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 — What Jason Bateman Taught Me About Money Laundering

If you've ever watched *Ozark*, you already know: Jason Bateman's character, Marty Byrde, is one of the most prolific money launderers ever written for TV. Over five seasons, he cleaned millions for a drug cartel using cash-intensive small businesses and shell companies—all while dodging law enforcement and pretending it was just another day at the office.

Whether they meant to or not, the showrunners built a masterclass in what happens when BSA/AML controls fail. Here's what stood out:

Structuring: The Basics Still Matter
Early on, Marty breaks up large cash deposits to avoid triggering reporting thresholds. Classic structuring. And it still works when institutions rely only on raw thresholds instead of looking at both amount and behavior. If your system is only watching for single transactions over $10,000, Marty's deposits would've flown under the radar. Barnett's approach monitors for both—because patterns tell the real story.

No KYC = No Chance
Marty uses shell companies, fake owners, and implausible revenue streams. It's fiction, but not far off from real-world laundering. Without beneficial ownership data and a solid Know Your Customer process, you're flying blind. Compliance isn't about checking a box—it's about knowing who you're doing business with. When KYC and CDD factors are used to drive risk ratings, your analysis gets sharper—and your institution gets safer.

Transaction Monitoring: It's Not Just for the Big Guys
The Blue Cat Lodge. A funeral home. A casino. All cash-heavy businesses. All used to launder money. Each should have triggered alerts for volume, velocity, and source of funds. But they didn't—because no one was watching the full picture. When data stays siloed, red flags get missed.

SARs as Shield
In the real world, a bank dealing with someone like Marty should've been filing SARs from the jump. What *Ozark* shows well is how SARs protect more than just the public—they protect you. Good documentation is your legal defense. That's why our DCK (Digital Customer Knowledge) module retains customer documents and internal notes alongside transaction activity. When regulators ask questions, you'll have answers ready.

Ozark might be fiction, but the risks are real. Illicit funds move fast when the systems watching them move slowly. Strong policy, smart people, and the right software make all the difference. We help you spot the Martys before they make you a headline.

Glenda was 81 years old when she met someone online who claimed to be a U.S. citizen working overseas. He said he needed money for his business and to return to the United States. Over time, he convinced her to send him funds, then began directing others to send her electronics—items she was told to pawn and forward the proceeds to him.

When that no longer worked, he asked her to open multiple bank accounts, both personal and business. He began depositing funds into the accounts and instructing her on how to move the money.
Despite warnings from bank staff, local law enforcement, and federal agents, Glenda continued to follow the scammer's instructions. She never met him in person or spoke to him by phone. Her loyalty to a man she had only known online led to serious consequences—she ultimately pled guilty to two federal felonies.

Anatomy of an online dating scam:

These scams usually have a long timeframe, lasting 6–8 months on average.

   Initial Contact: The scammer starts by reaching out to the victim on a dating site or social media, crafting a fake identity. They often use attractive photos of someone they've found online and present themselves as kind, caring, and interested in a relationship.

   Building Trust: The scammer spends weeks or even months developing a relationship with the victim. They will frequently communicate through messages, phone calls, or video chats (though the scammer may never meet the victim in person). They often share emotional stories, such as being a soldier overseas or facing a personal crisis, to increase the victim's sympathy and trust.

   The Ask for Money: Once a strong emotional bond is formed, the scammer begins asking for money. This could be framed as a "sudden" emergency—needing money for a medical situation, a business opportunity, or travel expenses. Sometimes they send gifts or try to create a false sense of intimacy to make the request seem more legitimate.

   Manipulation: If the victim doesn't immediately comply, the scammer might use guilt, threats, or emotional manipulation to pressure them. They may say things like "I love you, but I need this help to get back to you" or "If you really cared about me, you'd help."

   Escalation: As the victim continues to send money or goods, the scammer may escalate the situation by inventing even more urgent or complicated reasons for needing more money. They might also create elaborate schemes to hide the scam, such as having fake business deals or promising to meet in person soon, only to come up with more reasons why it's not possible.

So, how do we, as the financial industry combat romance scams? Banks and credit unions play a critical role in monitoring for suspicious activity. Barnett Software can assist banks in identifying suspicious activity through customer risk ratings, KYC (Know Your Customer) factors, fraud detection and transaction monitoring. These help your team ask the right questions and follow up on accounts with unusual activity.

If you like the stories we tell in our newsletters, you'll love our easy-to-use software. We're Wayne Barnett Software—not a big company, but our products hold their own against Verafin, Abrigo, and the others. Have a question or want a demo? Reach out at rrigdon@barnettsoftware.com or call us at 469-464-1902. Thanks for reading *The BSA Examiner.*