narmi

Mastering the Balance: Tackling Fraud While Prioritizing User Experience

The Impact of Fraud on Financial Institutions

Fraud. It's the constant, ever-evolving threat that plagues financial institutions of all sizes. However, in recent years fraud has become increasingly prevalent and a deeper existential threat to smaller banks and credit unions.

The 2023 State of Fraud Benchmark Report from Alloy revealed some alarming stats about the rise of fraud across the financial services sector:

- **91%** of financial institutions reported an increase in fraud in 2022, while only **1%** experienced a decrease.[1]
- **70%** of financial institutions lost $500,000 in a 12-month period, and **27%** lost over $1 million.[1]
- **67%** of financial institutions have over half of their workforce working on fraud-related activities.[1]

The report also found that 31% of regional banks and 20% of community banks and credit unions have experienced over $1 million in fraud losses in the last 12 months. That in itself would be a shocking statistic. However, fraud experts believe that every $1 dollar in fraud actually costs an institution $4 over the lifetime of a customer - in other words, smaller institutions may be losing millions every year to fraud.[2]

Aside from the dollar cost, fraud also carries additional business and reputational risk. Institutions can face regulatory penalties and legal repercussions for failing to adhere to fraud prevention standards. At the same time, data breaches, phishing scams, and customer identity theft erode customer trust, which is what smaller banks and credit unions are built on. We know that because 1 in 3 consumers have said they are willing to walk away from a business after one bad experience.[3] Therefore, for smaller financial institutions that rely on strong relationships to drive deposit and loan portfolio growth, fraud represents a direct threat to attracting and retaining customers.

Watch a replay of our recent webinar, "Mastering the Balance: How Alloy, Socure, and Middesk Tackle Fraud Prevention while Prioritizing User Experience."

“This is a call-to-action for all of us to continue investing in fraud solutions so that we can stay one step ahead.”

—

Jarad Gilmore
Head of Partnerships | *Middesk*

What is the solution?

Certainly, financial institutions can continue to ramp up spend on fraud analysts and enhanced security controls and systems. But as the frequency and sophistication of fraud attacks continues to rise, this may not be a scalable long-term solution for smaller financial institutions. Furthermore, too many fraud protocols and controls can negatively impact the digital user experience or lead to false positives. As financial institutions continue to fight to retain customer deposits, they’re going to have to strike a balance between enhanced security and user experience.

Rather than overhauling their entire fraud prevention strategy, smaller financial institutions should consider focusing their efforts on the area where fraud begins: their digital front door. By adopting a modern identification verification (IDV) process during the account opening process, financial institutions can root out fraudsters without creating unnecessary layers of friction for new business customers and individual members.

In this whitepaper we’re going to explore:

- Why synthetic identity and account opening fraud are growing concerns for financial institutions
- How IDV and decisioning can help identify bad actors while improving the digital experience
- The power of leveraging fintech partnerships to drive fraud innovation

The Rise of Synthetic Identity and Account Opening Fraud

Fraud attacks can come in many forms, from credit card fraud and account takeovers to phishing scams and payment fraud. But the two fraud vectors that banking executives are most concerned about in 2023 are synthetic identity fraud and account opening fraud.

1. Synthetic Identity Fraud

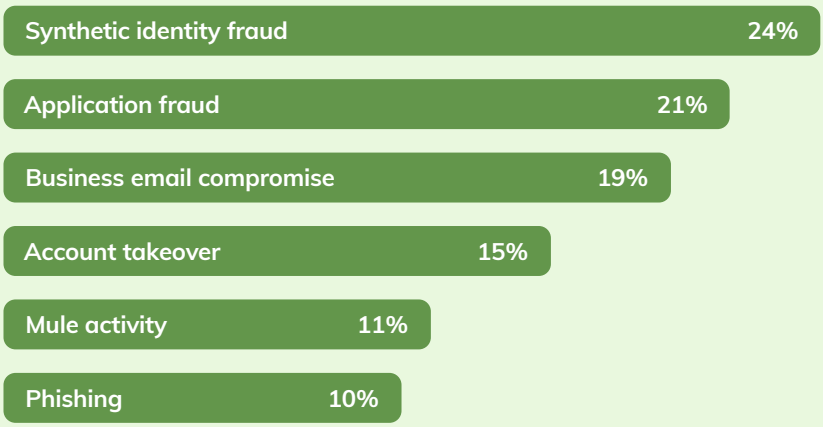
Synthetic identity fraud occurs when a fraudster uses a blend of real and fake personally identifiable information (PII) to create a false identity. A synthetic identity can be created using just a real name, date of birth, or Social Security number (SSN) and be paired with falsified additional information such as a telephone number or email.

2. Account Opening Fraud

Account opening fraud, as the name suggests, occurs when a fraudster opens a new account either using a synthetic or stolen identification. In some cases, fraudsters will use their actual identity to commit fraud (i.e. “first-party fraud”). Other times, fraudsters purchase “identity kits” that contain a person’s SSN, date of birth, and address and use them to apply for credit cards or loans, or open bank accounts in that person’s name. These accounts are often opened to establish credit history and or launder funds.

In the next 12 months, which type of fraud are you most concerned about?

Source: Alloy, 2023 State of Fraud Benchmark Report



There has been a notable uptick in account opening and synthetic fraud in the past few years. This is largely due to a shift towards digital transactions and online commerce that has greatly expanded the opportunities for digital fraud. It is estimated that 15% of consumers conduct between three quarters to 100% of their transactions online. The increase in online activity has given fraudsters considerably more avenues to collect PII and use it to perpetrate synthetic or real identity fraud. As a result, there has been a 52% rise in digital fraud globally between 2019 and 2021.[4]

"Mule activity is going to rise and become the number one concern for deposit accounts next year because of the shifting liability of consumer scam financial laws going back to the receiving bank. That's where receiving banks are going to realize that probably 1-4% of their accounts are synthetic. If you don't do a portfolio scrub now, you might experience heightened losses by the synthetic fraud accounts already in your system."

—

Mike Cook
VP of Fraud Solutions Commercialization | Socure

The COVID-19 pandemic took synthetic and new account fraud to new heights. As the Paycheck Protection Program (PPP) was introduced in the United States to provide financial assistance to small businesses impacted by the COVID-19 pandemic, fraudsters took advantage of a massive opportunity to spin up synthetic identities and business accounts and apply for PPP loans on their behalf. While it is unclear exactly how many synthetic loan applications were created during this scheme, as much as 10% of the $800 billion handed out through PPP loans is estimated to have been fraudulent.[5]

But the initial fraud losses are just the tip of the iceberg. As Carolyn Lu, Fraud Analyst at Alloy explained:

"Synthetic fraud identities are usually built over the span of multiple years as fraudsters build their fake identities' credit history. Fraudsters typically wait 3-5 years to "warehouse" the stolen information before they start using it to apply for accounts. We expect a lot of the PIIs that were stolen in early 2020 when the pandemic started to surface in 2023-24 (exactly three years after the leaks)."[1]

Mike Cook, VP of Fraud Solutions Commercialization at Socure estimates that between 1 and 4% of open active accounts are synthetic. Many of these synthetic accounts may be dormant, quietly acting as "mule accounts" (i.e. accounts set up to fund money laundering or other criminal activities).

Estimates around synthetic fraud losses at financial institutions range from $6 billion to $20 billion per year, but the true totals could be much larger.[6] More alarmingly, financial institutions may be sitting on massive quantities of synthetic accounts within their existing lending and deposit portfolios.

Rethinking Identity Verification and Decisioning

The inconvenient truth for financial institutions is that preventing synthetic and account fraud will become increasingly difficult. Digital fraudsters will continue to find more attack vectors and use sophisticated tools that allow them to duplicate efforts across multiple financial institutions. These fraudsters are also familiarizing themselves with Know Your Customer (KYC) and Know Your Business (KYB) protocols and will go to great lengths to appear legitimate. Some synthetic fraudsters will even spend years making legitimate transactions and building credit before launching a large-scale fraud attempt.

Rather than simply verifying individuals based on their name, date of birth, SSN and credit, what if financial institutions could layer in more complex identity and behavioral biometrics data into their IDV process?

Imagine being able to connect a new applicant's PII to their tax information, utility bills, DMV records, social media profiles, and online spending activity.

All of this data could create a more robust and verifiable profile that would be much more difficult for a synthetic fraudster to fake.

The problem with this approach today is most of this behavioral data is stored in disparate locations. To create this holistic customer profile, new applicants would need to answer more questions during the application process and, in some cases, supply supporting documentation. Then, back-office teams would have to verify that information and make real-time decisions on each new applicant. Some of this is already happening across the banking industry. Around 61% of financial institutions are adding document verification in their onboarding process, according to Alloy.

While document verification and forms of biometric data can mitigate fraud, financial institutions must be mindful that each layer of verification potential creates friction for the end-user.

"There's a balance between security and usability that has to be part of every touchpoint that you have with the customer from onboarding to funding and account maintenance. You want to create friction for bad actors without creating a lot more effort for your customers."

—

Sara Seguin
Principal Advisor | *Alloy*

Bringing Intelligent Automation to Life Through Fintech Partnerships

To strike a balance between fraud prevention and user experience, a new wave of fintechs have emerged to deliver intelligent automation to IDV. Using machine learning algorithms, these fintechs can analyze huge data sets, recognize users' behavioral patterns, and then confirm or deny identities almost instantly.

This approach to IDV can not only deliver faster and better decisioning and approvals, but also allow staff to reallocate time towards enhancing customer service for new digital account holders. Best of all, automated decisions don't require customers to supply additional data or documentation during the application process.

But a good fintech partnership is about more than just new technology. Here are four benefits financial institutions can look forward to when they leverage the right fintech partner for smarter IDV:

Spotting the Bad Actors Faster

New technologies create the means to more accurately segment customers by risk, enabling lower-friction digital experiences (and higher satisfaction levels) for low-risk customers. This means that easily-verifiable applicants can sail through the process, providing more time for back-office teams to review suspicious applicants.

Being Able to “Future-Proof” with Agility

Fintechs partner with institutions of all sizes, giving them a broader view across the fraud landscape. This knowledge gets directly fed into their platforms and solutions, which means their customers benefit from staying ahead of the fraud curve.

Outsourcing fraud innovation means that institutions can handily adopt new protocols, fraud-fighting tactics, and technology as they emerge.

Greater Digital Personalization

Automating IDV opens up a vast universe of data that can help financial institutions understand their customers better. Leveraging existing customer data in smart ways enables institutions to incrementally build trust and offer more personalization across their digital touchpoints.

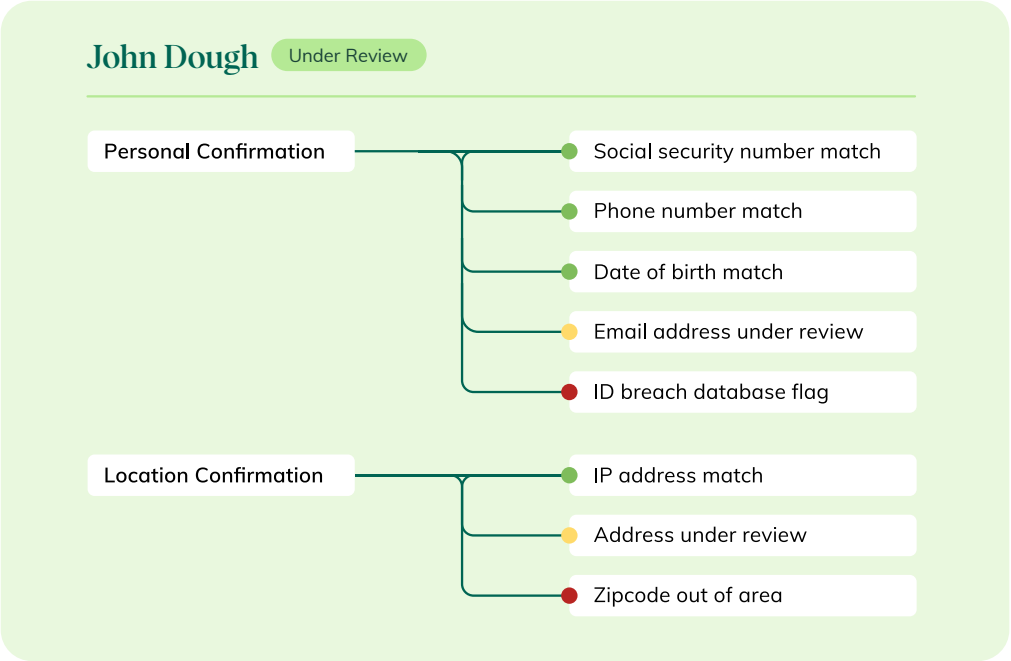
Guidance While Making the Switch

Introducing greater automation to IDV and decisioning is a big mindset shift. However, fintech partners can help take a lot of the risky guesswork out of the process. Since fintech vendors serve a wide variety of financial institutions, many are able to provide templates as a starting point and consult on a wide-array of compliance best practices. Ultimately, a good fintech partner can give teams the extra muscle they need to innovate while taking into consideration the unique challenges and quirks institutions may have.

> **“The fraud landscape is evolving so quickly that it makes sense to leverage external innovation through your partners.”**
>
> —
>
> **Jarad Gilmore**
> Head of Partnerships | *Middesk*

How Narmi Makes Your Life Easier When Decisioning Applicants

Adding automation does not remove back-office employees from the IDV process, but rather gives them a direct look into how the decisioning process is done. In order to make the process as easy as possible for both employees and customers, it is important to weave the automation process into existing protocols. While undergoing the integration, it is recommended to still have the team perform a manual review process to ensure reconciliation. In order to simplify this as much as possible, Narmi offers easy-to-understand, color-coded decision results that allow teams to see red flags in an instant.



Key Takeaways

- By all indications, fraud appears to be a growing threat to financial institutions and their customer relationships.
- Synthetic and new account fraud are two particular vectors to watch, as they carry the hidden risk of long-term fraud losses, customer attrition, and reputational damage.
- Implementing automated IDV can help financial institutions identify fraudsters without diluting their user experience or putting additional strain on their back-office and fraud prevention teams.
- Fintech partnerships can help put financial institutions on the path to automation, while also helping them stay ahead on the ever-evolving fraud curve.

Sources

1. Alloy. “Annual State of Fraud Benchmark Report”; 2023.
2. LexisNexis. “2022 True Cost of Fraud™ Study.
3. PwC. “Experience is everything: Here’s how to get it right”; 2021.
4. TransUnion. “2022 Global Digital Trends Report”; 2022.
5. NBC News. “‘Biggest fraud in a generation’: The looting of the Covid relief plan known as PPP”; 2022.
6. Fiverty. “2021 Synthetic Identity Fraud Report”; 2021.