White Paper

Achieve Sophisticated Fraud Detection and Prevention at a Fraction of the Cost of an Enterprise Solution

effectiv

September 2022

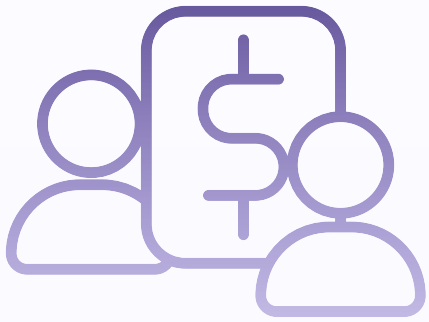
effectiv

Achieve Sophisticated Fraud Detection and Prevention at a Fraction of the Cost of an Enterprise Solution

How a scalable, turnkey, customizable fraud prevention solution can level the competitive playing field for community banks and credit unions and protect against increasingly sophisticated threats

State of the Industry

The race to digital transformation has been a hot topic in financial institutions for the last several years—but the global pandemic, with forced lockdowns, temporary branch closures and social distancing requirements ramped up consumer demand for digital banking. Conditioned by leading retailers to have 24/7/365 access to everything from anywhere—seamlessly—set the stage for customer expectations for banking.



Digitalization also ramped up the pace at which fraudsters targeted the financial services industry. Comparing the period from September – December 2020 to January – May 2021, suspected digital fraud attempts increased 149 percent—most of it from identity theft.[1] In comparison, fraud increased 24 percent across all industries.[2]

Fraud from new online account and loan applications is particularly noteworthy—and costly. Every dollar of fraud lost in 2021 cost financial services firms $4.00, up from $3.64 just before the pandemic—and online banking accounted for one-third of those costs.[3] The impact to consumers is also staggering. Consumers lost nearly $52 billion to traditional identity fraud and identity fraud scams last year—and almost $7 billion of it was due to new account fraud.[4]

Some figures show as many as 50 percent of new accounts opened in 2021 were fraudulent[5], but finding the exact impact of losses due to identity fraud is difficult because many times, financial losses resulting from non-payment of fraudulently cultivated and nurtured accounts just look like typical consumer non-payment. While the exact monetary impact of account opening, loan application and payments fraud is hard to specify, all agree it is a massive—and growing—concern. And, it's keeping executives awake at night.

---

1 "Increase in Digital Banking Facilitating Equal Rise in Financial Fraud Attempts". The Fintech Times. June 25, 2021.

2 Ibid.

3 "Study: Banks See Rise in Fraud Attempts, Associated Costs in 2021". ABA Banking Journal. January 6,2022.

4 "New-Account Fraud: A Threat Down Every Avenue". Javelin. June 9, 2022.

5 "New Fraud on the Block Causes Bank Losses to Rise". Bank Info Security. April 13, 2022.

Current Know-Your-Customer (KYC) controls designed to confirm the identity of consumers opening accounts and applying for loans are designed to mitigate identity fraud, but can be cumbersome for resource-strapped financial institutions (FIs) to manage. And fraudsters, employing laser focus and capitalizing on resourcing and servicing challenges faced by financial services firms, often manage to stay one-step ahead.

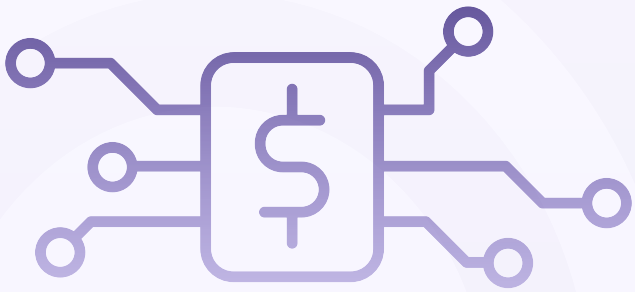
In the ever-evolving fight against fraud, technology to effectively and efficiently fight financial crime is mission critial. While "big banks" have been adding significant capabilities due to their deeper pockets, other FIs have been at a disadvantage against these competitors and are also seeing more incoming pressure from fraudsters as evidenced by the numbers above. Disadvantages around budget, resources and talent have conspired to chip away at competitive advantage. And FIs of all sizes have been reluctant to add points of friction to onboarding that threaten the consumer experience and risk lost business. But there is a technology-based solution that can help level the playing field by providing community-based financial institutions the same level of safety and sophistication—as well as a seamless consumer digital experience—as large competitors for a fraction of the cost of an enterprise fraud solution—all enabled machine learning (ML).

The Capabilities Gap

As consolidation of U.S. financial institutions continues), the competitive gap between large and smaller FIs widens.

Increasingly, "big banks" and the largest credit unions are better positioned to leverage competitive advantages around increased product and service innovation, speed of delivery, convenience and fraud detection/prevention capabilities enabled by vast investments in sophisticated technology. James Bessen from Boston University argues, "Advanced information technology, investment in automation and the accumulation of proprietary data and insights are allowing the largest financial institutions to dominate the banking ecosystem."[6]

Overall technology spending rose 10 percent in 2021, according to respondents of Bank Director's 2021 Technology Survey, with only 20 percent of large banks believing they don't spend enough compared to 41 percent of banks under $500 million.[7]



The survey also revealed that while the U.S.'s largest banks invest around one percent of assets in technology, smaller banks (less than $500 million in assets) spend more—three percent. Ten percent of that spend is earmarked for ancillary technology—but that still does not matching big bank competitors in terms of efficiency, sophistication or capabilities.

---

6 "How Big Banks' Tech Advantage Hinders Innovation and Hurts Competition". The Financial Brand. July 12, 2022.

7 "2021 Technology Survey Results: Tracking Spending and Strategy at America's Banks". Bank Director. August 30, 2021

8 Ibid

And America's largest banks fully comprehend the competitive advantages enabled by technology. In response to the survey, JPMorgan Chase & Co. Chairman and CEO Jamie Dimon said, "We think we have [a] huge competitive advantage…," and believes that technology will be one of the leading drivers of revenue for the bank.[9] For example, Chase spent $11 billion on technology last year that fueled projects including a buy now, pay later (BNPL) loan product and a digital investment platform as well as direct investment in fintech companies.[10] To compete, smaller FIs will need the same level of sophisticationat a more reasonable cost to help level the playing field.

When it comes to investments in fraud detection and prevention capabilities specifically, most thoughts around ROI revolve around stemming financial losses from fraud, but, as consumers become increasingly aware of and concerned about the safety of their accounts and financial identities, the perception of their FI's ability to protect them can make or break a relationship and result in lost business for institutions thought—or proven—to be less capable than larger counterparts.

According to one survey, 11 percent of credit union members choose other financial institutions for certain offerings because they believe they will be greater protected from data and identity theft—and nine percent believe these other FIs provide a higher degree of protection from fraud.[11]

Regarding fraud detection and prevention technology, 35 percent of financial institutions in one survey didn't believe they had the "correct level of investment and proper technology in place in any stage of the customer life cycle to detect and prevent fraud."[12] Research also shows that 40 percent of FIs still use legacy, rules-based systems and 26 percent rely on manual reviews for detecting fraud.[13]

The fact of the matter is for community banks and credit unions to not only survive, but thrive in the face of increased consolidation and competition, they must offer the same level of protection and sophistication as large competitors when it comes to detecting and preventing fraud.

Sophistication goes beyond just accuracy in detecting fraud before it happens—it also means minimizing friction across all points in a transaction—whether opening a new deposit account, applying for loan, paying by credit card, or completing a person-to-person (P2P) payment—wherever and whenever consumers choose to do so. And the ability to provide them with a superior, seamless and safe application and payments experience across every channel has been one way big banks have leveraged expensive enterprise fraud solutions to gain a competitive advantage.

9 Ibid

10 Ibid

11 "How Credit Unions Can Work to Identify and Eliminate Fraud Risks". PYMTS.com. December 30, 2021.

12 "Don't Wait to Optimize Fraud Technology." Guidehouse. 2021.

13 "How Credit Unions Can Work to Identify and Eliminate Fraud Risks". PYMTS.com. December 30, 2021.

Online account abandonment, for example, is a costly problem for financial institutions. Both consumer expectations for a seamless, delightful experience and account abandonment are at an all-time high.[14] Abandonment rates increase significantly as the time to open an account or complete an application increases.[15] If it takes longer than five minutes to open a new

account or complete a new loan application, the abandonment rate can be as high as 60 percent.[16] Processes that are faster than five minutes; however, can reduce abandonment rates to 25 percent or less.[17] Eliminating points of friction that threaten a seamless, end-to-end experience has the potential to double or triple the number of new accounts opened and loan applications submitted.

Processes that are faster than 5 minutes can reduce abandonment rates to 25% or less.

On the other hand, increasingly savvy and wary consumers will also abandon the onboarding process if they don't perceive it as secure. Among consumers who have already experienced new account fraud, the number-one reason for application abandonment was the "...process was taking too long" and the next three related to perceived safety and security.[18]

Yet another way big banks are benefiting from large scale investments in enterprise fraud technology is in reengineering the behavior of fraudsters.

As early and obvious targets for identity fraud—as well as early adopters of sophisticated enterprise fraud solutions in response—big banks are beginning to see their investments pay off. Nimble fraudsters are turning their attention to financial services providers that are more likely to suffer weaknesses in prevention due to lagging technology. Community banks and credit unions as well as fintechs, such as BNPL providers, are now likely to be targeted more than ever as big banks shore up their fraud detection and prevention capabilities.

So, how can smaller FIs level the playing field given these challenges and the delicate balance needed to meet and exceed consumer expectations for speed, convenience and safety as well as mitigate losses due to fraud?

---

14 "Solving the Mystery of Online Application Abandonment". Credit Union Times. July 12, 2021.

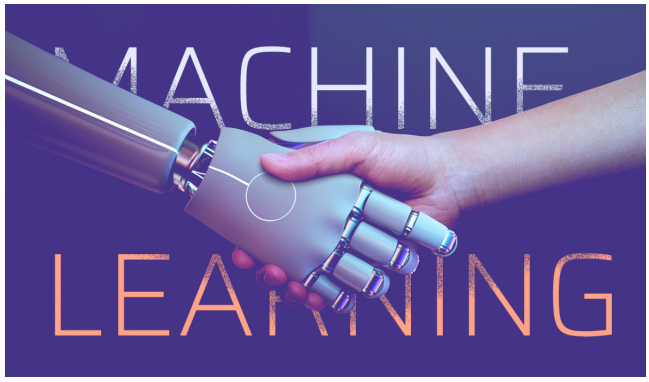
15 "How Banks Can Increase Their New Loan Business 100% (Or More)". The Financial Brand. April 13, 2021.

16 Ibid.

17 Ibid.

18 "New-Account Fraud: A Threat Down Every Avenue". Javelin. June 9, 2022.

Machine Learning: The Game Changer



What do underdogs do when the chips are stacked against them? They work smarter, not harder. Progressive advancements in integrating machine learning with fraud solutions allow community banks and credit unions to do just that.

In one survey of financial institutions, 55 percent identified KYC process improvements as the top benefit of leveraging ML against financial crime.[19] Make no mistake, large financial institutions are already using fraud solutions built with ML, but smaller FIs can now benefit from the same protection and process improvements as their larger counterparts for a fraction of the price.

How Machine Learning Works for Fraud Prevention

Machine learning works by assimilating large amounts of available information and identifying patterns that can differentiate between normal and abnormal attributes and behaviors. By automatically updating rules and limits, ML allows FIs to reduce false positives that drive manual reviews, increase auto-approvals for new accounts and applications, and simplify fraud analysts' jobs by providing deeper insights when manual reviews are necessary. Additionally, fraud detection powered by ML only gets more accurate over time. As false positives are identified by the solution, the solution will eliminate them going forward.

For a simple example of how ML drives a more accurate and efficient KYC process as compared to a manual or rules-based system, let's say that a potential identity fraudster attempts to apply for a credit card using your website. Using a mix of stolen credentials (a synthetic ID)—the name of someone local to your institution, a stolen SSN from a deceased person, a different, but real, address in the area, a picture ID showing their name and address matches, an email address and mobile phone number they control, and other pieces of actual or manufactured information—their application passes a rules-based review process. Fast-forward 6 months and they'll have maxed out their credit line and suddenly stopped paying the minimum monthly payment, leaving your institution with a charge-off. What's more, you may not even ever realize you've been hit with identity theft. Without ever knowing, you may just assume the consumer was no longer able or willing to repay their debt.

19 "Using Machine Learning to Thwart Financial Crime." Guidehouse. 2020.

Now, with a machine learning-enabled solution, that application information would be run through numerous integrated data intelligence checks in real-time. The solution would identify that the SSN, the email address and mobile phone number, for example, as well as the address does not match up with the most recent information available in the ether for the person claiming to be the applicant. Depending on the severity of the mismatched information, as well as customized risk tolerance levels set by the institution, the application would either be flagged for manual review by a fraud analyst or denied altogether.

Benefits of Machine Learning in Fraud Prevention

While all fraud detection and prevention solutions require some level of human intervention to analyze exceptions and rejected applications, a solution that employs machine learning will minimize this, freeing up resources for more strategic initiatives. Specifically, fraud prevention enabled with ML offers these benefits:

- **Improved accuracy** – The solution will be continually trained to analyze and detect patterns across large amounts of seemingly disconnected data that would be impossible for humans to analyze and detect. This not only helps better detect suspicious activity, but it will also help reduce false positives.
- **Increased speed** – ML can evaluate enormous amounts of data in a very short amount of time—in near to actual real-time —in line with consumer expectations for speed and convenience.

- **Improved efficiency** – With its continuous learning and improvement, ML can catch subtle changes in patterns across large amounts of data. This means the process of fraud detection becomes not only more accurate over time, but also speedier as unproductive processes get eliminated from the workflow, saving analysts even more time on reviewing exceptions.
- **Scalability** – ML capabilities level the playing field for community banks and credit unions. Staff resources do not have to be increased even as application volume or fraud activity increases—all while sacrificing nothing in terms of accuracy and protection. You can offer your account holders the same level of protection and security as larger, more sophisticated competitors at a fraction of the cost.
- **Better ability to navigate financial downturns** – When the economy takes a downward turn, financial crime increases. During the 2008 financial crisis, for example, financial fraud increased 75 – 100 percent, according to the FBI.[20] Machine learning can keep pace with an increased influx of information and activity. Without a machine learning-enabled solution that continues to refine itself and advance, FIs would need to ramp up staffing exponentially to meet the increased threat in direct opposition to what is strategically sound during financial headwinds.

20 "Online fraud jumps 87.5% in < a year during economic downturn". Fiverity.

- **Focus on more strategic initiatives and customer/member experience** – Financial institution IT executives and staff have more on their plates than ever. The increasing occurrence of digital workspaces, hybrid work environments, virtualization and increased consumer demand for digital banking—in addition to increased threats from fraudsters—make even the smallest interruption a big deal. Increasingly, concerns over financial crime—and more importantly, how the institution is positioned to respond—are moving upstream to the C-suite and the board room. Concerns over financial losses, consumer protections and reputational damage are potentially big-dollar problems that IT execs must be prepared to address. Leveraging ML-enabled fraud prevention frees up IT resources to focus on delivering even more value for internal stakeholders and account holders alike.

Machine Learning-Enabled Fraud and Compliance from Effectiv: Scalable, Turnkey, Cost-effective and Accurate

Effectiv's turnkey, customizable application and onboarding fraud detection and compliance automation platform helps community banks and credit unions stop fraud at the source while minimizing friction for legitimate applicants because it's built with ML capabilities that help eliminate false-positives—at a fraction of the cost and time to implement as expensive enterprise solutions.

Where enterprise solutions can take 6 to 12 months to implement and fine-tune, Effectiv's platform comes already integrated with trusted third-party data intelligence providers and can be deployed out of the box with built-in rules or customized so rules can be added, deleted or adjusted based on your institution's unique risk profile and tolerances. Better still, customizations are as easy as drag and drop and don't require any intervention from IT staff or programmers, further lowering the total cost to own and maintain the solution.

And the financial benefits extend beyond bottom line efficiencies and mitigated fraud losses. Financial institutions can heavily impact top-line revenues by eliminating false positives that risk abandonment from legitimate account holders. Remember that account application abandonment rate? Digital consumers have a low tolerance for online transactions that take longer than expected or do not flow end-to-end uninterrupted. Just one car loan application that is falsely flagged or rejected can risk thousands of dollars in losses. On the other hand, failing to identify potential identity fraudsters can also have catastrophic financial consequences. The Effectiv platform is an elegant solution that gives community banks and credit unions the best of both worlds—stop fraud in its tracks while enabling business continuity, all while reducing costs and increasing revenues at an affordable price point.

The Effectiv platform also protects in real-time across all channels wherever fraudsters attempt to strike: new account applications, loan applications, credit card transactions, BNPL and P2P payments. This simple single solution provides full coverage and protection.

Digital change happens at the speed of light and fraudsters move nearly as quickly to exploit vulnerabilities and gaps in fraud prevention capabilities. Machine learning-enabled fraud detection and prevention finally puts community banks and credit unions on similar footing with big bank counterparts for offering protection and peace if mind to banking consumers—as well as mitigating the financial risks associated with identity fraud.

Effectiv's platform offers a sensible, cost-effective and elegant way for FIs to protect account holders and build long, loyal relationships from the very first impression.