THE FINANCIAL BRAND.com

Can Banks Reduce False Positives in AML?

Anti-criminal procedures meant to catch criminals can inadvertently snare bank customers. Understanding the problem, using data better, optimizing models and communicating more deliberately with customers can all help banks improve the situation for their clients.

By Ingrid Case

In various articles in late 2023, media outlets (including the New York Times) have written about a growing phenomenon: financial institutions unilaterally closing customer accounts, leaving customers bewildered, angry, and without recourse — beyond talking to reporters and making a scene on social media. The fine print they signed gives the bank the right to close their accounts for any reason. But that doesn't soothe suddenly former customers who have lost access to their funds.

The reason, of course, is banks' responsibility to follow laws that aim to prevent customers from laundering money, funding terrorism, doing business in sanctioned countries or violating a long and involved list of international regulations. Sometimes that effort succeeds. But sometimes the procedures meant to catch criminals accidentally snare unsuspecting bank customers. What (if anything) can financial institutions do to improve the situation for their clients?

AI and the Mysterious Red Flags it Offers

A customer's transactions can raise a red flag from one of three sources: The first is the federal government. When it says that a bank needs to shut down a customer account, "there's no recourse," says Aaron Ansari, a principal consultant at Side Channel who works as a chief information security officer for several clients.

The second source is the financial institution's own internal controls. "A financial institution is supposed to create a transaction monitoring system," says Jaco Sadie, a senior managing director at FTI Consulting in San Francisco. That system's design should alert on transactions that aren't normal for a

particular customer, so it works best when the bank collects sufficient information about the customer when someone first opens an account.

But many banks lack the computing power to compare transactions with individual norms, so they assign customers to peer groups and look for transaction activity that isn't normal for that peer group. "It's difficult to get that right," Sadie says.

Building their own internal alert system is expensive and time-consuming, so some banks decide against it. Rather than create a system in house, they buy a third-party offering. That software isn't generally a standalone product, Ansari says. Rather, the functionality that spots potential malfeasance is part of the bank's overall operating software.

"Banks buy one platform that can do multiple things," Ansari says, adding that cost effectiveness is typically the primary driver behind the choice of platform. "It's much more efficient to have one system for everything." Minimizing the number of systems means less training, fewer vendor relationships to manage and fewer instances in which one program won't talk to another. An average bank might have a single software platform handling 80% of its functions, Ansari estimates. Vendors typically test for false anti-money-laundering positives, but not until the system is installed. So. the question "How many innocent customers will we anger?" isn't one that bank managers can easily consider when they choose a software platform.

Most third-party systems use artificial intelligence to spot potentially troubling account activity. That can be cost-effective for financial institutions, but it offers virtually nothing to explain the reasons behind a red flag. "A black box spits out an alert, you're on the list and no human being knows why," Ansari says, adding that this is "really troubling."

> "There's no way for banks to not screw up here. It's a cost of doing business. This too shall pass."
>
> — Aaron Ansari, Side Channel

Without a known reason for the alert, a bank doesn't have a reason to either close an account or look for more, potentially exculpatory information. So, it takes the lowest-risk option and closes the account, figuring that an upset customer is still better than an angry regulator. "There's no way for banks to not screw up here," Ansari says. Banks, he says, "just assume that they're going to break some eggs. It's a cost of doing business. This too shall pass."

That's especially true if the alert has to do with international banking regulations. To investigate that, banks typically bring in one or more attorneys with specific expertise. It's easier and less expensive to simply write off a customer than to perform that deep dive, Ansari says.

Can Banks Reduce False Positives?

But simply closing accounts that garner red flags and enduring customer anger isn't the only way forward for banks around this issue.

"I don't think there's anyone inside a financial institution who would disagree that they want to do better on false positives. No one wants to intentionally hurt customers," says Marcia Tal, who is the current CEO of Tal Solutions in New York and spent 25 years working at Citi. "When there's an error, you're causing your customer pain. That involves risk, too. Even if it's a small percentage of customers, it's happening to a lot of people, and they're not just sitting around being understanding. They're vocal about what's happening. It combines with other feelings of discrimination for them."

Incorporate your own data

Larger banks, Tal says, must decide if they'll make or buy their detection system. If they make their own, she thinks it's possible for financial institutions to incorporate multiple data sources that a third-party system might not.

"Let's say that, as a customer, I have a risk score from behavioral data," Tal says. "I have a set of transactions, a pattern of how money goes into and out of my bank account and my credit card. I've called three times in the last month to ask for account balance. Is there a new calculation we could create that uses information from all those sources? The banks have no shortage of variety and diversity of information."

Banks that choose third-party solutions should keep in mind that they're still in charge of minimizing false positives. "It doesn't matter who built [the system]," Tal says. "You're taking on the decision and the outcome is impacting your customers. You own the risk."Vo

AI can be one part of detecting problematic accounts, but it shouldn't be the only data source in the system, Tal says adding that she'd like to see more caution around how artificial intelligence models are integrated into bank processes. "AI should not be the only tool banks use to decide whether they will close a specific account," she says.

Check your outcomes

If you were designing a mouse trap, you'd look inside it periodically to see if it was actually snaring rodents. Finding the family dog caught in the mousetrap would likely send you back to the drawing board.

That's not how flagged account closures work, points out New Zealand-based Nicholas Gilmour, co-author of The War on Dirty Money and co-founder of Vortex Risk. "No one ever goes and sees whether a bank has actually helped move money illicitly or fund terrorism," he says. Banks and regulators alike are satisfied when banks respond to red flags by closing an account, no matter what activity actually prompted the alert.

This isn't good enough, Gilmour and Tal agree. "The model will never be 100%," Tal says. "But if you wanted to strive to minimize your error rate, you would introduce complimentary processes that would check your model's outcome on a regular basis."

> "The model will never be 100%. But if you wanted to strive to minimize your error rate, you would introduce complimentary processes that would check your model's outcome on a regular basis."
>
> — Marcia Tal, Tal Solutions

Ask third-party vendors about their false positive rates and precautions. Whether you're working with a third-party or home-grown system, checking the model — an activity that's also called tuning or model validation — should happen at least annually, Sadie says. A bank should look for a sweet spot that minimizes false positives while also detecting real suspicious activity. That's a hard point to hit, but trying to get there is still worthwhile.

Get human staff involved

Train employees who receive account flags on how to investigate and consider suspicious activity. "If they see something that doesn't make sense, they should be asking for information from client service teams, which them try to get information from the client," Sadie says. "Maybe a chunk of change that isn't normal for an individual or peer group is an inheritance or gift."

That process requires a good working relationship between investigators and client service team. That relationship gets a huge boost if someone in the bank personally knows a customer, but that's decreasingly likely in a world where more and more people handle their banking entirely online.

Suspicious activity shouldn't necessarily mean immediate account closure — and someone other than the investigator should decide whether an account stays open. Devoting staff time to this process costs money, but the experts interviewed for this article by The Financial Brand thought this was money banks should spend.

Talk to your customers

"If you don't have a means of communication with customers about this, you should get one," Ansari says. Put a dedicated email or telephone number on a bank's website, so customers know how to reach out. Assign a small team to respond.

A closed account "really puts the pain on the customer," Ansari says, and a runaround only increases the misery. Educate customer-facing teams about the account-closing process, so they can explain what's happening to anyone whose account is closed.

A bank can’t release the funds from a cancelled account until law enforcement tells them it can, Gilmour says. Pushing for that to happen in fewer than 90 or 180 days is a service to a customer who may not be able to meet financial commitments without that money.

“We need conviction that we can and want to improve on the outcome,” Tal says. “As sophisticated as we are, we can always get better.”

Ingrid Case is an award-winning journalist and ghostwriter based in Minneapolis. Her work has appeared in Bloomberg Markets, Money, Financial Planning, and other outlets.