Quick Q&A

ON FIRST-PARTY FRAUD

with CRYSTAL BLYTHE

Vice president of customer success and fraud prevention at IDology

With her unique title—vice president of Customer Success and Fraud Prevention—IDology's Crystal Blythe knows full well that her financial services clients can't succeed if they're bedeviled by bad actors.

Advanced identity verification, Blythe says, is the key to thwarting fraudsters who aim to swindle banks and their customers with a combination of first-party and third-party fraud. She's alarmed by the growth of fraud in an increasingly online and mobile environment in reaction to the global pandemic.

IDology, a digital identity and authentication services provider, reported in its 8th Annual Fraud Report in 2021 that fraud attempts increased 53 percent over the previous year across nearly every channel. The most targeted channel, according to the report, was mobile, with a stunning 89 percent increase in fraud attempts.

1 How is first-party fraud different from third-party fraud?

The most common first-party fraud is when an individual applies for a loan and has no intention of paying it off. There are other instances when a consumer misrepresents their financial situation to get a more favorable rate or when a cardholder asks their credit card company to reverse a charge, even though they actually received that purchase. Third-party fraud is, at the base level, identity theft. It's when an individual doesn't know that their information has been stolen and a fraudster has created some type of profile and used their information to apply for a loan. About 34 percent of financial institutions have told us that they see first-party fraud as the most prevalent form of fraud. About 67 percent of institutions reported card-related fraud, which can be both first-party and third-party.

"Financial institutions face competitive market pressures to drive revenue by smoothly onboarding legitimate customers with a secure and frictionless journey while trying to deter fraud at the same time."

2 What is one of the most common forms of first-party fraud?

One form is what we call a "mule"—a consumer who has been persuaded by someone else to use their own information to obtain credit or merchandise on behalf of a larger fraud ring. For example, you're persuaded by fraudsters to apply for a credit card, and they give you $500 upfront to apply for it. But later, you tell the bank or credit-card company that you never applied for it.

3 Why is it difficult for banks and credit unions to identify first-party fraud as the source of their institution's losses?

It's often difficult because the individual applying for a card or a loan is using all their valid information: their first name, last name, street address. Yet they later turn around and say they didn't do it. That's when it becomes difficult to pin down whether this is actually identity theft. Or is this first-party fraud? Either scenario underscores the importance of successfully verifying identities at a time when consumers are not applying as often face-to-face in the branch but online. Financial institutions face competitive market pressures to drive revenue by smoothly onboarding legitimate customers with a secure and frictionless journey while trying to deter fraud at the same time.

4 Is first-party fraud increasing, and if so, why?

From conversations I've had recently and from what I'm seeing in the data, first-person fraud is definitely increasing. The pandemic drove hyper-digital adoption. More people are working remotely. Americans were pushed more online, and those consumers are staying online. Eighty-three million Americans have signed up for online services that were once done in person since the COVID-19 pandemic. Some 50 million online banking accounts were opened in the same time frame, and 94 percent of consumers plan to continue to use all of those new accounts. Those are huge numbers, which unfortunately increases the risk of fraud.

5 How can financial services organizations stay ahead of fraud without adding friction to customers' digital identity verification experiences?

Identity verification is an important security measure as the first line of defense in combating new-account fraud. That's in addition to Know Your Customer (KYC) and anti-money laundering efforts to assess and monitor customer risk. It's critical that businesses have a robust, multi-layered identity verification program beginning at the new account application stage. The best place to prevent first-party fraud is at the point of application because that is where first-party fraud is most likely going to occur. It's essential to be able to verify those individuals in the beginning and taking steps then to make sure that your bank or credit union is pulling in people who are actually going to pay their bills. Banks can balance fraud and friction by taking advantage of data diversity. Fifty-two percent of bankers surveyed said they believe multiple layers of verification were critical to onboarding legitimate customers.

*Content sponsored by IDology. Crystal Blythe can be reached at **cblythe@idology.com**.*

BAI POWERING SMART DECISIONS.