The BSA Examiner©

A Quarterly Publication from Wayne Barnett Software
Volume 101, 3rd Quarter 2026

The BSA Examiner is a quarterly newsletter published by Wayne Barnett Software. If you have a question to ask or a story to tell (we promise anonymity), please call us at 469-464-1902.

Case #1—Message from an Old Friend

Tom, a 52-year-old farmer and longtime customer of Mainstreet bank, visits a branch office requesting a $15,000 wire transfer. When questioned about the purpose of the wire, Tom states that he is going to invest in cryptocurrency. He explains that his old friend, Bill, had contacted him through Facebook and told him about a cryptocurrency investment opportunity that had "doubled his money in three months." Tom says he has already invested $5,000 and has been shown screenshots indicating his account is now worth over $18,000.

To withdraw his profits, the investment company says he must first pay a "release fee" of $15,000. Rather than simply processing the transaction, the banker asked: "Have you ever actually received money back from this investment?" Tom paused. He admitted he had only seen screenshots and online account balances. The banker asked Tom if he would come into his office to discuss the matter. After they reviewed the situation, they discovered:

- The investment website had only existed for a few months.
- The company's address was fake.
- The listed phone number was disconnected.
- Online reviews described nearly identical experiences.

The "profits" were completely fabricated. A fraudster had hacked Bill's Facebook and was operating a cryptocurrency investment scam designed to convince victims to send increasingly larger amounts of money. Had Tom sent the $15,000, the funds likely would have been converted into cryptocurrency and transferred to wallets controlled by criminals overseas—making recovery extremely difficult.

By taking the time to ask additional questions and discuss the situation privately with Tom, the banker helped prevent what appears to be a cryptocurrency investment scam. Financial institutions play a critical role in protecting customers from fraud by recognizing warning signs, educating customers about common scam tactics, and encouraging them to verify investment opportunities before sending money. In this case, the banker's diligence may have saved Tom from losing an additional $15,000 and highlighted the importance of proactive fraud prevention.

The Question

How do banks differentiate legitimate crypto investing from scam-related activity?

Many community bank customers are not actively seeking cryptocurrency. Instead, they encounter crypto through:

- Social media
- Dating sites
- Text messages
- Facebook groups
- Online investment advertisements

The cryptocurrency itself is not the problem. The real risk is that criminals use digital assets because:

- Transactions can move quickly
- Transfers are often irreversible
- Funds can cross borders easily
- Victims believe they are making legitimate investments

Red flags to watch out for are:

- First-time cryptocurrency activity
- Large wires to crypto exchanges
- Sudden liquidation of savings
- Guaranteed investment returns
- Pressure to act quickly
- Requests to pay fees to access funds
- Communication through WhatsApp, Telegram, or social media

Case #2— Where's My Money?

Magnolia Construction, a local construction company and long-time community bank customer, mailed a $12,500 check to one of its regular suppliers for building materials. The company had worked with the supplier for years, and the payment seemed routine.

About three weeks later, the supplier called: "We're showing your invoice as unpaid. Did you send the check?" The owner immediately responded: "Yes, we mailed it almost a month ago." The supplier insisted they never received it.

Concerned, the company's controller logged into online banking to investigate. To her surprise, the check had already cleared. But something wasn't right. The check had not cleared for $12,500, with the supplier's name. Instead, the image showed that the check cleared for $18,900 with the payee being an unfamiliar individual. The original check had been altered.

Following an investigation, it was determined that the check had been stolen from the mail, washed, and deposited into an account opened at another institution. Funds were withdrawn before the fraud was detected.

This scheme is commonly referred to as check washing. Fraudsters use chemicals to remove the original payee and dollar amount while preserving the legitimate signature. Once altered, the check is redeposited with a new payee and a higher dollar amount.

In this case, what began as a routine supplier payment evolved into mail theft, check fraud, and potential money mule activity. The incident highlights the growing threat of mail theft-related check fraud and demonstrates why financial institutions continue to focus on monitoring unusual deposit activity, newly opened accounts, and rapid withdrawals following large check deposits.

Barnett Software Corner

Barnett Software recently updated the Account Trends Report. This report is designed to help institutions look beyond a single transaction and identify changes in customer activity over time. A transaction may not look unusual until you compare it with everything that came before it. That's where trend monitoring becomes valuable. Because sometimes the suspicious activity isn't one giant transaction. It's the change in the customer's story.

Instead of asking only: “Did the customer exceed a threshold?”

You can also ask: “Is this normal for THIS customer?”

Transaction trends can help highlight:

- Significant increases or decreases in activity
- Changes in cash behavior
- ACH activity changes
- Wire activity changes
- Unusual transaction spikes
- Activity inconsistent with established customer patterns
- Potential indicators of elder financial exploitation

BSA Officer's Fall Checkup

Take a few minutes this quarter to review your program:

☐ Have we updated our ACH fraud-monitoring procedures for the 2026 requirements?

☐ Do frontline employees recognize cryptocurrency investment scams?

☐ Do Fraud, Operations and BSA communicate when unusual activity is identified?

☐ Are we monitoring changes in customer activity—not just dollar thresholds?

☐ Does our staff understand the difference between SAR confidentiality and communicating with a customer about fraud?

☐ Are we monitoring significant changes in elderly customers' activity?

☐ Can we demonstrate that monitoring thresholds and parameters are tied to your institution's actual risk?

☐ When activity doesn't make sense, do we keep digging?

☐ Have beneficial-ownership procedures been reviewed following FinCEN's 2026 relief?

Awareness is the first line of defense—but recognizing the activity is only the beginning. Connecting the dots is where an effective BSA/AML program makes the difference.

If you like the stories and helpful guidance that we tell in our newsletters, you’ll love our easy-to-use software. We are Wayne Barnett Software, and our fraud reports highlight both unusual crypto and unusual check activity such as the examples above.

We’re not a big company, but our products compare nicely with Verafin, Abrigo and the others. You can contact us at rrigdon@barnettsoftware.com or 469-464-1902. Thanks for reading our newsletter.