NICE · ACTIMIZE

Aité

Report

SECURING DIGITAL ACCELERATION:

THE COMMUNITY BANK AND CREDIT UNION IMPERATIVE

Xceed

Aité PARTNER. ADVISOR. CATALYST.

Securing Digital Acceleration: The Community Bank and Credit Union Imperative

APRIL 2021

Prepared for:

NICE · ACTIMIZE

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Securing Digital Acceleration: The Community Bank and Credit Union Imperative, commissioned by NICE Actimize and produced by Aite Group, examines the importance of delivering seamless, yet secure digital experiences and faster payments options, and how NICE Actimize's Xceed solution can help community banks and credit unions execute on that very critical mandate. For all financial institutions (FIs), a digital-first strategy is now a critical imperative for not only new customer acquisition but also ongoing customer satisfaction. But digital acceleration introduces vulnerabilities for increased fraud, money laundering, and other illicit activities. Those community banks and credit unions that are successful in securing digital acceleration will set themselves apart from their competition and flourish.

Key takeaways from the white paper include the following:

- Traditional payment mechanisms have often been slow, unpredictable, and at times, expensive. Consumers and businesses expect faster and more economical alternatives. For today's consumers, their always-on and always-connected mindset demands quick and easy experiences. For businesses, faster payments can advance business goals and financial strategies.

- The U.S. is moving to faster payments along four tracks: the well-known same-day automated clearing house (ACH) transaction; Zelle, a near-real-time person-to-person (P2P) option; the Real Time Payments (RTP) system from The Clearing House with real-time settlement; and FedNow from the Federal Reserve, slated to go live in 2023 or 2024.

- Faster payments demand is accelerating in many unanticipated ways and niches. Previously, P2P services were mainly used for splitting dinner bills, then advanced to dividing rent. Soon, P2P services will be about paying merchants—maybe even using cryptocurrency. To keep pace with larger FIs, fully digital de novo banks, and fintech companies and stay relevant in the digital era, many community banks and credit unions must speed up their adoption of faster payments rails.

- FIs are experiencing competition from fintech provider offerings such as Venmo and Square Cash. But for community banks and credit unions, they must keep their independence from larger banks, which are owning these real-time payment networks. Although it is still unclear which real-time payment system will become the dominant option for consumers and businesses, community banks and credit unions recognize the intensifying competition landscape, and they are gradually migrating to faster payments.

- The COVID-19 pandemic fast-tracked digital acceleration. Use of remote and mobile banking services expanded dramatically. Even long-time holdouts for traditional in-person banking experiences sought digital, online, and electronic channels.

- Mobile fraud has been steadily on the rise, compounded with massive data breaches. Faster and interconnected payments systems and more digital and online platform users expand the vulnerabilities for fraudsters. Real-time payments are

unfortunately at higher risks of fraud. For instance, a primary feature across Zelle, RTP, and FedNow services is the convenience; registration only requires a mobile phone number. Yet, that feature elevates fraud risk as organized criminal networks can easily acquire stolen phone numbers from the dark web. To effectively interdict pre-transaction authorization, FIs need artificial intelligence (AI)-driven real-time behavioral analytics fraud detection.

- Through social engineering, many individual consumers can be "scammed" to make real-time payments to fraudsters and their illegitimate accounts. These are often referred to as "authorized push payment frauds." Community banks and credit unions must protect their customers and members from real-time digital banking fraud. They must perform continuous Know Your Customer (KYC)/customer due diligence (CDD) and real-time transaction risk analysis, all without disrupting the end-user experience. In another words, community banks and credit unions must conduct real-time digital-entity KYC, identify unusual or suspicious digital behaviors before transaction processing, and interdict in real time. Operating detection rules at the time of transaction processing will be too late, as real-time payments are irrevocable, and the money will be already gone.
- NICE Actimize's Xceed solution provides a fully integrated fraud and AML (FRAML) platform for small and midsize financial organizations. By integrating an AI-first design for real-time fraud intervention and continuous data intelligence in a cloud-native platform, Xceed is a modern FRAML solution enabling "friction-right" financial crime risk management. Moreover, NICE Actimize's deep technology integration with Zelle and RTP, along with its partnership with the Federal Reserve Fraud Classifier model, facilitates the labeling of authorized payment fraud and thus more efficient detection.
- Since 2006, Star One Credit Union, a California-based credit union, has benefited immensely from Xceed's omnichannel real-time fraud detection and intervention solution. Through its evolution from online and mobile banking fraud detection to same-day ACH, real-time wire fraud detection, and real-time P2P Zelle fraud intervention, Xceed has enabled Star One to deliver superior, yet secure, products and services to its members.

INTRODUCTION

Over the last few years, the ways consumers and businesses transact every day have evolved considerably. They are increasingly adopting faster payments and expecting more digital experiences. For FIs, a digital-first strategy is now a critical imperative for not only new customer acquisition but also existing customer satisfaction and loyalty. The COVID-19 pandemic fast-tracked this already accelerating shift. Millions of consumers, particularly those not previously engaged in digital channel activity, were thrust into increased online and mobile banking use. Yet, digital acceleration elevates vulnerabilities for fraud, money laundering, and other illicit activity.

Facing strong competition from larger commercial FIs, fully digital de novo banks, and fintech companies, community banks and credit unions must offer a healthy mix of digital banking channels, friction-right customer experiences, and real-time payment options. But, as community banks and credit unions further embark on their digital acceleration journey, they must take the appropriate steps in fighting crime and protecting the end-to-end customer life cycle.

This white paper examines the importance of delivering seamless, yet highly secure digital experiences and faster payments options, and how NICE Actimize's Xceed solution can support community banks and credit unions on that very critical mandate. Those community banks and credit unions that are successful will set themselves apart from their competition and flourish. Those that do not deliver on those very key mandates will lose customer trust, and ultimately their business, to those firms that do.

METHODOLOGY

The research supporting this white paper is largely based on ongoing Aite Group interviews with executives and financial crime risk practitioners at FIs, including Star One Credit Union which shared its experiences with the Xceed solution. It is also informed by multiple surveys conducted by Aite Group: 30 financial services professionals at Aite Group's September 2019 Financial Crime Forum, 47 fraud executives from 30 financial services firms at its September 2020 Financial Crime Forum, 117 community banks and credit unions in Q2 2020, and 8,653 U.S. consumers in December 2020.

The consumer survey data have an approximately three points margin of error at the 99% confidence level, and the bank study data have an eight-point margin of error at the 95% level of confidence. The findings from the survey among fraud executives can be considered a directional indication of market conditions. Statistical tests of significance among groups, where shown, were conducted at the 99% level of confidence. In addition, research examined how the COVID-19 pandemic influenced many consumers to change ingrained banking behaviors.

EMBRACING FASTER PAYMENTS

Traditional payment mechanisms have often been slow, unpredictable, and at times, expensive. Consumers and businesses are now expecting faster and more economical payments alternatives. For today's individual consumers, their always-on and always-connected mindset demands quick and easy experiences. They have become accustomed to the instant nature of products like Venmo, Square Cash, and Zelle. Consumer demand for P2P payment options is accelerating in many new and unanticipated ways. Initially used to split dinner bills, P2P services are now helping consumers split rent and other larger items. Consumers will soon adopt P2P options to pay merchants—maybe even with cryptocurrency. For businesses, faster payments can advance business goals and financial strategies, and can create differentiation in the market.

Faster payments have been around for years. For example, wire transfers provide immediate electronic fund transfers across FIs around the world. Although frequently used, wire transfers are expensive and rarely used by individual consumers. Conversely, same-day ACH transactions offer a lower price point. Yet, settlement times are not immediate, and they are frequently restricted. Remittance information travels separately from the payment itself. With recent technology advancements, easier, more efficient, and at times, cheaper instant payment mechanisms are emerging, and they are becoming available to individual consumers and businesses but only as long as their FI adopts them.

Table A illustrates several U.S. real-time payment channel options that FIs can provide to their customers. It is still unclear which real-time payment system will become the dominant option for individual consumers and businesses.

Table A: U.S. Real-Time Payment Channel Options

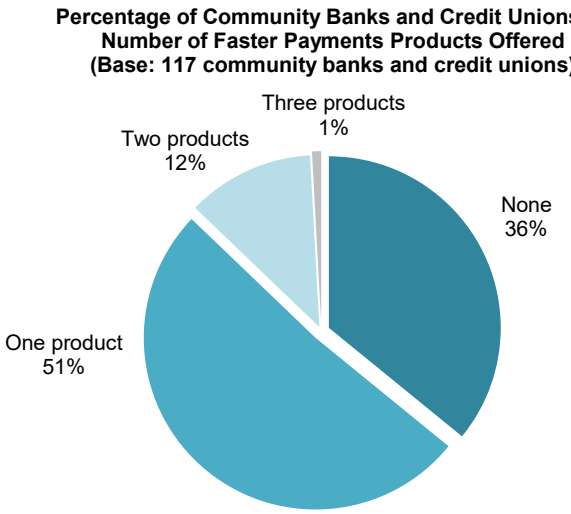
Option	Description
Zelle	As a privately owned U.S.-based digital payment network, Zelle facilitates real-time low-value P2P payments between U.S. demand deposit accounts (DDAs). Through a partnership with Mastercard and Visa, Zelle reaches 97% of DDAs across the U.S. But Zelle does not facilitate real-time settlement.
RTP	Owned by The Clearing House, a private financial services company owned by 24 of the largest U.S. commercial banks, RTP is a payments network that facilitates real-time interbank settlement for high-value payments. Reaching more than half of U.S. DDAs, RTP offers enhanced speed, security, and payments messaging. Although best-suited for business-to-business payments, the RTP network can be used for low-value retail payments.
FedNow	Currently being developed by the Federal Reserve, FedNow is expected to be a new real-time payment system for clearing and settling of real-time low- and high-value payments. FedNow is anticipated to go live in 2023 or 2024.

Source: Aite Group

INCREASING FASTER PAYMENTS ADOPTION

To keep pace with larger FIs, fully digital de novo banks, and fintech companies and stay relevant in the digital era, many community banks and credit unions are gradually migrating to faster payments, recognizing their growing importance to individual and corporate customers. As illustrated in Figure 1, 64% of today's community banks and credit unions now offer connectivity to at least one faster payments rail, with about 13% offering two or more. Given the existing links to ACH rails, same-day ACH connectivity is currently the most prevalent. Most community banks and credit unions have not yet implemented Zelle or RTP. Although many are investing in faster payments, more than one-third have yet to adopt them.

Figure 1: Community Banks and Credit Unions With Faster Payments Capabilities



Source: Aite Group survey of 117 community banks and credit unions, Q2 2020

However, existing customers at community banks and credit unions are seeking increasing connectivity to faster payments, particularly Zelle and same-day ACH. Demand will only grow as individual consumers and businesses have positive experiences with these payments rails. Without offering more digital banking options and faster payments alternatives, community banks and credit unions will be challenged to attract new clients, keep existing ones happy, and grow deposits and revenue. Poor, slow, and clunky digital and payment experiences will only erode customer satisfaction. Hence, it is no surprise that over 80% of community banks and credit unions indicate that adopting at least one additional faster payments rail is an organizational priority (Figure 2).

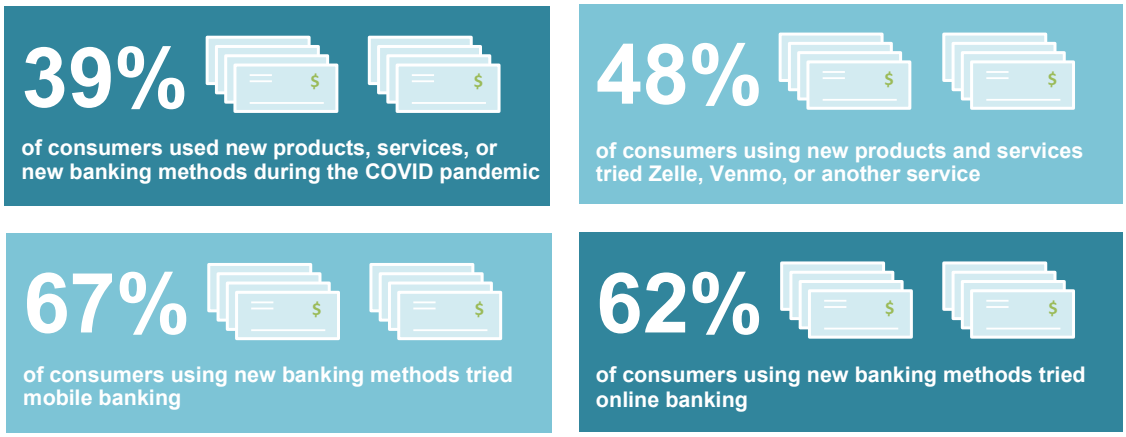
Figure 2: Rising Faster Payments Demand

Source: Aite Group survey of 117 community banks and credit unions, Q2 2020

DIGITAL NEWBIES AND THE COVID-19 PANDEMIC EFFECT

The COVID-19 pandemic turned the world upside down. It changed how global society lives and works—for many, permanently. Often expecting no unjustified delays, individual consumers gravitated to more digital behaviors. Use of remote and mobile banking services expanded dramatically. Even long-time holdouts for traditional in-person banking experiences sought digital, online, and electronic channels. According to a recent Aite Group consumer survey, almost 40% of consumers used new digital products, services, or banking methods during the COVID-19 pandemic. Of those who used new products and services, more than three of every five individuals used mobile banking (67%) and online banking (62%). Of those who used new methods of banking, 48% tried Zelle, Venmo, or another money transfer service. Not only are most of these digital newbies (more than three out of every four) pleased with their experiences with these new products and services, but they are also likely to continue using them going forward (Figure 3).

Figure 3: The COVID-19 Pandemic Effect



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

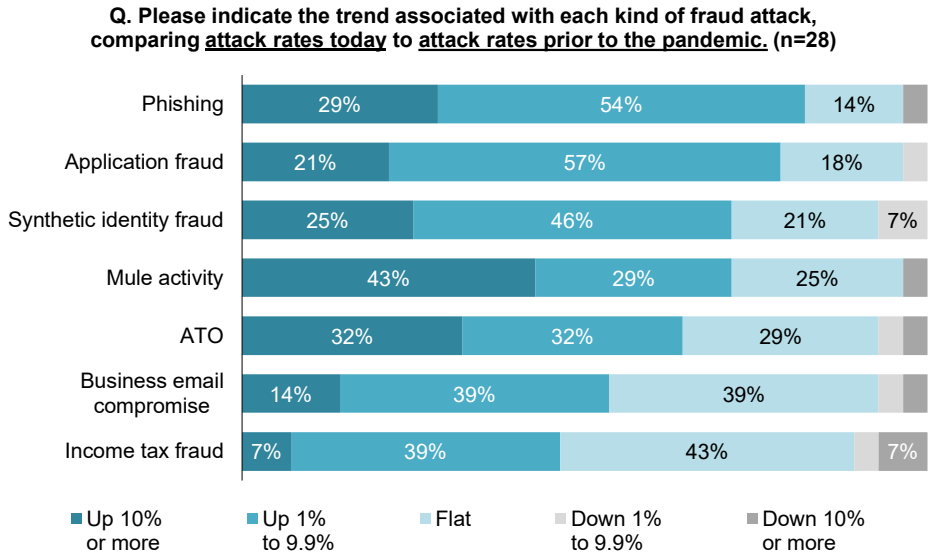
DIGITAL ACCELERATION: ESCALATING CRIME

With the rise of faster payments, concerns about escalating financial crime threats are growing. Fraud and other illicit activity can and do happen across all banking channels and payment types. Yet, organized criminal networks are relentless in their war against the financial services industry. They seek new opportunities to exploit and launch more sophisticated and automated attack modes. Faster and interconnected payments systems and more digital and online platform use expand financial crime vulnerabilities. A recent Aite Group survey of fraud executives in September 2020 indicates that about 66% of FIs offering P2P options experienced higher fraud losses in 2020 compared to two years ago:

- Faster payments streams enable illicitly gotten funds to be moved more quickly and more frequently, and criminal activity to be hidden more easily.
- A primary feature across Zelle, RTP, and FedNow services is the convenience; registration requires only a mobile phone number. Yet, that feature elevates fraud risk, as organized criminal networks can easily acquire stolen phone numbers from the dark web.
- Through social engineering, many individual consumers can be scammed to make real-time payments to fraudsters and their illegitimate accounts; these are often referred to as “authorized push payment frauds.” As real-time payments are irrevocable, the money is frequently already gone by the time the customers or their FIs discover the illegitimate transfers.
- Expanded online and digital channel use expands the pool of potential victims. Digital newbies are more likely than most to be susceptible to social engineering, scams, and coercion, as they are less likely to practice sound security practices. Increasing digital adoption often triggers increased proliferation of stolen personally identifiable information.

Not surprisingly, the COVID-19 pandemic magnified financial crime risks, especially with the upticks of synthetics and identity theft. Social engineering and automated attacks surged as fraudsters embraced credential stuffing, phishing, smishing, and rogue applications. The hundreds of billions of dollars stolen from government stimulus programs elevated application fraud and mule activity, already a rising problem ignited by rampant data breaches. Moreover, the considerable shift in customer behavioral patterns further complicated ongoing financial crime prevention, detection, and investigation efforts (Figure 4).

Figure 4: Trends in Fraud Attack Methods in 2020 Versus the Pre-Pandemic Period



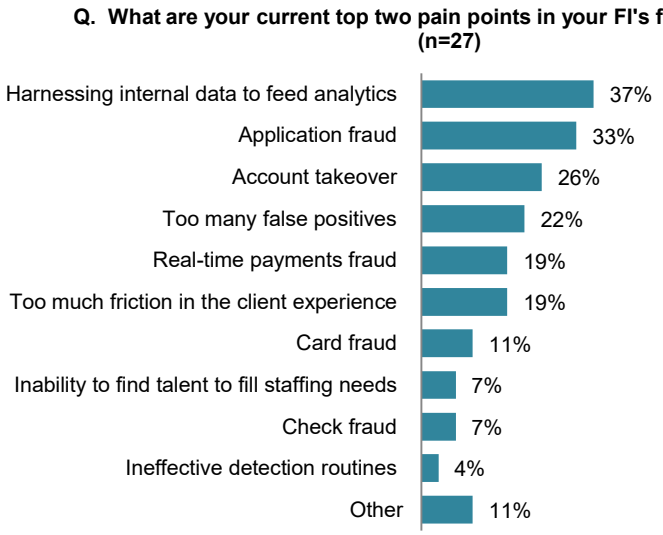
Source: Aite Group's survey of 47 financial services fraud executives, September 2020

FINANCIAL CRIME OPERATIONAL CHALLENGES

For decades, billions of dollars have been spent on people, processes, and technology in fighting financial crime and achieving regulatory compliance. Even with this enormous investment, financial organizations run into operational pain points, making effective and efficient prevention and detection an ongoing struggle (Figure 5):

- Loosely connected systems have left many with fragmented, incomplete, and, at times, inaccurate data. Critical customer and transaction information resides in unstructured and other difficult to access and ingest formats.
- Lack of holistic views of customers and their risk profiles obstruct customer experiences as well as effective financial crime monitoring. Many regulator enforcement actions trace back to poor customer risk profiling and surveillance practices.
- Heavy reliance of rules-based monitoring, especially in AML operations, generates too many false positive alerts requiring needless reviews and increased staffing. Ineffective detection can delay customer onboarding and processing of transaction requests, frustrating customers and back-office staff. Good applicants often take their business elsewhere.

Figure 5: Top Pain Points in Fraud Operations



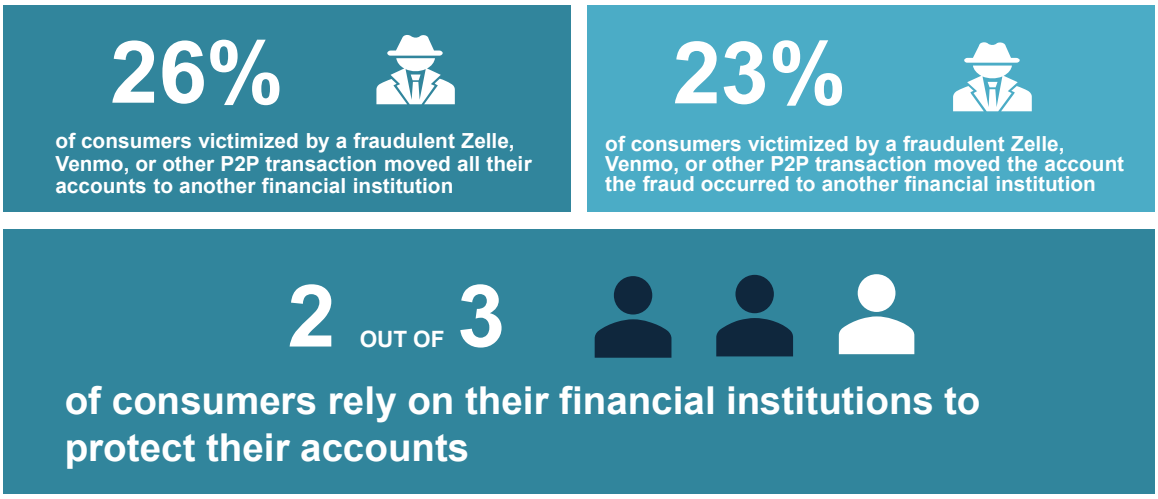
Source: Aite Group survey of 30 financial fraud professionals, September2019

THE FINANCIAL CRIME RISK MANAGEMENT VERSUS CLIENT EXPERIENCE DILEMMA

Community banks and credit unions face a tricky dilemma. They must figure out how to stop financial crime without impeding new customer onboarding times, slowing down transactions, and generally injecting too much friction into the end-to-end customer life cycle:

- Customers desire quick and easy experiences. They want greater access to mobile and online channels and near-real-time, if not real-time, payments. Faced with increased competition, community banks and credit unions are under great pressure to deliver on compounding customer demand for convenience and ease of use.
- But security and fraud prevention are important to consumers and businesses, too. In a recent Aite Group study, about two of every three individual consumers surveyed indicated they depend on their FI to protect them and their accounts. Yet, managing these expectations are particularly challenging with faster payments and higher digital use. Those victimized by fraud in a Zelle or other P2P transfer will often switch accounts to other FIs. As such, it becomes critical for financial organizations to strengthen security practices and detection models (Figure 6).
- Regulators are pushing for more effective financial crime prevention as they become increasingly concerned by escalating crime and its horrific consequences to society. Moreover, with the massive stimulus fraud during the COVID-19 pandemic, some are concerned that regulators could question whether FIs did enough to stop it. FIs are under intensifying pressure to ensure they are meeting both the letter and spirit of the law; they are looking for innovative ways to ensure that they are compliant.

Figure 6: Impact of Fraud on Customers



Source: Aite Group's online survey of 8,653 U.S. consumers, December 2020

Successfully balancing these two contrasting expectations is no simple task. It requires an organizational understanding and commitment that friction is not always bad, nor should it always be avoided. Whereas good customers should not be encumbered with unnecessary friction, bad actors should and must receive heightened scrutiny. This delicate balance can be achieved by effectively harnessing data and cultivating superior contextual and risk-based insights. Sharper intelligence can distinguish good customers from bad ones, trigger risk-relevant friction across the customer life cycle, and drive consistent decisioning and superior outcomes.

FINANCIAL CRIME CONVERGENCE

Historically, fraud and AML have been distinct operational units with unique processes and systems. However, a segmented approach can often lead to incomplete financial crime risk identification and understanding, driving down effectiveness and operational efficiency. When fraud and AML teams work in silos, investigation work can be fragmented, duplicated, and slow.

As financial crime becomes more diverse, complex, and automated, convergence accompanied by innovation can be an essential tactic in disrupting financial crime. More integrated and technology-driven approaches can facilitate threat identification, detection, and intervention, while driving up operational efficiency and uplifting the customer experience:

- Increased intelligence sharing can cultivate more proactive and preventive intelligence. Elevated multidimensional customer risk views can be built. Hidden, unknown, and emerging risks can be spotted and addressed more quickly.
- More cohesive and aligned financial crime strategies can identify and eliminate redundancies, streamline systems and processes, and optimize resource utilization.

Those community banks and credit unions that can better connect fraud and AML will more responsively adapt to a changing landscape. Those organizations will better tackle financial crime, achieve regulatory compliance, deliver better customer experiences, and increase customer trust and loyalty.

THE TECHNOLOGY IMPERATIVE

A faster business landscape and escalating crime require real-time and elevated intelligence. Innovation can support faster, smarter, and more efficient detection and intervention as well as positively impact the end-to-end customer life cycle. Today's emerging technologies are facilitating data gathering and analysis and eliciting greater insights on customer risk. Community banks and credit unions can become more agile and responsive to evolving and emerging threats. Augmenting human decision-making, advanced analytics can perform continuous KYC/CDD and can sharpen real-time transaction risk analysis. Truly unusual and abnormal behavior can be immediately discovered, fraud and AML operations can be streamlined, and the customer experience can be optimized. Table B presents specific advancements in technology that can unlock the potential within data, dramatically uplift current detection schemas, and build sharper intelligence.

Table B: Ongoing Technology Advancements

Technology advancement	Benefits and AML implications
Entity resolution	Through standardizing, enriching, and consolidating disparate information, entity resolution tools can construct more holistic and multidimensional profiles of customers and their risk. By unlocking the power within fragmented and diverse internal and external data sets, entity resolution can produce richer and more consistent customer views and drive greater operational efficiencies.
Network and link analytics	Network and link analytics can uncover relationships and connections among parties and transactions and graphically display them in user-friendly and easily digestible diagrams. Network and graph analytics can deliver enhanced context—honing financial crime detection and investigation.
Advanced analytics	Able to process large data volume, advanced analytics and machine learning can detect anomalies in customer behavior and unknown and emerging risks, while minimizing false positive alerts. Machine learning augments human decision-making as opposed to replacing it. Supervised machine learning models leverage previously identified suspect activity as training data. Conversely, unsupervised machine learning models identify clusters, patterns, and groups, and detect anomalies and outliers using their differences to those identified groupings.
Cloud deployments	By enabling increased scalability, IT efficiencies, and quicker processing speeds, cloud-based deployments can yield more integrated, modern, and dynamic financial crime technology ecosystems. This is especially relevant to smaller firms that may not have extensive and scalable infrastructures. Cloud technology enables greater agility and adaptability, especially to changing circumstances, and optimized system utilization, maintenance, and upkeep.
Upgraded case management	Case management has been an essential financial crime-fighting tool as a single platform to investigate alerts and record all decisions. Upgraded case management platforms can enable community banks and credit unions to tackle their unique challenges more effectively and efficiently. Updated technology delivers superior user experiences, automated intelligence, and enterprise customer risk views.

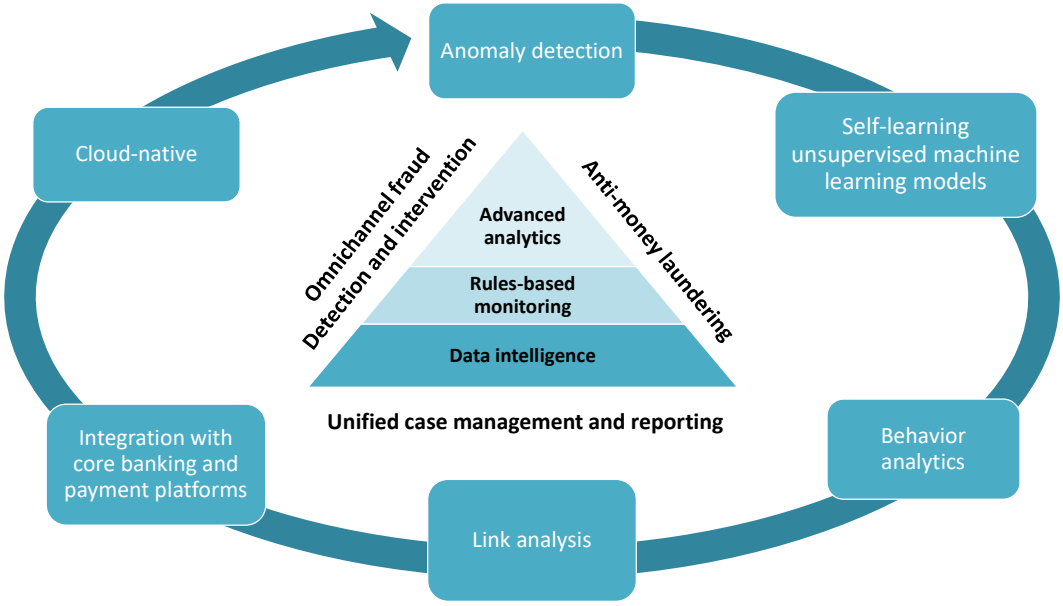
Source: Aite Group

NICE ACTIMIZE'S XCEED SOLUTION: BRINGING DATA INTELLIGENCE AND ANALYTICS TO THE FOREFRONT

NICE Actimize's Xceed solution provides a fully integrated FRAML platform for small and midsize financial organizations. By integrating AI, data intelligence, and advanced analytics within a unified cloud platform, Xceed is a modernized financial crime risk management ecosystem with quick time to value (Figure 7):

- Xceed offers out-of-the-box unsupervised models with real-time fraud detection and intervention across multiple digital banking and payment channel use cases. It protects against online and mobile banking account takeover as well as wire, same-day ACH, account-to-account, P2P, check, and card fraud.
- Xceed's self-learning behavioral analytics and anomaly detection models do not require labeled data to train them. As Xceed is connected to over a hundred core banking and payment processors platforms, data wrangling is substantially minimized. Moreover, NICE Actimize's deep technology integration with Zelle and RTP, and its partnership with the Federal Reserve Fraud Classifier model, facilitates the labeling of authorized payment fraud and supports more efficient fraud detection.
- Calibrated across hundreds of FIs, Xceed automatically creates and maintains behavioral profiles against which individual customer activity and events are uniquely risk scored and assessed. AI-generated risk scores help to sharpen financial crime detection and lower false positive alerts as well as prioritize alert management and optimize resource utilization.
- Xceed creates unique and holistic identities for every customer constructed upon and enriched by behavioral, digital, and biometric data. Transforming online and mobile banking activity as well as device, geolocation, and IP information into contextual intelligence drives more informed risk-based decisioning and higher-quality outcomes. As such, Xceed tracks in real time, from first touch to last touch, all digital entities representing the user and enables real-time interdiction.
- Offering a comprehensive AML product suite, Xceed enables financial organizations to also meet their AML needs across the customer life cycle—on-boarding and KYC/CDD obligations, ongoing transaction monitoring, watchlist screening, and regulatory reporting. Xceed's AML module blends rules-based monitoring with advanced analytics.
- Xceed's unified all-in-one case management platform connects its fraud and AML modules, facilitating efficient investigations and cross-functional intelligence sharing. Offering ample out-of-the-box functionality, Xceed can expedite the end-to-end financial crime investigation process. Relationships and linkages across parties and transactions are automatically discovered and displayed, and case details are auto-populated for suspicious activity reporting and other regulatory filings.

Figure 7: The Xceed Solution—A Modern Financial Crime Risk Management Ecosystem



Source: Aite Group

Xceed enables friction-right financial crime risk and customer management. By risk scoring all events in real time and immediately uncovering unusual and anomalous activity, financial organizations can dynamically adapt and respond to new and emerging financial crime risks without disrupting the experience of good customers. Integrated across internal systems, Xceed promotes immediate interdiction to prevent sham accounts, account takeovers, and other fraudulent or suspect events.

THE STAR ONE CREDIT UNION EXPERIENCE: AN INSIDE LOOK

Since 2006, Star One Credit Union, a California-based credit union with over US$10 billion in assets and 120,000 members, has benefited immensely from deploying Xceed's omnichannel fraud real-time detection and intervention solution. Recognizing the importance of the customer experience, Star One has leveraged Xceed in delivering superior, yet secure products and services. For nearly 15 years, Xceed furthered Star One's core values of convenience, service, and trust.

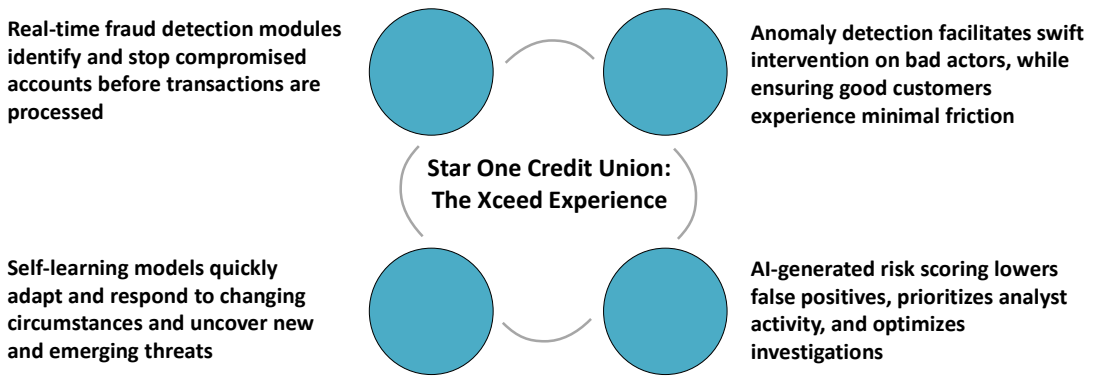
Pursuing an aggressive business strategy, Star One has launched numerous digital banking experiences over the past few years. And to further attract a younger demographic, the credit union has accelerated its digital and instant payments channel adoption. Zelle, same-day ACH, and other faster payments modes have been critical for its continued growth. Yet, building and maintaining member trust has been equally vital. Acknowledging faster payments and online and digital banking magnify its fraud risk, Star One is committed to appropriately securing and protecting its members while not disrupting the overall customer experience.

XCEED AND ITS BENEFITS:

Embraced as part of Star One's internal DNA, Xceed has enabled the credit union to compete with much larger financial organizations, deliver on its member-centric vision, and generate high member satisfactions scores. With Xceed's AI-first approach, Star One is successfully advancing its digital acceleration strategy while protecting the organization and its members:

- Concerned with its members being susceptible to social engineering and malware attacks, Star One uses Xceed's real-time fraud detection modules to identify and stop compromised accounts before transactions are processed. For example, behavioral analytics and anomaly detection models instantly spot suspect or unusual logins, IP addresses, or password changes.
- Through its self-learning models, Xceed helps Star One quickly adapt and respond to changing circumstances and uncover new and emerging threats, especially significant during the COVID-19 pandemic.
- With simplified data ingestion, Xceed easily consumes vast amounts of data from different sources, enabling accurate and immediate detection.
- Through Xceed, Star One is ensuring that good customers experience minimal friction, while swift and appropriate intervention is taken on identified fraudsters and other bad actors.
- Xceed's AI-generated risk scoring lowers false positives, prioritizes analyst activity, and optimizes investigations. This facilitates decisioning, expands risk coverage, and drives up operational efficiency. This has been especially invaluable as Star One does not staff a large fraud investigations unit.
- Xceed's P2P Zelle solution helped Star One become Zelle-certified. Once a user opens a Zelle app, Xceed immediately starts monitoring for fraud risk, enabling intervention before fund disbursement (Figure 8).

Figure 8: Star One Credit Union: The Xceed Experience



Source: Aite Group

With the COVID-19 pandemic, Star One experienced reduced branch activity, higher numbers of member logins, and increased digital platform use and faster payments. Yet, the COVID-19 pandemic did not significantly impact its fraud losses. Star One attributes much of this accomplishment to Xceed and its agility in digesting and synthesizing vast amounts of data and adapting quickly to changes in member behavior. By prioritizing higher-risk events, Xceed's AI-generated risk scoring helped Star One and its fraud teams manage the increased member activity.

Moving forward, Star One is extending Xceed to other use cases across the organization. Xceed will facilitate the credit union's pending initiative to consolidate its diverse network of internal systems and disparate banking channels. And Star One is deploying Xceed to its AML operations in a broader strategy of bringing its financial crime platforms under a single vendor ecosystem.

CONCLUSION

Securing faster payments and digital banking channels and solidifying customer trust often mandate increased innovation. Successful adoption can become a competitive advantage for community banks and credit unions. By leveraging new and emerging technologies, community banks and credit unions can more easily extract valuable and predictive data intelligence, minimize customer friction, and more effectively and efficiently tackle financial crime risk. Resources can be extended and optimized, detection accuracy can be sharpened, and more agile responses to new and emerging threats can be cultivated.

As you embark on your transformation journey in securing digital acceleration, here are a few things to keep in mind:

- **Define your needs and the key drivers for increased technology investment.** Understand your organization and its key financial crime risks. Know your organization's current and future strategic goals as well as its near-term product roadmap. Is it adopting faster payments? Identify the available data and its sources and differing formats. It is also critical that you pinpoint the available budget and resources as well as the expected timeline.

- **Scrutinize the efficacy of your existing financial crime risk solutions.** Are they producing actionable intelligence and swiftly and accurately capturing illicit activity? Are there too many false positives? Are they keeping up with the accelerating pace of business, faster payments, and customer demands? Investment in financial crime technology can expedite customer experiences and help to accelerate business growth.

- **Develop an expertise in new-generation technology and the evolving financial crime technology market.** Today's leading platforms can effectively ingest, harness, and enrich a growing volume of data as well as uncover anomalous and suspect behavior, and detect previously unknown relationships, networks, and connections. Superior solutions offer dynamic out-of-the-box rules, machine learning models, expansive use cases, and real-time risk scoring and monitoring. Remember the impact on operations and customer experiences.

- **Identify a vendor that can become a long-term strategic partner.** Leading vendors possess substantial financial crime and technology expertise. They are also deeply committed to research and development and to integrating customer feedback. Before making a long-term investment, many organizations have found it beneficial to evaluate vendors and their solutions through smaller proofs of concept.

- **As you build, start small and take your time.** Bring in as much data as you can. Methodically introduce advanced analytics in detection, investigation, and intervention. Consider a single financial crime technology ecosystem.

Successful technology adoption will elevate the customer experience, protect your organization and your clients, and drive up resource utilization and operational efficiency.

ABOUT NICE ACTIMIZE

NICE Actimize is a provider of financial crime, risk, and compliance solutions for regional and global financial institutions, as well as government regulators. NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers' and investors' assets by identifying financial crime, preventing fraud, and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, AML detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence, and insider trading. NICE Actimize also offers cloud-based machine learning analytics optimization and development solutions, which leverage collective intelligence to proactively optimize analytics for members.

CONTACT

For more information, please go to www.niceactimize.com, @NICE_Actimize, or Nasdaq: NICE.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

Charles Subrt
+1.617.338.6037
csubrt@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com