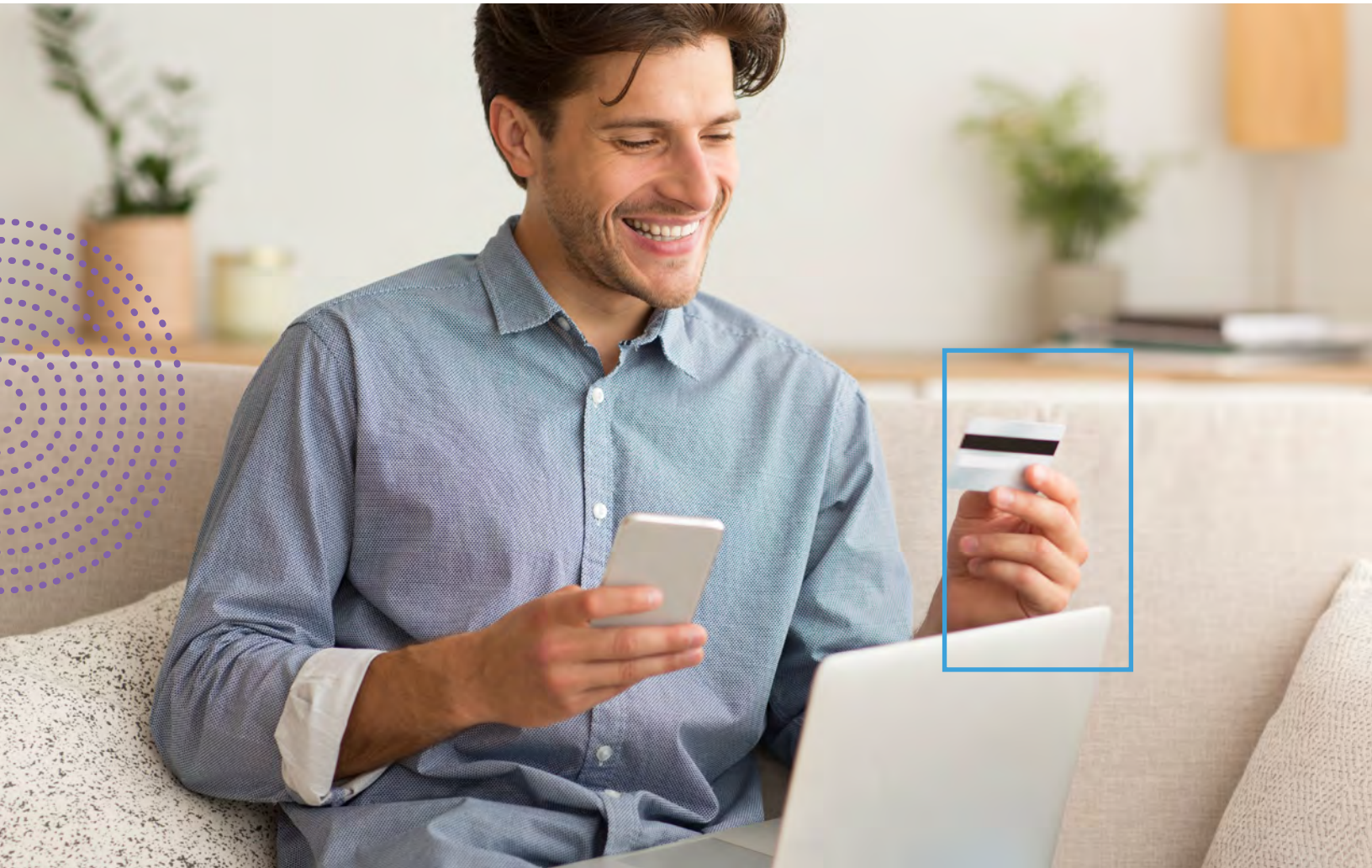
feedzai

A Guide for Community Banks

Democratizing Machine Learning



feedzai

Contents

COVID-19: A Bane for Banks and a Boon for Fraud

In an always-on, interconnected digital environment, today's consumers have certain expectations of their financial institutions. Specifically, they want to be able to conduct their banking business at whatever time they like, from any place in the world, and from any connected device.

The global COVID-19 pandemic accelerated the shift to digital banking services for many consumers. As the pandemic forced communities worldwide to implement social distancing guidelines and lockdown measures, many consumers were unable to visit a local bank branch or ATM kiosk in-person. Many consumers were unwilling to put their financial lives on hold, even during a time of unprecedented disruption. Instead, they engaged with their banks and financial institutions using mobile devices and online portals instead.

How the pandemic changed banking

The report, *Leveraging the Digital Banking Shift*, a collaboration between Feedzai and PYMNTS, outlines how U.S. consumer banking practices changed in light of the pandemic. The report surveyed nearly 2,200 U.S. banking consumers about how their banking habits changed since the pandemic's early days and found:

~30%

of respondents had opened new bank accounts in the previous three months.

78.6%

of respondents saying they'll keep using these features beyond the pandemic.

40%

of consumers from all age groups described themselves as mainly digital banking consumers, including older consumers who fall into the baby boomer and senior age bracket (ages 56 and older).

74%

of respondents said they intend to maintain all or some of the digital banking habits they picked up during the pandemic.

Based on these figures, it's clear many of today's banking customers prefer to use online channels and mobile devices to connect with their banks – and they're highly unlikely to change back. This means bank customers may never set foot inside a physical branch or interact with bank employees.

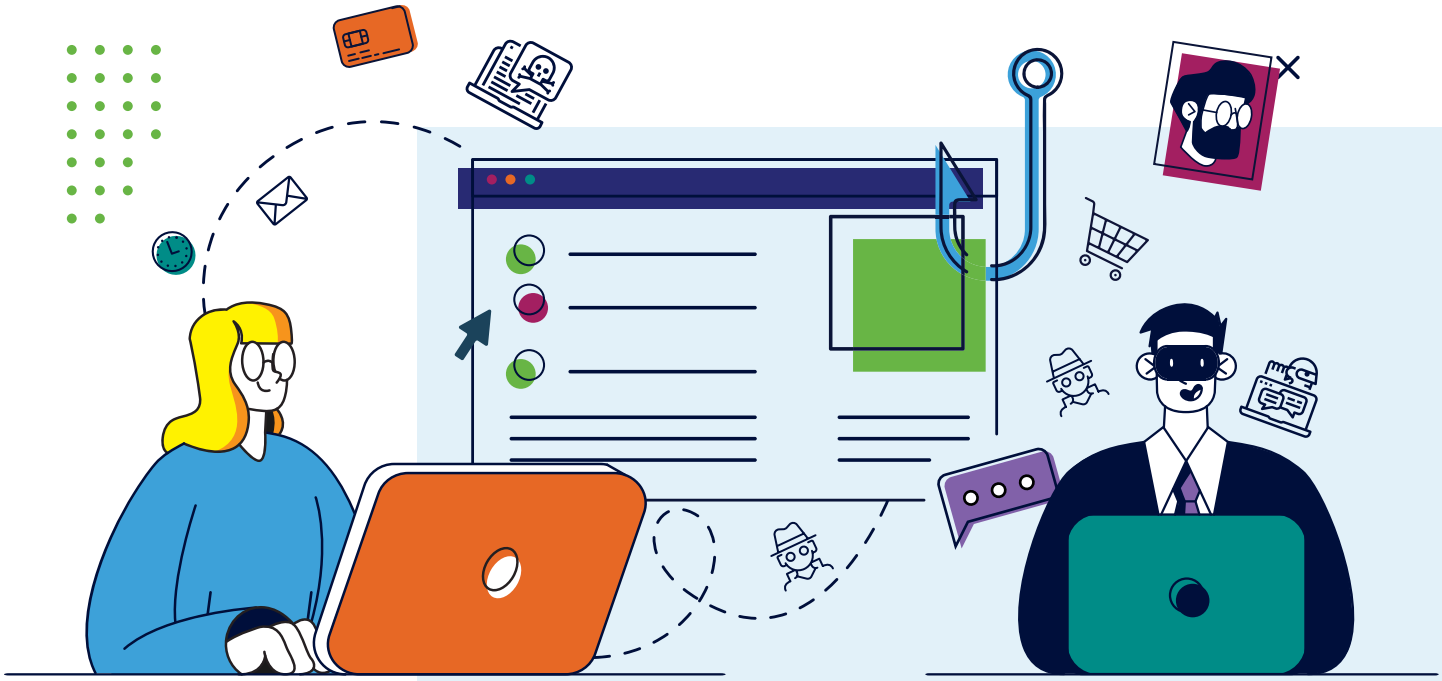
The Future of Fraud

While the pandemic created chaos for banks and customers, fraudsters saw something different: A new world of opportunity. Uncertainty, sky high unemployment, small businesses in collapse, and inexperienced digital banking customers essentially presented a feeding frenzy for bad actors to make ill-gotten gains.

COVID-19: A fraudster's paradise

COVID-related fraud came with a hefty price tag. In the U.S., the Federal Trade Commission received more than 200,000 consumer complaints as fraudsters targeted unemployment benefits and federal stimulus payments and pushed scams related to personalized protective equipment (PPE) and COVID-19 antibody tests. The total value of these fraud losses surpassed $145 million USD.

The U.S. isn't alone. Across the pond, the United Kingdom's Bounce Back lending program – which was designed to help the nation's economy recover from the pandemic's economic devastation – reportedly lost £26 billion (equivalent to $35 billion USD) to fraud.



How was fraud on such a large scale possible?

Banks, like other industries, had to adjust to new routines because of COVID. This includes call center workers and fraud teams displaced by being forced to work from home. This disruption often made it challenging to collaborate and communicate effectively with other team members. Bank employees found themselves physically distanced from co-workers and unable to ask important questions about suspicious transactions. Some bank employees and fraud teams faced delays in receiving their work equipment at home, had to use slower internet connections, and were unclear about remote work policies.

22%

of American consumers claimed they had been targeted by online fraud related to COVID-19.

On the other hand, the same social distancing practices and lockdown measures that disrupted the lives of countless everyday people hardly made an impact on many fraudsters' routines. While being forced to work from home took some getting used to for people who normally commuted into an office on a daily basis, fraudsters tend to work from home already and were prepared to take advantage of the resulting confusion and chaos.

Displaced fraud and risk teams, an influx of unseasoned and inexperienced eCommerce consumers, and rapidly developing news about the pandemic gave fraudsters numerous opportunities to pull off different scams, sometimes by tapping into fears over scarcity and uncertainty. Fraudsters might offer an unsuspecting consumer a deal on a high-demand item – like NPP masks or other medical supplies – using phishing tactics like a fake website or an email promotion. The consumer believes they've purchased much-needed products. In reality, however, they've been tricked into divulging sensitive information like credit card numbers, bank accounts, or possibly their home addresses. A TransUnion study released earlier this year found 22% of American consumers claimed they had been targeted by online fraud related to COVID-19.

Making Machine Learning Accessible for Community Banks

Machine learning can help banks as they seek to balance maintaining the level of trust they have built with their customers, delivering engaging and user-friendly digital banking experiences, and preventing fraud. In the digital banking era, going back to traditional banking practices, like requiring in-person visits for onboarding or manual reviews, is off the table. Having machine learning platforms in place is essential for banks to meet the needs of today's digital-first customers. It's also essential to staying a step ahead of tomorrow's fraud challenges.

By some estimates, banks could save approximately $1 trillion through AI investments. The potential benefits for banks that invest in AI and machine learning technology include:

- **An estimated 30% increase in revenue.**
- **A 25% reduction in costs.**
- **A 54% reduction in false positive alerts.**
- **In some cases, saving roughly 360,000 labor hours per year with process automation.**

Walking the Cost and Control Tightrope

Both larger banks and challenger banks have the financial resources available to make investments in technology like machine learning. Community banks and credit unions, on the other hand, tend to be more conservative with their innovation agendas, which is likely why many have put off investing in machine learning platforms.

As if the price tag wasn't enough to worry about, uncertainty over whether a machine learning platform investment will dominate community banks' limited resources is another cause for anxiety. Some banks will wonder if a machine learning platform will require them to divert personnel resources away from day-to-day operations and take a long time to fully implement. Adding to the uncertainty is the question of how to measure a machine learning platform's effectiveness. Because community banks often lack the tooling, expertise, and operational models to support a 24/7 monitoring system they are more likely to turn to a third-party service provider to handle fraud on their behalf.

At the end of the day, machine learning platforms can reduce their fraud losses and false positive rates and bolster their anti-money laundering efforts. But these potential rewards come with heavy risks, such as how much the investments could cost banks in financial resources, personnel resources, time, and whether they will cause massive operational disruptions. The risk of not investing in AI and machine learning, hoZwever, considerably outweigh these other considerations.

Community banks may also be concerned about being able to support and continually maintain an on-premise machine learning solution. With IT resources already stretched thin, some banks worry whether the investment will lead to significant downtime or interrupt their customers' experiences.

However these concerns do not need to be an impediment for banks to pursue their machine learning ambitions. Instead of on-prem solutions, banks can instead choose cloud-based machine learning platforms solutions that can help community banks to quickly realize the rewards of their machine learning investment. These cloud-based solutions can be put to use immediately without requiring banks to make physical accommodations or requiring constant attention from bank employees.

How to Close the Machine Learning Gap

How can community banks access the power of machine learning without depleting all of their resources and giving up control of their systems?

It's important to focus on the essential machine learning features that you need without getting distracted by any unnecessary bells and whistles. Think car shopping: The Cadillacs and Teslas might be flashy but a Prius or a Civic will also get the job done.

What Should Community Banks Look for in Machine Learning Solutions?

When selecting a machine learning solution, community banks need to look at solutions that are capable of solving three major challenges:

6 Questions to Ask When Investing in an ML Fraud Platform

Of course, there are numerous machine learning solutions available, and choosing the right one can feel overwhelming. At the end of the day, however, community banks should ask the following questions about the machine learning solution they want to purchase:

1. **Does it aid in the bank's evolution of becoming a digital-first business?**
   The solutions should have the ability to score transactions from both old and new digital channels. An even more capable solution will not just score these channels in isolation, but will take scores from across channels into consideration when making decisions.

2. **Does it assist in the development of new and more modern customer experiences?**
   With new experiences come major shifts in customer behaviors. Machine learning solutions that are built for community banks should have the capability to adapt to these behavioral changes and, as a result, provide customers with both a secure and smooth banking experience by easily identifying fraud.

3. **Does it ensure compliance across banking products?**
   While doing the above, machine learning solutions need to also ensure that as community banks move through this digital evolution that they don't unnecessarily expose themselves to risk. Maintaining compliance is at the forefront of every banking official's mind, and a machine learning solution built for a community bank should not only meet compliance requirements, but also help reduce the legwork that goes into it (through reduction of false positives, etc.).

4. **Will the vendor do the heavy lifting?**
   Becoming a machine learning expert doesn't happen overnight. And, it's okay if the information doesn't reside internally. Machine learning providers should have teams that can help guide community banks in the creation of a cohesive data strategy — ensuring that once you make an investment in the technology that you can achieve the maximum benefits.

5. **Should I go with a custom or packaged solution?**
   While custom solutions often boast the most features and overall greatest controllability, they come with their own set of challenges. Custom solutions take a lot of upfront work, often resulting in much longer deployment periods and harder-to-justify ROI at community banking scale. While you might have more options with a custom solution, the higher cost might (and should) quickly disqualify them. Alternatively, packaged, or standardized, solutions are a great way to leverage the benefits of machine learning without incurring nearly the same cost and resulting maintenance requirements.

6. **Does the solution deploy on the cloud?**
   Deploying a solution on the cloud, as compared to on-premise, greatly reduces the overall maintenance costs that are typically associated with machine learning solutions. Also, not having to invest in the framework to support such a solution reduces the necessary upfront investment — and, in turn, the risk of adopting a new ML solution.

Affordable Fraud Prevention Machine Learning Checklist

Future-Focused

The machine learning platform should deliver best-in-class risk detection that can address both today and tomorrow's fraud-related challenges. Banks should ask if a machine learning platform:

- Packages fraud with anti-money laundering (AML) – or FRAML – solutions.
- Can scale rapidly and easily.
- Provide ready-to-go detection scenarios and case investigation scenarios.
- Leverage financial crime expertise that enables banks to focus on their day-to-day operations.

Regulatory-Friendly

Customers are not the only ones banks and FIs need to keep happy. Machine learning platforms need to deliver decisions that meet existing financial regulations – and that can ensure banks meet updated ones. To meet regulatory body requirements, machine learning platforms should:

- Deliver transparent models and decision-making.
- Enable users to meet regulatory scrutiny.
- Offer new approaches to risk (such as FRAML) and provide all relevant information to enhance investigation results.

Customer-Friendly

Any machine learning platform should be able to meet the needs of digital-first banking customers who conduct their business using multiple channels. Machine learning platforms should:

- Provide banks with greater certainty over decisions and reduce friction for legitimate customers.
- An omnichannel view that delivers the same experience to customers across all banking channels.
- Support new and emerging channels that allows customers to bank how and when they want to.

Easy to manage

Like a car, banks will want to be able to control and manage their machine learning investments. Machine learning platforms should:

- Provide zero downtime to deploy across an organization.
- Be agile with strategic decisions and enable third party implementations.
- Offer free product updates to allow continued performance and prevent interruptions.

Tackles Risk

Machine learning platforms should enable banks and FIs to convert their data into actionable intelligence and determine the best approach to fight fraud and reduce risk. Machine learning platforms should:

- Quickly operationalize data across all banking touchpoints.
- Enable banks to build 360 degree customer profiles to determine normal behaviors.
- Be able to use rules and models to detect subtle shifts in behavior and initiate an appropriate response.

Understanding these criteria are essential for smaller banks and credit unions that are eager to bridge the machine learning gap that separates them from larger FIs. No bank wants to spend money on an investment that fails to deliver. Having a checklist to measure a machine learning platform's effectiveness can assure banks that they made the right investment and can match their larger competitors in technological innovation.

feedzai

One Platform to Manage Financial Crime

Every year, Feedzai's risk management platform scores trillions of dollars of transactions to protect the world's largest companies. Fully AI-enabled to stay ahead of emerging financial crime and money laundering patterns, Feedzai mitigates even the most deceptive criminals so that banks, issuers, acquirers, and merchants can focus on growth.

Feedzai is considered best in class by Aite and one of the most successful AI companies by Forbes. The world's largest banks, processors, and retailers use Feedzai's fraud prevention and anti-money laundering products to safeguard trillions of dollars and manage risk while improving customer experience.

Account Opening | Transaction Fraud | Anti-Money Laundering

feedzai.com **info@feedzai.com** **sales@feedzai.com**