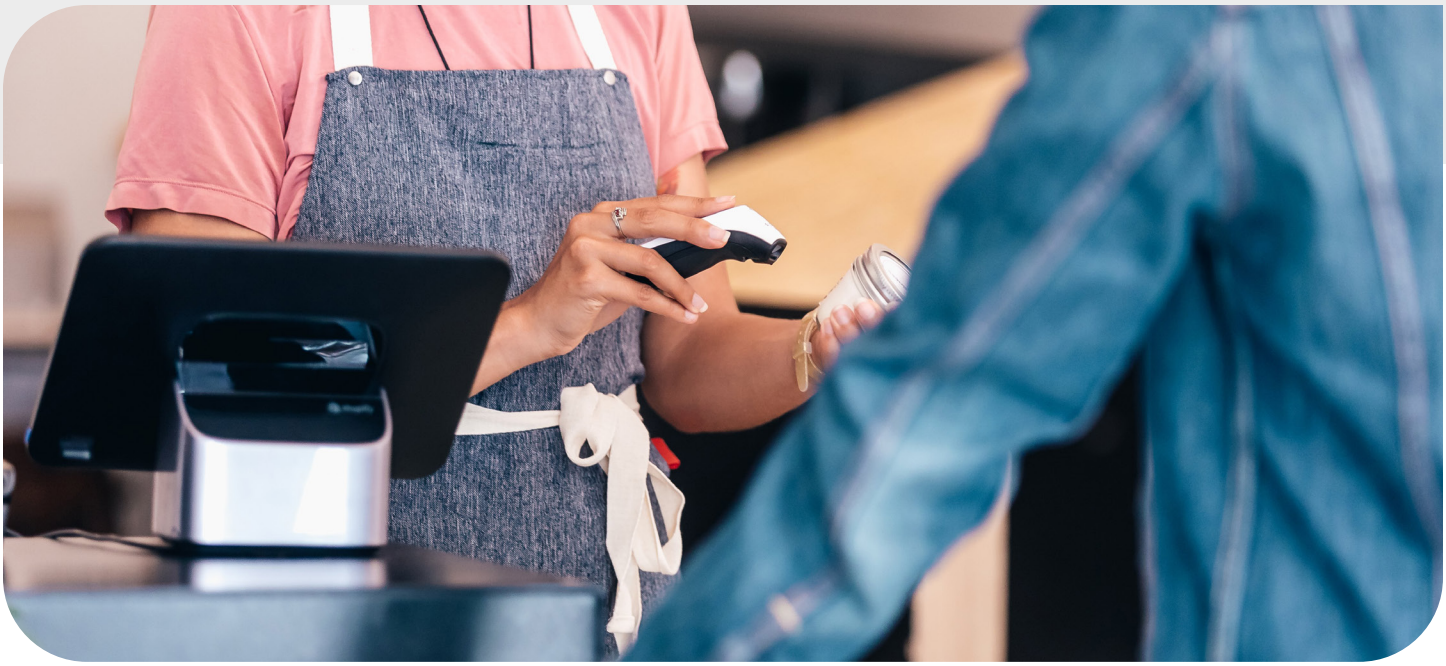
AMOUNT

4 Costly Myths of Fraud Prevention

Is your financial institution falling for them?



Without rock-solid fraud prevention and detection, your digital loan origination strategy can't succeed. But in their effort to develop impenetrable anti-fraud frameworks, many banks and credit unions fall prey to misconceptions that undermine their strategies. For one, it involves much more than just ensuring that the person applying for a loan is who they say they are.

The fraud prevention myths floating around can lead to wasted investments, inefficient security processes, poor customer experiences, and of course, fraud and all of its consequences — including direct financial losses, regulatory fines, and reputational damage. Let's dive into some of the most common misconceptions about fraud detection and why they lead financial institutions down the wrong path.

MISCONCEPTION #1

More Data Partners Always Equals Better Fraud Detection

Let's say you work with a banking technology vendor that touts a huge list of data vendors as its secret sauce to fraud prevention. It's easy to assume that with access to more data, you can make better decisions about a potential customer's identity risk.

Adding more data partners may seem like a surefire way to improve fraud detection, but there's a tipping point where additional data sources offer diminishing returns. It also requires that you know how to work with all of that data and make the most of each of those providers. Instead of aiming to work with as many partners as possible, focus on the most effective partners — those that provide unique, essential coverage.

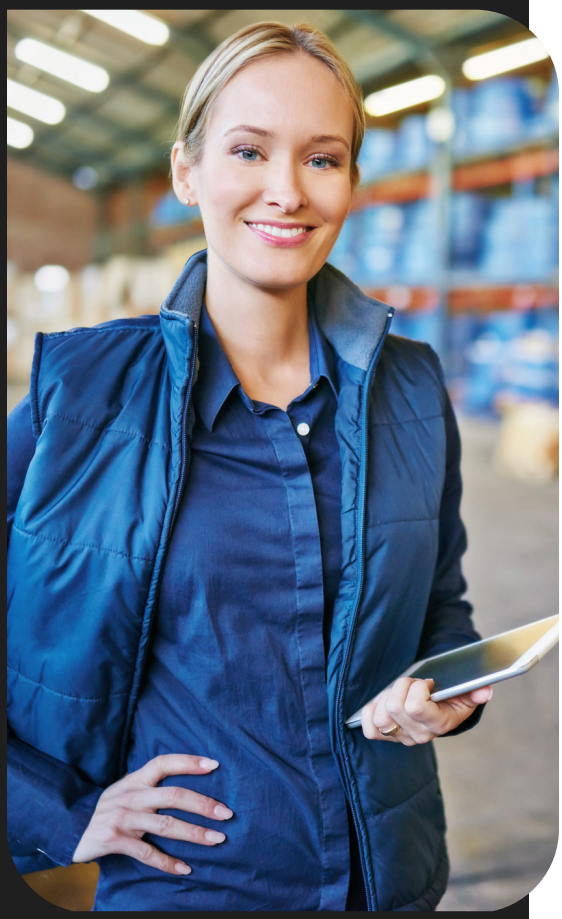
While more partners isn't always better, the opposite is also true. Be wary of consolidating all of your fraud prevention efforts into a single identity risk solution. KYC (Know Your Customer) and KYB (Know Your Business) checks that confirm name, DOB, SSN, and address are table stakes. Beyond screening an applicant's identity, risk-savvy financial institutions will also verify their devices, recent credit activity, bank account ownership, phone, email, and more.

So, instead of working with a laundry list of redundant data partners or over-indexing on a single identity verification provider, financial institutions should select a few essential data partners that each cover a unique aspect of the application process. Additionally, having double coverage in certain areas, such as phone and device intelligence, ensures their fraud detection services remain uninterrupted if one vendor experiences an issue.

Create an extensive and robust fraud detection network by focusing on one or two partners who specialize in each of the following categories:

- **KYC and KYB Verification:**
  Basic KYC efforts for consumer loans are an essential starting point. Verifying information like name, date of birth, SSN, and address can often be handled through credit bureaus. As an extra precaution, financial institutions can access the Social Security Administration's eCBSV (Electronic Consent-Based Social Security Number Verification) service for confirming name, DOB, and SSN.

  For small business loans, the focus shifts to verifying business ownership and legitimacy, which can be managed through KYB services.



- **Sanction Screening:**
  Screening applicants against sanctions lists, such as the OFAC (Office of Foreign Assets Control) list, or Politically Exposed Persons (PEP) lists, ensures compliance with AML (Anti-Money Laundering) and BSA (Bank Secrecy Act) regulations. While these checks are separate from direct fraud prevention, they're critical components of a strong risk management strategy.
- **Email and Phone Verification:**
  Verifying email ownership can reveal the use of compromised or disposable email addresses. Vendors that specialize in telecom data can verify phone numbers, checking who owns the number and how long it's been active.
- **Address Verification:**
  Address data verification confirms whether the provided address is legitimate and matches the applicant's information. This can also help identify potential red flags, such as the use of PO Boxes or commercial receiving agencies.
- **Device Intelligence:**
  Device intelligence tools analyze the device being used to submit the application. By working with vendors like ThreatMetrix or Iovation, financial institutions can identify anomalies in device behavior or detect whether a device has been associated with previous fraud activities.
- **Velocity and Activity Monitoring:**
  Velocity checks help financial institutions understand the frequency and patterns of an applicant's recent credit activity. Services like ID Analytics by LexisNexis offer insights into whether specific identity elements have been used excessively in a short period, which might indicate risk of third-party or first-party fraud.
- **Bank Account Ownership:**
  Verifying bank account ownership is crucial, especially for loan disbursement. The Early Warning Service, a consortium of banks and credit unions sharing data for fraud detection, is highly effective in confirming account details like ownership, account status, and transaction history. Other solutions, like those offered by ValidiFi, leverage ACH networks to verify account validity and status.

MISCONCEPTION #2

Your Strategy Will Prevent All Kinds of Fraud

"Fraud" is a very general term. But when financial institutions discuss their fraud approach, they're often referring to something designed for a specific kind of fraud. There are many different types of fraud, each requiring a different approach. Using the same strategy to tackle all types of fraud can leave some serious attack vectors.

While there are myriad types of fraud financial institutions need to deal with, we'll focus on the three most significant categories impacting account origination:

1. **Third-Party Fraud**
   This involves identity theft, where someone applies for loans, credit cards, deposit accounts, or other credit products using stolen information. Third-party fraud is often the end product of data breaches as well as simpler methods such as dumpster diving, family fraud, or social manipulation
2. **Synthetic Fraud**
   Synthetic fraud involves combining real and fake information to create a new identity. Synthetic identities may pass through traditional identity checks if they include enough legitimate data.
3. **First-Party Fraud**
   First-party fraud occurs when a person applies for a loan using their own real information with no intention to repay or abide by the terms of the financial product. Unlike third-party or synthetic fraud, first-party fraud is as much a credit problem as it is a fraud problem, making it all the more difficult to detect and manage.

Types of Fraud

Third-Party Fraud

Synthetic Fraud

First-Party Fraud

Why Lumping All Fraud Together is a Mistake

When different types of fraud are treated the same way, it becomes impossible to effectively address each one. For instance, identity verification does little to prevent first-party fraud, where intent to repay and creditworthiness are the primary concerns. The tools and strategies that solve for first-party fraud don't overlap with synthetic and third-party fraud. Trying to solve all types of fraud with a single solution creates risk vulnerabilities everywhere.

Instead, financial institutions need a multi-layered defense that applies the appropriate tools and strategies for each type.

MISCONCEPTION #3

AI is the Best/Worst Thing to Happen in Fraud

Depending on your perspective, AI is our most powerful tool in the fight against fraud yet, or a harbinger of the worst attacks we've ever seen. On one hand, machine learning models can identify suspicious patterns and flag potential fraud with sweeping precision. On the other, AI-related threats are real and growing, such as deep fake documents and IDs that are increasingly difficult to detect.

AI isn't a silver bullet for fighting or fueling fraud because many of the most successful schemes rely on good old-fashioned social manipulation. Social engineering and phishing attacks, where fraudsters trick individuals into revealing sensitive information, remain highly effective because they exploit human vulnerability rather than technology. Because attackers don't need to breach a financial institution's IT system directly, no amount of AI can prevent these types of attacks.

That's why human oversight is essential. AI can flag potential issues, automating a valuable part of the fraud detection process. But human expertise is often required to interpret the data. For example, if an institution detects a spike in suspicious activity, it's up to risk experts to determine whether the activity is truly fraudulent and take appropriate action. Educating staff and customer or members about how to manage social engineering risks is essential to staying ahead.

Your financial institution will create a more comprehensive and resilient fraud prevention strategy by acknowledging AI's limitations and addressing the persistent threats posed by social engineering.

MISCONCEPTION #4

Zero Fraud is the Ultimate Goal

Every financial institution should aim for zero fraud. Right? Actually, zero fraud isn't always desirable. Overly stringent fraud prevention measures can lead to rejecting legitimate customer or members and creating unnecessary hurdles in the loan origination process. Financial institutions aiming for zero fraud tend to implement measures that not only deter fraudsters but also drive away genuine customer or members. If the application process is too cumbersome, good customer or members may simply choose a competitor with a more streamlined experience, creating an adverse selection problem.

The truth is, it's unlikely that most institutions will be able to achieve zero fraud. Fraud methods are pervasive and ever-evolving. What's important is how you respond to the fraud that you do see. Having access to the right data and tools to analyze that data will allow you to determine if one instance of fraud is just that — an isolated occurrence — or part of a larger trend that needs to be addressed.

Focus on minimizing fraud as much as possible while keeping the application experience smooth and easy for your best customer or members. Aim to strike a balance between protecting the institution and turning away good business.

Discover how Amount achieves the right balance between security, usability, and customer experience to combat fraud in loan origination. See the platform in action today.

ABOUT AMOUNT

Amount is a global digital origination and decisioning SaaS platform powering high-velocity consumer and SMB origination for financial institutions. Developed by lending industry experts, Amount helps banks and credit unions drive profitability and achieve a Performance Advantage with a fully integrated and flexible platform underpinned by enterprise bank-grade infrastructure and compliance – enabling banks and credit unions to deliver new and differentiated offerings within months, not years.

Let's talk about what we can do for you.

REQUEST A DEMO