

THE TOP 10 LIST & FIXES FOR POST OFFICE FINANCIAL COMPLIANCE

Cash retained accountabilities examinations not timely.

FIX: Monthly spot check amount of cash retained by clerks overnight (F-1 532.51a and d). B-weekly: count clerks cash retained, PS 3294-C; PS3368-P; PS3369-P: all signed. A clerk's cash retained must not exceed ten per cent of the stamp credit or \$100, whichever is smaller.

Duplicate key envelopes not prepared or fully completed.

FIX: Semi-annually check inventory of PS 3977, verifying date, source and location. The Duplicate Key Inventory envelope is used to secure keys, passwords and combinations. (F-1, 372.1)

Credit examination results not documented on PS Form 3368, Stamp Credit Examination Record.

FIX: Each employee's fixed credit should be counted at least once every four months. Counts should be unannounced and completed before the clerk has completed any retail transactions. Document the counts on PS Form 3294 and PS Form 3368.

Credit examination results not documented on PS Form 3294, Cash and Stamp Stock Count and Summary, or retained.

FIX: PS Form 3294 should be signed by the two individuals who performed the counts. Independent counts should be performed by the stock custodian and one other employee. One employee must be non-bargaining. (F-1, 487.53)

Annual verifications that accountability keys did not open another accountability were not performed.

FIX: Physically perform this verification and document the action. (F-1, 377.6). Keys that can open multiple credit drawers jeopardize the security of those credits.

Retail floor stock exceeds the 2-week postage sales limit.

FIX: Retail floor stock is the sum of display stock plus loose stock. It must be limited to a 2-week level as determined by same period last year (SPLY) stamp sales. (Formula: $SPLY = \frac{\text{general ledger account (GLA)}}{\text{account identifier code (AIC) 852, Total Sales, minus GLA/AIC 096, Vending, plus GLA/AIC 094, Stamps by Mail.}$) The limitations must be enforced to minimize the risk of losses that might be associated with the concept of common accountabilities. (PO 209, 11-4.2)

Financial differences were not monitored or resolved.

FIX: Discrepancies of \$100 or more are to be reported to the Inspector General using PS Form 571. Overages and shortages exceeding established tolerance levels should be posted to either trust or suspense on PS Form 1412. (F-1, 429.16)

Unit cash reserve accountability examinations were not timely.

FIX: Postmasters should review PS Forms 17, Stamp Requisition/Stamp Return; and 3958, Main Stock (or Unit Reserve Stock) Transaction Record, each day there is activity in the main stock.

Advance deposit accounts were not monitored for inactivity.

FIX: Close inactive Business Mail, periodicals, and BRM/PD advance deposit accounts and/or refund balances. Have a process in place to ensure that inactive customer trust accounts are closed and that funds are refunded as required. (Field Accounting Procedures 1907)

The unit did not properly prepare bank deposits.

FIX: When submitting funds for deposit, the count should be inaccessible to the public and concealed from view. Close-out employee and retail associate should make separate and independent counts. Witness, close and seal the bank deposit envelope, with both signing the deposit slip and envelope seal. If no witness is available, endorse deposit slip receipt with NWA. (FAP 901)

When the OIG Auditor Rings ...

David C. Williams, Inspector General, USPS, talks with the LEAGUE

You've heard that quote, "Honesty is the best policy." It's just one of the many famous quotes uttered by Ben Franklin. Others you may not have heard are "Fish and visitors smell in three days," and "I'm here to help!" The first was a commentary on some house guests who just wouldn't go home. But the latter was the greeting Ben used when he appeared, unannounced, at the door of colonial Postmasters, fulfilling his additional duties as Postmaster of Philadelphia of "*regulating several offices, and bringing the officers into account.*"

Ben Franklin's additional duties in the fledgling colonial postal system were designed to ensure that the British Crown was accurately receiving the monies due for the carriage of mail and for postal services. In effect, he was performing the audit functions that are now done by the Field Financial Team auditors of the Office of Inspector General. The OIG auditors also follow that age-old tradition of greeting you with "We're here to help." Which, of course, you follow up with the second biggest lie—"I'm happy to see you!" But that old joke is just that. We in the OIG are approaching our role with the Postal Service and with you in a different way. We want to truly help you and help make a better Postal Service.

As Postmasters, you work hard and continue to be the backbone of the Postal Service. Thank you for that and your commitment to service to your community and the public we serve. In the face of all types of obstacles—shrinking budgets, fluctuating mail volume, not enough work hours—you continue to do a great job providing great service.

Field Financial Audits

The mere mention of auditing a post office often brings that queasy feeling to Postmasters. But it does not have to be that way. We are not playing the "gotcha game." Our audit process starts with a random selection of about 200 offices to be audited during the year. With over 37,000 offices, stations and branches, the chances that your office will be randomly selected are about 1 in 185. However, that's not to say you should kick back and not keep your office in compliance. Another interesting point is that in the vast majority of our financial audits, we find that the offices are being operated in compliance and there is little that needs corrected.

Many of the shortcomings are a result of a lack of training. Or as Ben Franklin so aptly put it, "I didn't fail the test. I just found 100 ways to do it wrong."

We want to help you do it right. In our Field Financial Audit Directorate, we cover three main areas—Post Offices, Business Mail Entry Units (BMEU) and Automated Postal Centers (APC). Because of increased attention on Postal Service credit card usage, we are also doing more audits of the SmartPay Purchase Cards (formerly called IMPAC cards). Overall, our audits show financial information related to field operations is accurately and fairly presented and internal controls are in place and effective. However, we have noted the prevalence of lax controls over two areas:



Most Common Postmaster “Mistakes”

Using position for personal benefit
Nepotism
Sexual Harassment
POS (1412) Manipulation
Untimely or falsified Till Count
Overages/Shortages
“Borrowing” postal funds
Samples/magazines taken from the mail
Discarding mail
Stamp destruction irregularities
Falsified volume recording
Incorrect postmarking
Personal use of Postal Service supplies
Timecard falsification
Alcohol and drug abuse

Do’s and Don’ts

- Do:** Sell stamps for face value only.
Don’t: Use stamps in payment for debts or purchases of merchandise.
- Do:** Provide the highest available security to cash and accountables.
Don’t: Permit access between accountabilities.
- Do:** Count all flexible credits at least once every four months.
Don’t: Fail to complete Form 571 for discrepancies over \$100.
- Do:** Collect and record all box rents.
Don’t: Use or permit others to use post office boxes without payment.
- Do:** Accurately report the condition of the office.
Don’t: Falsify reports or attempt to coverup unfavorable conditions.
- Do:** Promptly deliver all mail.
Don’t: Delay, obstruct, or remove any mail received for delivery.
- Do:** Properly account for and promptly deposit all postal funds.
Don’t: Convert postal funds to personal use; knowingly accept insufficient funds (IOU’s); or cash personal checks.
- Do:** Properly rate and account for postage-due mail.
Don’t: Use the “honor” system with employees or customers.
- Do:** Properly safeguard and account for all personal property.
Don’t: Convert postal supplies or property, or undeliverable samples, to personal use.
- Do:** Safeguard the sanctity of the mail.
Don’t: Permit the opening or reading of mail addressed to customers.
- Do:** Comply with the Fair Labor Standards Act.
Don’t: Violate the provisions by personally working, or permitting other employees to work “off-the-clock,” or by working over time without proper compensation.

- Stamp/cash accountability in post offices
- Mail verification procedures at BMEUs

We have a checklist of items we cover when we are doing a financial audit. If you’re performing all these things, you should be in good shape. In this article, we provide the top 10 findings we consistently encounter during our audits. If these things are not receiving attention in your office, start fixing them as soon as you finish reading this article, because just like Ben Franklin, there is no advance warning that we are coming.

Post Offices

First and foremost, we look at whether financial transactions are reasonably and fairly represented in your accounting records and whether the internal controls are in place and effective. We test transactions and controls related to stamp, cash and money order accountability; post office boxes; payroll and disbursements.

Let me tell you about a recent audit we conducted in a District. We found significant weaknesses in the internal controls over financial operations at 14 units related to stamps, cash, money orders, post office boxes, and disbursements. Specifically, we noted issues regarding safeguarding of and accountability for stamp stock, money orders, and cash; accurate and timely collection and recording of post office box and caller service fees; and adequate tracking and support of disbursements. Because of the lack of internal controls and insufficient oversight of unit financial operations, just in this District alone, there is significant increased risk for loss of stamps, cash, and other assets, and an increased risk of unrecorded revenue. The monetary impact totaled over \$120,000. Further, the internal control weaknesses placed \$11.1 million of assets and accountable items at risk. That’s just one District.

A good way to keep current on the activity in your office is to monitor unit performance using the Enterprise Data Warehouse. It provides data for managing your unit such as master trust balances, expense reports, fee payment reports, and an excess stock report.

Here are some other tips:

- Perform timely credit examinations and document the results.
- Monitor financial differences transmitted to your unit from the Accounting Service Center. Research discrepancies thoroughly and ensure the adjusting entries are performed.
- Safeguard your unit’s assets by ensuring duplicate keys are secured in properly completed duplicate key envelopes.
- Participate in the closeout of the retail window whenever possible to ensure bank deposits are properly prepared and disbursement transactions are supported. This is an

When the OIG Auditor Rings ...

Postmasters have a difficult job. You have to balance mail volumes with tight workhour budgets; you have to get the mail out on time, yet keep up with all the paperwork and documentation required with the job. And then we come in and do a financial audit. The good news is that in the overwhelming majority of the audits we conduct, we find that your offices are in compliance and little needs to be corrected. You are to be commended for this type of effort and performance. —David C. Williams, Inspector General, USPS

easy one for many of you since you not only participate; you actually take care of this process by yourself, since there are no other employees to witness the closeout.

Business Mail Entry Units

Not all of you have Business Mail Entry Units, but quite a few of you have business mailers. The following tips are useful in both cases. Revenue seepage at mail entry points remains a challenge for the Postal Service. BMEUs are right at the top of this challenge. Unless business mailings are properly prepared to qualify for the discounts claimed, the Postal Service incurs increased processing costs. There are over 2,400 BMEUs that generate over \$20 billion in revenue annually, so you can see how lax verification, acceptance and clearance procedures can really hurt the Postal Service financially.

Our BMEU audits have consistently turned up the same shortcomings. If you have a BMEU, make sure they don't happen to you by doing these functions:

- Perform accurate mail verifications. Review and complete all postage statements and timely collect postage due.
- Review inactive accounts and close, as appropriate.
- Ensure non-profit and periodicals mailers have received and maintained their authorization from the Pricing and Classification Service Center to mail at the reduced rates.
- Monitor periodicals mailers' compliance with the terms of their authorization. Review items such as frequency requirements, advertising percentages, and statements of ownership.
- Monitor and reconcile Master Trust balances.

• Verify all customers have paid their yearly fees.

• Review and update all Special Postage Payment System agreements and verify mailers are complying with the terms of the agreement.

The BMEU environment is one of the most rapidly evolving areas in the Postal Service. As the Postal Service moves towards electronic postage statements and customer advance deposit accounts that customers manage online, the revenue seepage issue becomes even more crucial.

Automated Postal Centers

In 2004, the Postal Service started deploying Automated Postal Centers (APCs), the friendly kiosks where customers can ship packages, buy stamps and verify ZIP Codes. The plan was to generate more revenue for the USPS.

The APCs have not resulted in wheelbarrows full of money for the Postal Service coffers, so APCs are going to be redistributed. You may be getting one.

Here are a couple things to watch out for:

- Conduct timely credit examinations and properly document them.
- Conduct credit examinations in a secure location, not in the post office lobby.
- Keep control of the keys. Use duplicate key envelopes, use a key control log, and ensure APC keys are checked-out and returned daily.

Contracts

The Postal Service manages more than \$42 billion in postal contracts. More than likely, you don't have a multi-million dollar contract that you oversee. But there's a good chance you have one of the other 48,000 smaller ones. Contract

fraud that we've uncovered comes in several forms:

- Overbilling or false claims
- Making false statements/falsifying records
- Bribes/gratuities
- Arranging for secret profits, kickbacks or commissions
- Conflict of interest
- Theft

You could be a victim of contract fraud if your office has a contract and you are paying for:

- Lawn service...and you cut the grass.
- Roof repairs...and your workroom floor still has buckets to catch the drips.
- Cleaning...and no cleaners have shown up for weeks.
- Snow removal... and you're relying on the sun to come out!

Unfortunately, we have also uncovered instances where the Postmaster is the violator, rather than the victim.

Recently a Postmaster in Colorado lost his job by providing a landscaping and snow removal sole source contract to a company. However, he was doing all the landscaping and snow removal, because the company awarded the contract was a shell company owned by his wife. It cost the Postal Service \$36,000 and the Postmaster his job. He and his wife were arrested and are awaiting trial. In addition, he has to pay back all the money!

Crimes by Postmasters

Unfortunately, despite all warnings, postal crimes are still committed by Postmasters. Last fiscal year, 120 investigations on Postmasters were opened by OIG Special Agents, resulting in 26 arrests and 89 administrative actions. *That's over two cases per week.*

Despite prevention and awareness

In our talks with management organizations, the issue of training has sometimes been raised. It is important that newly promoted Postmasters be given proper training to become proficient in their jobs. Along with the Postal Service, I know the LEAGUE is a good source of training, providing useful articles in the *Postmasters Advocate* and with workshops and speakers at state and national conventions. We, at the OIG, are participating with you by taking a proactive approach, sharing tips, findings and suggestions with you. —David C. Williams, Inspector General, USPS

messages, that figure has gone up this year. In just the first nine months of FY 2007, Special Agents opened 163 Postmaster cases, made 56 arrests and had 107 administrative actions taken. *That's a pace of over four cases per week—double activity from last year.*

Where are the problems? The biggest area is financial fraud—embezzlements—with 114 cases.

Embezzling: How does it happen?

OIG investigators employ various techniques to uncover embezzlements. Here are some common violations:

- “Borrowing” postal funds. Your credit belongs to the Postal Service. To borrow money, go to the credit union!
- Kiting money order funds

In July, a NC Postmaster was sentenced to 90 days of house arrest, 36 months of probation and ordered to pay back the \$40,000 she embezzled over six years. She kited money orders, stole box rents, stole from stamp accountability and stole vending machine funds. And do you know what she did with the money? She took her kids to amusement parks, ate dinner out and—this one makes no sense—took her family to Washington Redskins games!

In another case, a Kentucky Postmaster kited \$317,000 worth of money orders in one year and stole \$71,000 in postal funds. She cited two

recent divorces, the loss of her house and other financial problems as putting her in a position where “there was no way out.” She was indicted in federal court, pled guilty and is awaiting sentencing.

- Failure to post and deposit standard mail payments
- Fictitious invoices

A PM in Puerto Rico created an account called “Custodian Building Supplies” and proceeded to generate false invoices and payments of over \$42,000—to himself. Federal prosecution is pending.

Tampering with postal data ... COD funds ... Why does it happen? Why would a Postmaster or any postal employee risk his or her career by stealing from the Postal Service?

Integrity and Accountability

If you go to the USPS website, to get to the OIG site, you click on our seal that says, “Promoting Integrity.” That’s what we do. But the integrity starts with you. You’ve spent your career building up that trust and integrity. Don’t ever do anything to have your customers or your employees lose faith in that trust and integrity. As Ben Franklin so aptly stated, “It takes many good deeds to build a good reputation, and only one bad one to lose it.” Don’t be one of those “four Postmasters per week.” How can

The Three “C’s”

Credit

- Financial difficulty, bankruptcy
- Overwhelming medical bills
- Irresponsible spending habits
- College expenses
- Marital difficulty

Chemicals

• Drug or alcohol addiction ... Although the Postal Service is always looking for new ways to generate revenue, selling drugs over the counter at your office is not exactly what they have in mind. A Missouri Postmaster and her PM Relief were arrested and prosecuted for selling methamphetamine and prescription drugs at their Post Office during business hours! Both resigned and are awaiting prosecution.

Chance

• Gambling addiction ... Here’s how gambling can get out of hand. An Alaska Postmaster manipulated postal deposits for 10 months. The discrepancies came to the attention of the OIG because the daily remittances were being submitted up to a month late. A net shortage of \$129,000 was uncovered. The Postmaster resigned and paid restitution out of her terminal leave and a withdrawal of her FERS funds. All of the embezzled funds were gambled away.

Postmasters stay out of trouble?”

- Keep personal matters and problems, that everyone has, separate from your job.
- Trust your judgment and conscience.

If you have a concern about whether something is right or wrong, don’t do it. If you have a problem, call us. We’re not looking to arrest Postmasters who make honest mistakes. But if you don’t want to call us, call one of your fellow Postmasters. Don’t let it get out of hand. Let’s work together to make sure a mistake does not turn into a crime!

Focus on doing things right—not avoiding detection. Remember, it takes years to build up a “good name,” but only seconds to destroy it. You are responsible for what you do—unless, of course, you are a politician or a celebrity! And remember—“We’re here to help!” •



1. Inactive business mail or Periodicals advance deposit accounts and/or refund balances not closed.
2. Mail not accepted according to PS instructions.
3. Periodicals advertising percentages or publishing frequencies not verified.
4. Postage payment/zone accuracy reviews not conducted or properly documented.
5. Mailer’s sections of the per-

BMEUs

- mit/business mail postage statement were not reviewed for completeness.
6. U.S. Postal Service sections of the permit/business mail postage statement not complete.
 7. Bypass Mail Log not used or maintained or no process in place to identify bypassed mail.
 8. Data from Permit/business mail postage statement not

posted to the mailer’s account within a reasonable amount of time.

9. The unit did not have or provide a scale for weight verification, properly test the scale, or calibrate the scale on an annual basis at the BMEU and/or DMU.

10. Data from the Periodicals postage statement not posted to the mailer’s account within a reasonable amount of time.

When the OIG Auditor Rings

Cracking Computer Crime Cases the CCU Way

Attacks on the Postal Service are as old as the Postal Service itself. From mail thieves to post office robbers, fraudsters to bombers, attacks on the Postal Service, its facilities, equipment and employees are nothing new. Today a new breed of attackers and techniques face the Postal Service. As the Postal Service information infrastructure expands and the number of products and services available over the Internet increases, the USPS faces increased exposure to online attacks. Unauthorized access to Postal Service networks and improper usage of computers by employees are just two types of computer crimes that now threaten to victimize the Postal Service.

The popular television show, *24*, has its CTU. The Postal Service OIG has its CCU. The OIG has created a specialized, highly-skilled unit to combat these intrusions and crimes to ensure the Postal Service's networks and databases remain secure. The OIG's Computer Crimes Unit (CCU) provides a wide variety of computer-based support to OIG investigations into crimes targeting the Postal Service computer infrastructure.

There's no hiding from these high tech sleuths who can forensically image a postal computer without ever entering the postal facility. These digital forensic examiners, some Special Agents and some non-agents with very specialized IT training, could be compared to smoke jumpers—with forensic tool bags in hand ready to go into facilities covertly or overtly to gather digital data to support investigations in the Postal Service. CCU specialists have years of investigative and forensics training. They often have such specialized knowledge of crimes they are called into interrogations to discuss and explain the digital trail that a suspect has left on a postal computer. And, of course, are called to testify as an expert witness pertaining to forensic findings in a federal court of law or in a Postal Service administrative hearing.

The forensic examiners, 13 in all, work in forensic labs located in Arlington, Virginia; Los Angeles; Dallas; Miami; and at the USPS Computer Incident Response Team in Raleigh. CCU specialists also conduct data seizures during the execution of search warrants at homes or businesses where officials are suspected of conducting frauds against the Postal Service.

In an OIG investigation in Alaska, a CCU Special Agent analyzed data seized from an employee's personal computer that revealed the employee failed to collect \$450,000 worth of postage for business mailings. That employee was sentenced to 30 months in jail. In Kentucky, the web-log review and hard drive imaging of a postal computer by the CCU revealed child pornography surfing activity by a postal employee. As a result of this investigation, the employee was sen-



tenced to 78 months in federal prison.

One component that sets CCU apart from other forensic is its integration with the customer—Postal Service. This relationship particularly pays off when reacting to electronic assaults against postal computer resources. This could mean there is an insider causing or attempting to cause damage to postal systems or it may mean someone external to the Postal Service is causing damage or attempting to cause damage to postal systems. Either way, the Postal Service officials who are responsible for triaging computer incidents readily know how to operate directly with CCU via its embedded Special Agent Examiner. The trust, data sharing policies, and mechanisms have been successfully practiced for more than six years.

One example of this successful investigative partnership was demonstrated during a recent investigation into a critical computer incident that resulted in damage to thousands of postal computers and hundreds of thousands of dollars in losses to the Postal Service. During this investigation, CCU members worked with Postal Information Technology officials sifting through and analyzing terabytes of data before identifying the culprit—a postal contractor who had made unauthorized changes to critical postal servers.

These changes were immediately replicated across the postal infrastructure making thousands of computers unusable. This person was identified and fired following a grueling technical investigation, but more importantly, CCU members teamed with the Postal Service to develop methods and procedures to prevent such unauthorized changes in the future. The CCU provides a service for the Postal Service to be relied upon to both aggressively investigate and help prevent computer crime within the Postal Service.



Field Office Area Special Agents-in-Charge

Atlanta, GA	Yeudele Allen	(404) 507-8301
Boston, MA	Joe Finn	(617) 603-6100
Chicago, IL	Scott Caspall	(312) 601-3900
Dallas, TX	Maximo Eamiguel	(214) 775-9100
Denver, CO	Dave Montoya	(303) 925-7400
Hoboken, NJ	Jane Hughes	(201) 499-5100
Los Angeles, CA	Torri Piper	(949) 296-8100
Philadelphia, PA	Beth Farcht	(866) 644-6546
Washington, DC	William Siemer	(703) 248-2100