The Gehman COMPASS

Volume 7 Issue 1 Summer **Newsletter**

Fraud Prevention Is Critical

Fraud is no longer a distant or unlikely threat for those of us living in the modern world. It touches our everyday lives—through phone calls, emails, text messages, and even the roadside mailbox—increasing our risk of identity theft and financial loss.

So how can we protect ourselves? In the following sections, we'll examine key areas that fraudsters target and list some practical tips to help us safeguard our information.

Rising Mail & Check Fraud

Mail theft, and especially check fraud, is surging in the US. In 2023, check fraud cost an estimated $21 billion, according to FINCEN.

Washing & Cooking—Check Fraud Explained

Wendy Smith spotted something suspicious while doing routine bookkeeping for a client of Gehman Accounting: A check had cleared the bank for a different amount than was recorded. After some brief investigating, she uncovered a scam in progress.

The fraudsters had stolen the check somewhere in transit, then washed and cooked it. To "wash" the check, they apply chemicals like bleach or alcohol to remove the ink used for the payee and dollar amount, leaving the signature intact. The check is then "clean" and ready for a new payee and/or amount. After the washing, scammers often "cook" the altered check by photographing it and using software to create multiple counterfeits.

After washing and cooking, the fraudsters in our story began phase two of their scheme. They entered a new payee on the check and cashed it for the original amount. When that worked flawlessly, they cashed a second copy using the next consecutive check number and a larger amount. This is where Wendy's sharp eye spotted an inconsistency. She reviewed the check image online and saw that not only was the amount incorrect, but also the payee. This led her to discover the first fraudulent check. As she worked with the bank, they found yet another counterfeit check still working its way through the system.

In this case, the story has a happy ending. The bank reimbursed the client for thousands of dollars since the fraud was intercepted quickly. After this alarming incident, the client began using Positive Pay.

continued on page 2

Stopping Check Fraud

Tackling the problem of check fraud requires two things: prevention and vigilance.

Proactive Prevention. As the wise Benjamin Franklin once stated, "An ounce of prevention is worth a pound of cure." Here are some ways to stop check fraud before it begins:

- **Avoid mailing checks.** This is the easiest way to prevent fraud. There are several alternative options to consider:
  - ✔ **Use ACH automatic payments** or other electronic payments.
  - ✔ **Use Positive Pay,** a service offered by many banks. The account holder submits check numbers, amounts, and payee names to the bank. The bank then matches this information against any incoming checks and rejects any check not on the list.
- Use checks with security features like watermarks, heat-sensitive ink, and chemically reactive paper.
- Use pens with black gel ink so it is more difficult to "wash" the check.
- Don't leave blank spaces in the payee or amount lines.
- Don't leave mail in your mailbox for long periods of time.
- Use the letter slots at your local Post Office to send mail.

Routine Vigilance. Keeping your eyes open is critical for detecting any check fraud.

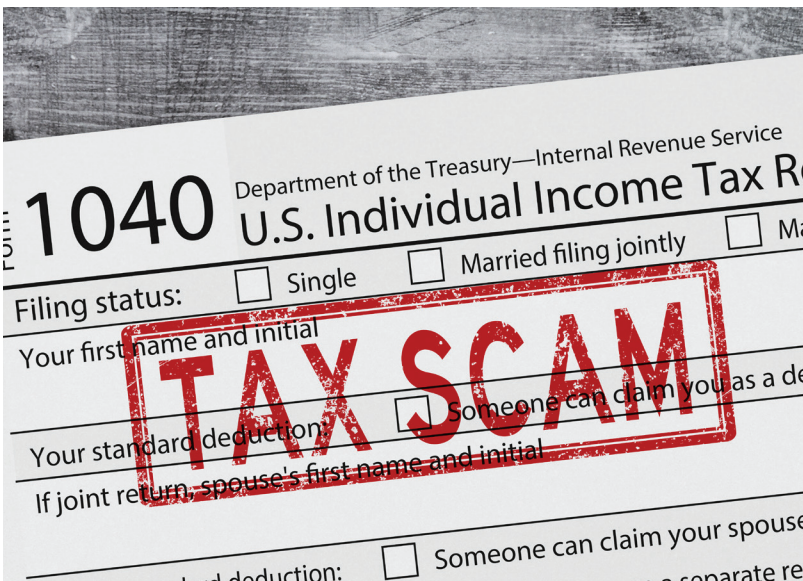
- The Best Advice: Review and reconcile your monthly bank statements promptly. Banks will often reimburse you if fraud is caught within 30 to 60 days.
- Notice duplicate payments, changed amounts, and unexpected checks.
- Look for payee names you don't recognize (if check images are available).
- Investigate, if you get a statement showing an invoice you remember paying. Don't assume it was your mistake.

Is It the IRS?

Many people feel nervous the moment the IRS is mentioned, and scammers use this natural fear against you. Here's how you can know if it's truly the IRS or a malicious imposter.

- **The IRS will generally contact you by a letter in the mail.** If you get an email, phone call, or text message claiming to be from the IRS, it is probably a scam.
- **Unannounced visits are rare.** The IRS will often send a letter before they visit.
- **The IRS will never:**
  - ✔ Ask for payment by cash, gift cards, a social media link, or prepaid debit cards.
  - ✔ Threaten to call law enforcement or immigration officials.
  - ✔ Ask for your driver's license or citizenship status.

If you're not sure if something's legitimate, you can always check with your tax preparer.



Tactics for Spotting a Scam

Scams of all kinds have become more sophisticated, making them more difficult to identify. But you can spot and prevent many types of scams using some basic tactics.

Pause, don't panic. Scammers try to hit your panic button, claiming that your account will be locked, you will be arrested, or the IRS will be at your door in 10 minutes. If you are pressured to act immediately, pause and investigate. Almost nothing is truly that urgent.

Return the call by a verifiable number. Always tell the caller you will return the call; then contact the company directly using official channels such as the phone number on a statement. If you use the internet for contact information, go to the company's official website and don't rely on Google or AI listings.

Check the details closely. If you get a suspicious email or text, examine the details for any abnormalities. For example, an email might be from micro**sft**.com instead of micro**soft**.com. You might notice odd language or a lack of identifying details, such as your unique account number.

Email Cautions

Email is a fast and cost-effective communication tool, but we need to be aware of the risks. Before sending an email, take a moment to evaluate the sensitivity of your information and/or the legitimacy of a request.

Seven Things to Never Send by Email

- Social Security numbers
- Passwords or account credentials
- Credit or debit card numbers
- Financial account numbers, such as bank accounts
- Driver's license and passport numbers
- Federal or state account numbers, such as EINs

Team Member Spotlight

Kevin Hibberd

Career. I have a dual role at Gehman Accounting, including IT Administration and Tax Support. Four years ago, I was about to finish up with college and was looking for a job. Steve Lapp recommended Gehman Accounting, so I applied. It was one of the first firms I applied to and was a top pick for me.

Reading. My favorite book genre is philosophy. I enjoy exploring the wide range of topics like values, wisdom, and personal growth.

Learning Goals. If I had time, I would learn to play a musical instrument. I've always thought it's a unique and impressive talent. I tried once when I was younger, but it never really stuck.

Places Lived. I've lived in several places throughout Pennsylvania, including Philadelphia, Bucks County, Lake Ariel, Mohnton, and Bowmansville. I currently live in Ephrata.

How to Be a Savvy Email User

- Check the sender's email address, not just the display name—look closely at what follows the "@".
- Hover over a link before clicking. If the web address is strange or doesn't match the sender, don't click it.
- Be wary of unexpected attachments, especially invoices, PDFs, ZIP files, or "secure documents."
- Remember that legitimate companies don't ask for a username, PIN, or password to be entered in an email link.

Table of Contents

Bulletin Board

New Faces at Gehman

Annetta Hoover – Bookkeeping Team
Bradley Weaver – Tax Team
Dixi Weaver – Secretarial Team
Fred Weaver – Tax Team

Come and See Us

Shed Builder Expo
Sept. 23 & 24, Knoxville, TN
Knoxville Convention Center (Booth #1624)

Eastool Auction & Expo
Sept. 25 & 26, Quarryville, PA
Solanco Fairgrounds (Booth #807-810)

Inspiring Confidence™

Gehman Accounting™
180 Diller Avenue • New Holland, PA 17557
12485 Old Turnpike Road • Mifflinburg, PA 17844

Update on IRS Requirements for Refunds and Payments

The IRS is making a swift transition away from sending or receiving paper checks based on a 2025 executive order. They are requesting that taxpayers provide their bank account information for any refunds and pay any tax due by electronic methods.

Are electronic payments mandatory? For now, the IRS is accepting mailed check payments. However, taxpayers should begin transitioning to making electronic payments.

You can pay the IRS in these ways: 1) On your tax return with bank account information 2) Online via IRS Direct Pay 3) Through an individual or business IRS account.

What happens if you did not provide bank account information for a 2025 refund? You will receive a series of IRS notices requesting additional information. If you do not respond, your refund will be delayed. For this year, the IRS will eventually issue a paper check, but that could change soon.