MANTL

Fighting back against fraud

A faster, safer approach to online account opening

Introduction

As community banks and credit unions adapt to shifting customer demands, a consensus is emerging: online account opening isn't just another digital tool—it's what you need to remain competitive in the changing world of banking. Here's why.

It's where the industry's headed.

In 2017, 44 percent of primary checking accounts were opened through online or mobile channels. In 2020, that figure rose to 64 percent.

It's what people want.

Consumers who opened a new account digitally in the last three years ranked the experience more highly than those who opened a new account in-branch.

It's the most effective way to grow.

Compared to building a branch, online account opening costs a fraction of the investment and can drive 10 times the results.

However, with every new avenue for account opening comes a new avenue for fraud. As you expand your FI's digital capabilities, it's important to understand how fraud occurs on digital channels, and what you can do about it. The purpose of this paper is to help you answer these essential questions:

Why is fraud escalating in financial services?

How effective is technology in combating fraud?

What are smaller FIs doing to successfully combat fraud?

By gaining a clearer understanding of the current state of fraud, you can find a balance between fraud prevention and customer experience. And with the right tools, your FI can limit the impact of fraud while still offering customers a straightforward path to open new accounts and join your community.

Table of contents

The next frontier in fraud prevention

It's not enough for your FI to simply offer customers the ability to open accounts online.

A fast, seamless experience that is easy to use will not only make customers happier. It's been shown to drive tangible outcomes for your bank in the form of improved conversion rates, higher initial deposits, and deeper customer relationships.

However, online fraud is a growing threat to FIs. Not only does fraud threaten FIs with losses, but it also consumes resources, as staff and budget must be dedicated to its management. Moreover, FIs without best-in-class fraud prevention face a cumbersome volume of manual reviews which may impact other operations across your compliance team.

If you want to open a significant volume of accounts online, your FI needs to put measures in place that will prohibit fraud as much as possible without impacting the user experience.

Protect your FI with a combination of:

Smart CIP verification

Integrated fraud detection and prevention tools

Proven, repeatable best practices

Ongoing study of emerging fraud tactics

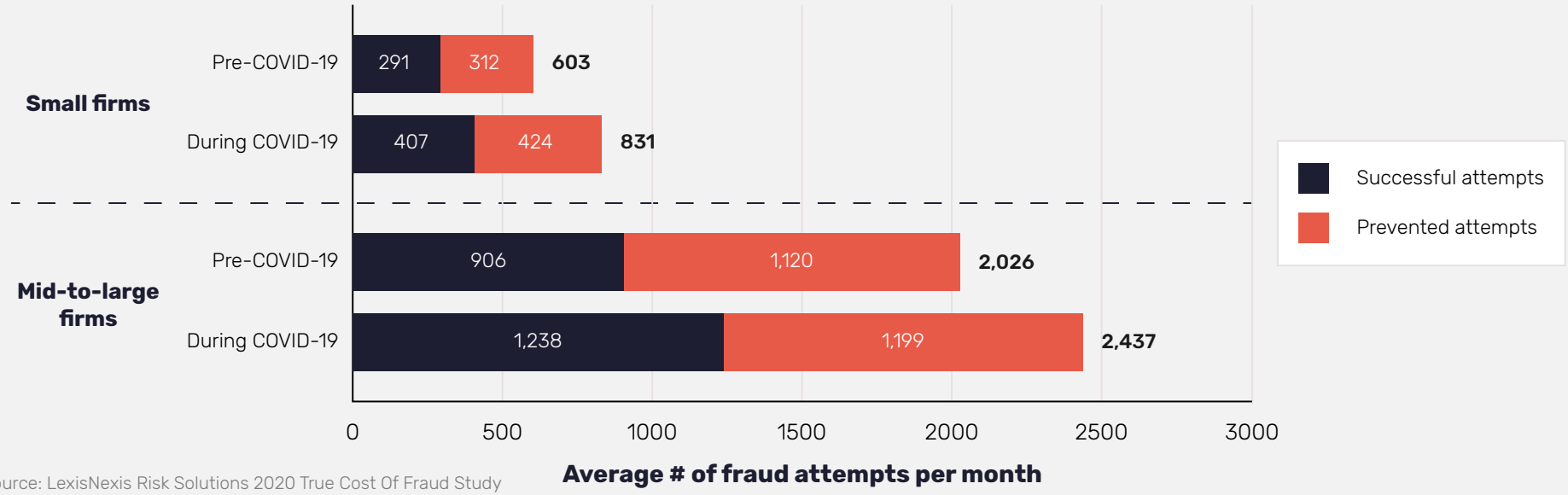
FIs who invest in fraud prevention will find that online account opening, while indeed a new frontier, doesn't have to expose you to more risk than you're comfortable with. And not only will the right tools help you stay protected—they'll actually help you understand what's possible for your FI in the digital space, and allow you to chart the journey ahead.

Digital fraud: an escalating concern

As FIs are becoming more sophisticated digitally, so are fraudsters.

Fraud attempts have become more frequent across financial services—particularly in the case of small institutions, according to LexisNexis's *True Cost of Fraud* study. Since the COVID-19 lockdowns took effect, small FIs (defined as those with annual revenue under $10 million) have been subjected to about 37 percent more fraud attempts each month, on average. Large and mid-sized FIs ($10 million or more in revenue), meanwhile, have seen an increase of about 20 percent.

Digital fraud attempts spiked during the COVID-19 shutdown.



Source: LexisNexis Risk Solutions 2020 True Cost Of Fraud Study

In addition, FIs where 50% or more of all transactions took place via digital channels saw significantly more fraud attempts than their "non-digital" (<50% online/mobile transactions) counterparts did in 2020. Large and mid-sized "digital" banks saw 22% more fraud attempts—including 30% more successful attempts—relative to "non-digital" banks of the same size.

This data suggests:

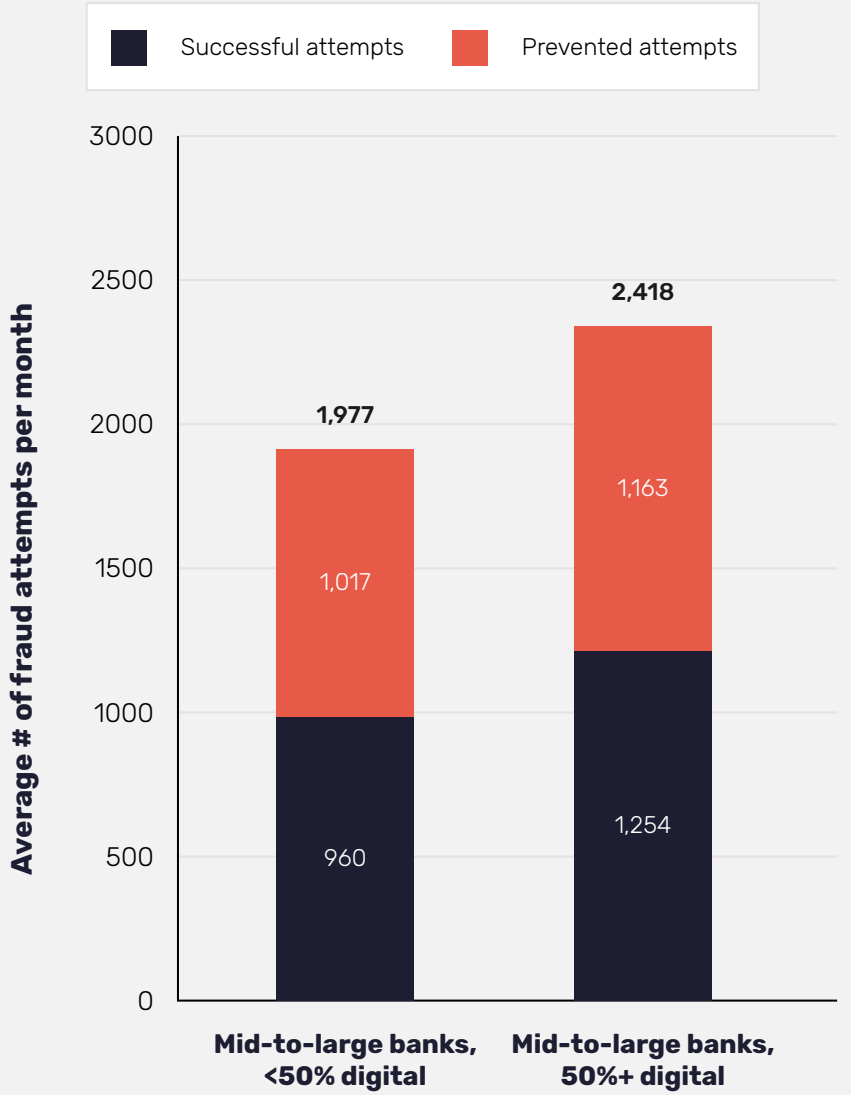
- The pandemic drove an increase in fraud across FIs of all sizes and types.
- FIs who do more business digitally are currently experiencing more attempted fraud.

In even simpler terms, it appears that the pandemic drove more financial activity online. And at first glance, more online financial activity leads to more attempted fraud. A version of this theory has also been proposed by Alloy, whose client FIs experienced a 137 percent increase in high-risk applications in 2020. According to Alloy, the increase was "driven both by overall growth in digital application volume and a comparatively risky population of applicants."

Other, related factors are also amplifying the risk of fraud, according to LexisNexis:

- Consumers are embracing mobile channels, exposing themselves to risk.
- Data breaches have compromised the personal information of nearly half of all Americans over the last five years.
- Economic uncertainty means consumer behavior becomes riskier, giving fraudsters more opportunities to attack.

Digital-heavy banks saw significantly more fraud in 2020.



Source: LexisNexis Risk Solutions 2020 True Cost Of Fraud Study

Fraud losses in FIs amounted to

$56 billion

in 2020

Source: Javelin Strategy & Research 2021 Identity Fraud Study

Clearly, FIs should be concerned about fraud losses, which amounted to $56 billion in 2020. Not only is the shift toward digital channels tied to increased fraud risk—the shift itself only goes in one direction. And it's unlikely to reverse course, as evidenced by the ever-climbing tech spend of megabanks, the persistent trend of branch closures nationwide, and other indicators.

Community FIs face a choice: invest in digital capabilities like online account opening (OAO) and mitigate the fraud as it comes, or avoid playing in the digital space with the intention of dodging the fraud risk altogether. For those who choose the former, the current state of fraud means vendor selection is critical. Those who choose the latter may avoid some risks and costs in the near term. But they run the much larger—even existential—risk of being abandoned by their customers, outpaced by their competitors, and rendered obsolete by the rising dominance of digital channels.

The simple fact is this: OAO is table stakes for growth. Your customers are moving in that direction. That's why it's critical to invest in the right solution, and the right controls, before it's too late. As many FIs have already discovered, choosing a product based on price alone is often a costlier bet in the long run, especially when fraud losses are taken into account. After all, a long-term problem rarely calls for a short-term solution—and FIs must act now to avoid losing any more ground in a rapidly shifting landscape.

Six ways that FIs can fight back

Without the right tools, FIs will find it difficult to combat fraud on digital channels. Many of the best tools, in addition to curbing fraud, also improve BSA, AML, and KYC processes in general, meaning that FIs can also enjoy efficiency gains when dealing with legitimate applicants.

They also automate an overwhelming majority of account decisions.

	Flushing Bank	**Quontic**
Before MANTL + Alloy	75% manual decisions	50% manual decisions
With MANTL + Alloy	10% manual decisions	3% manual decisions

Moreover, these tools are designed with user experience in mind, and fight fraud "behind the scenes" with minimal interruption to the user journey.

1. Layered decisioning

"Layered" decisioning refers to the practice of using multiple data sources at different stages of the account opening process to verify the identity of (and assess the risk associated with) a given applicant.

Alloy's decisioning model, for instance, allows your FI to check against one or more data sources to verify name, DOB, and SSN. Then, additional data sources can be used to verify address, phone number, and other info.

This multi-step approach allows your FI to verify the identity of an applicant against and between multiple data sources. It also allows you to develop a custom methodology that weighs risk factors and data sources according to your institution's needs and risk tolerance. Services like Alloy even allow you to dictate which data sources are called on at specific stages of the process—meaning you can save more expensive data sources for later in your sequence, when they will only be used to validate applicants who have passed all other checks.

2. Funding risk checks

Funding fraud via ACH is one of the biggest risks facing FIs who open accounts online. To combat this, MANTL can check the funding account and method on a new application and compare it to the

identity information provided by the applicant. Even if the identity checks out, the funding account can still be compromised.

Taking identity and funding information together can virtually eliminate funding fraud via ACH. OAO processes which don't include this key step across every channel are susceptible to significant amounts of fraud, as legacy KYC and risk processes don't typically coordinate between funding and identity information.

3. Metadata analysis

When an applicant opens an account with your FI digitally, they share an assortment of metadata: their device and device type, their browser, their IP address, their geolocation, and more. MANTL and Alloy collect this data, and through testing have developed guidelines for assessing the fraud risk associated with certain metadata profiles.

For instance: your FI can write a rule which interrogates each applicant's device IP address, and compares it against the applicant's physical address. While this comparison may not necessarily prove fraud, it can round out the applicant's overall risk profile, and your FI can set rules to automatically trigger manual review or rejection based on a combination of such factors.

4. Safe funding methods

FIs should provide multiple funding methods for new account applicants. However, some funding methods like credit cards are disproportionately correlated with fraud, and should be avoided in favor of safer methods like debit cards or instant account verification.

5. Smart security measures

Some security measures, like requiring out-of-wallet questions, will result in a significant hit to conversion rates. Instead, consider two-factor authentication. This feature can reduce submission rates by 8%, but nearly 80% of this lost traffic is likely to be fraudulent, according to an analysis of MANTL customers. So while 2FA does reduce conversion, its ability to curb fraud represents a worthwhile benefit.

6. Monitor usage patterns

Short of implementing real-time transaction monitoring, FIs can take other steps to understand how users are interacting with their products. If a given product or service (e.g., checks or debit cards) is being used in a manner other than intended, this may indicate potential fraud.

A superb account opening experience doesn't have to come at the cost of increased fraud.

> **With MANTL, your FI can efficiently open accounts online while enjoying the peace of mind that comes with best-in-class fraud prevention tools and automation.**