applies. Confirm how it applies with your bank or ACH provider.

If your agency sends vendor ACH payments or direct-deposit payroll, this likely includes you. Confirm with your bank or ACH provider.

Part 3: Segregation of Duties for One- and Two-Person Offices

The principle

In a well-staffed office, four jobs belong to different people**:**

1. **Authorizing** a transaction
2. **Having custody** of cash or payment tools
3. **Recording** it in the books
4. **Reconciling** the accounts

The Washington State Auditor says segregating duties isn't all or nothing. You separate as much as you can, then fill the gaps with oversight controls performed by a mayor, another qualified council member, or a paid third party.

Indiana's State Board of Accounts adds that where separation isn't feasible, you should document which areas lack it and which compensating controls you put in place.

If one person does this.. Add this compensating control

- **Receives cash and makes deposits** - A second person opens mail or reviews the daily receipt log; deposits are compared to receipts independently
- **Prepares and releases payments-** Online banking with dual approval; an elected official approves payment batches
- **Records transactions and reconciles the bank** - Bank statements go unopened to an elected official or contracted CPA who reviews them first
- **Sets up vendors and pays them -** Monthly vendor change report reviewed by someone else
- **Runs payroll and edits employee bank info -** Payroll change report reviewed before every payroll run

The New York State Comptroller suggests having a board member periodically review the treasurer's work, especially monthly bank reconciliations, when hiring another employee isn't cost-effective.

Tennessee's municipal advisory service describes the same idea for small cities: an elected official reviews daily and monthly reports, reviews reconciliations, and conducts unannounced spot-checks.

Two habits most small offices skip

Rotating duties. Swap tasks such as deposits and reconciliation between people at least quarterly, or have a second person cover the work when someone is out.

Mandatory vacation. Require at least five consecutive business days away from finance duties every year. Someone else runs the process during that time, without the regular employee's access. Many schemes depend on the perpetrator being there every day to keep them hidden.

Checklist for the elected official reviewer

- Receive the bank statement directly from the bank (or with a copy sent to you).
- Scan for unusual payees, round-dollar amounts, transfers between accounts, and payments outside normal patterns.
- Confirm the reconciliation ties to the statement and to the general ledger.
- Sign and date the review.
- Once a quarter, pick three to five random transactions and trace them to invoices and approvals.

Many schemes depend on the perpetrator being there every day to keep them hidden.

Part 4: Insider Fraud

Why Time Matters

The ACFE's 2026 study found that the average fraud scheme lasted 12 months before detection. Fraud caught within six months had a median loss of $40,000. The longer a scheme runs, the more it can cost. The goal is faster detection.

Warning Signs

The study found 84% of perpetrators showed behavioral red flags before detection. Watch for:

- Living beyond means or sudden financial stress
- Refusing vacation or refusing to share duties or passwords
- Being protective of records or resisting oversight
- Unexplained voids, refunds, write-offs, or adjustments
- Missing, altered, or late receipts and bank statements
- Vendors or payees with no clear agency relationship

Surprise Cash-Count Checklist

- Do it unannounced and vary the day and time.
- Use two people; neither is the cash handler.
- Count cash, checks, and change funds; compare with receipt logs, till tapes, and deposit slips.
- Have the cash handler sign the count sheet.
- Document attendees, date, results, and differences.
- Consider quarterly counts, or more often for high-volume counters.

Periodic Independent Reconciliation

Once a year, have someone outside the finance office—such as your outside CPA, another agency's finance staff, or an appointed board member—reconcile a sample month from scratch.

They should work from the original bank statement, not the reconciliation prepared by agency staff.

Give People a Safe Way to Report

In the ACFE's Occupational Fraud 2026: A Report to the Nations, organizations with a formal reporting mechanism had a median loss of $100,000, compared with $150,000 for those without one. Their frauds were also detected sooner: 11 months versus 17 months.

Consider a third-party hotline or another designated reporting channel that allows employees, vendors, and residents to report concerns. Explain how to report, who receives the report, how confidentiality is handled, and how the agency protects people from retaliation.

Allow anonymous reports when practical, prohibit retaliation, and make the reporting option visible on your website, vendor materials, and employee onboarding documents.

Part 5: Payroll Diversion

How It Works

A message that appears to be from an employee asks payroll to change direct-deposit information. The new account belongs to a criminal.

In another version, criminals steal an employee's credentials, access payroll or email, and create mailbox rules that hide change alerts. New Jersey's cybersecurity center described attackers who obtained a password and MFA reset through the help desk, then emailed payroll from the employee's real account. Payroll changed the account based only on the email; security monitoring later detected the inbox rule and locked the account.

Payroll Diversion Checklist

- Direct-deposit changes require in-person confirmation or a callback to a number on file. Never make a change based on an email, text, or phone request alone.
- Require MFA on payroll and HR self-service portals.
- Verify identity before password or MFA resets. Use manager or in-person confirmation for finance, HR, and payroll accounts.
- Send automatic notice of every bank change to the employee's existing contact information, not just the new one.
- Require a second person to review the direct-deposit change report before payroll is released.
- Review mailbox rules and unusual login times for payroll and HR staff.
- Confirm the first payment after a change reached the right person.
- Train staff to say: "We'll call you at the number on file."

Part 6: Reconciliation as a Detection Control

Reconciliation is a key fraud-detection control. A reconciliation completed late, prepared by the person handling the money, or never independently reviewed may fail to identify errors, missing deposits, or fraud promptly

The three-way match

1. Processor settlement reports show payment activity, fees, refunds, chargebacks, adjustments, and the net amount expected to be deposited.
2. Bank deposit shows what actually arrived.
3. General ledger shows what your books recorded.

The records should reconcile after accounting for documented timing differences, processing fees, refunds, chargebacks, and other valid adjustments. Investigate and document unexplained differences promptly.

Who and how often

Frequency	Task	Who
Daily or each business day	For higher-volume cash, card, utility, court, or online-payment activity: compare settlement reports with expected deposits; review refunds, voids, and unusual activity.	Someone other than the person handling cash
Weekly	“Review ACH returns, chargebacks, disputes, vendor-payment exceptions, and payroll bank-change reports	Finance staff, reviewed by a second person when staffing permits
Monthly	RReconcile bank statements to the general ledger. The preparer should not be the cash handler; arrange independent review when staffing permits	Preparer is not the cash handler; reviewer is an independent reviewer, such as a supervisor not involved in collection, an appointed official, another agency’s finance professional, or an outside CPA
Quarterly	Perform surprise cash counts and sample transactions back to source documents	Independent person
Annually	Arrange an outside review, audit, or targeted control review; update reconciliation and fraud-monitoring procedures	CPA and governing body

Illustrative example

- Your online settlement report shows $12,450.00 collected on Tuesday. The bank deposit posted Wednesday is $12,150.00. Trace the $300.00 difference the same day to a refund, fee adjustment, chargeback, or documented timing difference.
- If nobody compares the numbers until month-end, an unexplained $300.00 difference can go unnoticed for weeks. If the same person who processes refunds also reconciles, no independent person may detect it.

Your 30-Day Action Plan

Week 1
- Adopt the “no bank changes by email” policy and tell vendors.
- Start vendor-bank-change and payroll-direct-deposit change logs.

Week 2
- Ask your bank about dual approval for ACH and wire payments.
- Arrange for an independent reviewer—such as an elected official, supervisor, outside CPA, or another agency’s finance professional—to receive or review bank statements

Week 3
- Assign separate people to reconcile and review, or arrange an independent compensating review if staffing is limited.
- Write the one-page ACH-fraud monitoring procedure and schedule its annual review.

Week 4
- Set up and publicize a fraud-reporting channel.
- Put planned vacation, duty rotation, and independent review on the calendar.

Frequently Asked Questions

What is business email compromise (BEC)?
BEC is fraud where a criminal impersonates a vendor, executive or employee by email to redirect a payment. It often uses no malicious link or attachment, just a believable request.

Is voice-cloning (“deepfake”) fraud something a small agency needs to worry about?
A callback to a number already on file is a strong verification control, but not conclusive proof of identity. For high-risk changes, use additional verification and confirm the request against your vendor or employee record rather than relying on a voice alone.

What is the best control against vendor payment fraud?
Independent callback verification using contact information already on file, plus a second-person review before the bank change takes effect.

Does our vendor-verification policy apply to elected officials, or just staff?
It should apply to everyone who can request, approve, change, or release payment information, including elected officials. Consider adopting the policy through board or council action so it applies consistently to staff and elected officials.

A Legitimate Vendor Is Annoyed That Our Verification Process Is Delaying Payment. What Do We Say?
Tell the vendor the policy applies to every vendor without exception and protects their payments, too. It is the same process that would help catch someone trying to redirect money owed to them. Explain the policy in contract and purchase-order language upfront, so the callback is not a surprise. A brief verification delay is far less costly than attempting to recover a fraudulent payment.

We only have one finance employee. Can we still segregate duties?
Not fully. Separate what you can, then use compensating controls: an elected official's monthly bank review, rotation, mandatory vacation and surprise counts. Document the gaps and how you cover them.

Do the 2026 Nacha fraud monitoring rules apply to local governments?
They apply to non-consumer ACH originators, which generally includes agencies that send vendor payments or payroll by ACH. Confirm with your bank.

If we approve a fraudulent bank change, does our bank share any responsibility?
Sometimes, but don't count on it. Under the Uniform Commercial Code, liability for a fraudulent transaction can be split between your agency and your bank based on each party's own diligence, not automatically assigned to whichever one clicked “send.” GFOA notes that if your bank offers a fraud-prevention service, such as positive pay, and your agency chooses not to use it, your agency, not the bank, generally bears the loss. Ask your bank counsel which services you're declining and what that means for your liability.

We keep hearing BEC is the top fraud method. Isn't check fraud still a bigger risk for us?
Both matter. Business email compromise is consistently reported as the most common method used in attempted or actual payments fraud, but checks remain one of the most exploited payment types, since a check carries no built-in verification the way an electronic payment can. GFOA calls positive pay, a bank service that flags any check that doesn't match your issued list, the single best fraud-prevention tool available for check disbursements, and warns that a government that declines the service when its bank offers it typically bears the loss itself, not the bank. If your agency still writes checks, ask your bank whether positive pay, or payee positive pay, is available and enroll.

Should we carry cyber or crime insurance for a BEC loss, and what will it expect from us?
Most public entity crime and cyber policies do cover social-engineering losses, but read the fine print before an incident, not after. Insurers commonly require a call-back or independent verification step as a condition of coverage, and set a notice deadline measured in days. Confirm which of the controls in this guide your policy actually requires, and revisit the policy annually as your procedures change.

How often should we reconcile?
Match settlements to deposits daily or every business day, and reconcile bank statements to the ledger monthly, with an independent reviewer signing off.

What should we do first if we sent money to a fraudster?
Call your bank right away to request a recall or freeze, file a report at ic3.gov, notify your insurer, and preserve all records.

What is “friendly fraud,” and does it affect our agency?
Friendly fraud is a cardholder disputing a card payment they actually authorized, most often on an online utility, court or permit payment. It is a card-processing and chargeback issue for your payment processor to help manage, not the vendor and employee impersonation schemes this guide covers, and it calls for a different set of controls.

What If We Do Not Have Enough Staff to Separate Every Finance Duty?
Use compensating controls. Have an elected official, supervisor, outside CPA, contracted bookkeeper, or finance professional from another agency review bank statements, reconciliations, vendor-bank changes, refunds, and unusual payments. Document the review and any follow-up.

Where IntelliPay Fits

IntelliPay handles the payment side of your operation. Role-based permissions let you control who on your staff can issue refunds or change settings, and reporting helps you match settlements to your bank deposits. Its platform offers centralized dashboards with visibility across departments and hierarchical permissions that control access to specific functions.

IntelliPay can't stop a fraudulent vendor email or a payroll change request. Those controls are yours. Start with the five habits above, and ask your payment provider how its reporting supports your reconciliation.

Sources

FBI Internet Crime Complaint Center, 2025 Internet Crime Report (ic3.gov)
FBI Internet Crime Complaint Center, "Business Email Compromise: The $55 Billion Scam" (September 2024)
Association of Certified Fraud Examiners, Occupational Fraud 2026: A Report to the Nations
Nacha, "Risk Management Topics: Fraud Monitoring Phase 2," "Summary of Upcoming Rule Changes," and "Risk Management Topics: Company Entry Descriptions" (nacha.org)
Government Finance Officers Association, "Electronic Vendor Fraud" (gfoa.org)
Office of the Washington State Auditor, Segregation of Duties Guide
New York State Comptroller, Management's Responsibility for Internal Controls
Tennessee MTAS, "Common Audit Finding: Lack of Segregation of Duties"
Indiana State Board of Accounts, Uniform Internal Control Standards
National Institute of Standards and Technology, Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management
Financial Crimes Enforcement Network, Financial Trend Analysis: Mail Theft-Related Check Fraud (September 2024)
Federal Bureau of Investigation, "Mail Theft-Related Check Fraud Is on the Rise" (January 2025)
U.S. Postal Inspection Service, "Check Washing"
New Jersey Cybersecurity and Communications Integration Cell, "Direct Deposit Scams Continue" (April 2025)
Association for Financial Professionals, 2026 AFP Payments Fraud and Control Survey Report
Baltimore City Office of the Inspector General findings, as reported by CBS News Baltimore, "Baltimore lost $800,000 in vendor payment fraud scheme, inspector general finds" (August 2025)
Federal Reserve Financial Services, 2026 Risk Officer Report
Insurance Journal / Hunton Andrews Kurth, reporting on cyber-enabled fraud, social-engineering coverage, and funds-transfer-fraud sublimits (June 2026)
Citizen Portal, reporting on a Connecticut municipality's Positive Pay recovery of altered checks (August 2026)

Disclaimer: This article is for general educational purposes only and is not legal, accounting or compliance advice. Requirements vary by state and agency. Have your attorney, auditor or bank review your policies. Last reviewed: September 2026.