NICE
ACTIMIZE

Insights Article

Customer Experience and the Emotional Toll of Fraud

By Glenn Fratangelo

Introduction

When customers experience fraud, no matter where or how it occurs, their future behaviors are changed. The fraud threat landscape is evolving, and the competition within financial services is broadening. As a result, financial institutions must seize opportunities to become a trusted resource for their customers and optimize the customer experience (CX). This experience-driven age requires faster fraud prevention - predicting fraud before it happens and safeguarding the customer journey across every touchpoint. However, establishing competitive differentiation while elevating the customer experience isn't an easy task.

According to a recent Javelin Strategy & Research study, banks face many challenges, including declining customer loyalty, an emergent fintech market, and eCommerce platforms that continuously inch towards providing competing financial services. Ensuring a positive CX makes the difference in whether FIs can keep their customers or lose them to the competition.

CX and Payments Modernization

Momentum in payments modernization has yet to let up since the onset of the pandemic. While 2020 was undoubtedly the year of transformation within the payments ecosystem, disruption continues well into 2022. Consumers have wholeheartedly embraced the convenience and ease of digital banking and faster payments. The changing nature of their behaviors and habits, along with the unprecedented digital acceleration that has defined the course of the pandemic, has led to the emergence of new and innovative payments. As a result, the era of payments innovation has arrived and focused on an experience-centric environment in which typical consumer engagement practices are being transformed into value-driven experiences.

There are many developments in the digital payments ecosystem that are driving attention to improving CX. Instant payments and e-money are gaining popularity and are anticipated to comprise over 25% of global non-cash transactions by 2025, increasing by 14.5% from 2020. Gen-Z favored methods, like Buy Now, Pay Later (BNPL), is also gaining traction. A Capgemini Voice of the Customer survey revealed that 20% of respondents are currently using BNPL solutions, which is predicted to increase to 60% over the next two years. According to the same survey, 45% of consumers use mobile wallets to make payments, a jump from 23% in 2020. Mainstream cryptocurrency payments adoption is rising, and it comes with its own set of customer experience-related concerns.

Forward-looking financial institutions seek to capitalize on the evolving payments ecosystem by using the digital payments trajectory to enable improved CX via safe, seamless transaction experiences with more intelligent fraud protection. Unfortunately, consumers use mediums that are easier to defraud, and with money moving faster, the risk accelerates. In addition, with heightened concerns on identity theft and secure monitoring of phone numbers and email addresses, consumers expect that every interaction and transaction is based on a pillar of trust with their financial institution.

> "Criminals have increased their efforts with higher quality, larger volumes, and automated attacks. FIs need to step up and improve automation in response to tracking and preventing as many fraudulent attacks as possible. To do this, we need to have a holistic customer view and focus on data quality," said Terje Aleksander Fjeldvær, SVP - Head of Financial Cyber Crime Center, DNB, Norway's largest financial group.

CX at Account Application

Financial institutions are working to strike the right balance between risk and CX and allow access to accounts quickly, safely, and in a digital-first way that won't slow down customers who might have thin financial files.

> **According to Aite, there's eight times more fraud associated with digital account opening, and keeping the door open for legitimate customers while stopping fraudsters in their tracks is a significant challenge.**

In addition, FIs have already seen that friction at the point of application undoubtedly leads to higher abandonment rates, and conversely, bad actors exploit less friction. So how are financial institutions successfully balancing risk and revenue? Fortunately, enterprise fraud technology has advanced to the point where financial institutions can achieve high accuracy, passive verification to enable safe and fast account onboarding.

Identity verification is not stagnant and it doesn't stop at onboarding. The prevalence of sophisticated synthetic identity fraud (SIF) requires financial institutions to continually monitor account holders for risk signals indicative of SIF. The value of account opening data and continual identity monitoring is just not about stopping bad actors; it is about de-risking accounts earlier in the customer lifecycle to offer new products sooner to drive revenue growth rather than waiting for additional maturation.

Financial institutions have a prime responsibility to step in, provide support, and become that trusted resource because the outcome of that event will alter the customer's mindset. Additionally, it's not difficult for a customer to switch to a competitor bank, fintech, or emerging player, so preventing customer attrition is vital, especially given the expansion of the FI's competitive landscape.

Financial institutions must also establish customer relationships earlier; younger generations are experiencing life changes and addressing financial milestones, like car and home loans and investments. As a result, organizations are looking to start relationships early, build upon them, and grow alongside their customers as trusted partners.

Impact of Fraud on CX that Leads to Attrition

Victims of identity fraud are three times more likely to leave their primary financial institution (PFI) when they feel that their bank did not resolve their fraud issue. Customers depend on their primary financial institution to protect their identity and their assets from theft and fraud.

> **When a fraud event does happen, even if the FSO isn't at fault, customers are 31% more likely to leave the institution, according to the Javelin 2021 Identity Fraud Study Shifting Angles.**

There's a significant amount of compromised data that's stolen via phishing scams and social engineering, in addition to being purchased on the dark web. Data breaches and various scam tactics are all available to buy on the digital underground. Information that resides outside traditionally acknowledged personally identifiable information (PII), such as date-of-birth and social security numbers, is being targeted and used to steal identities and perpetrate fraud. Information such as passwords, email addresses, and mobile phone numbers are now increasingly vulnerable to criminals and fraudsters.

Cybercriminals constantly adjust their tactics, and a single negative experience can mean an entire transfer of all the products that a customer has at a financial institution. Therefore, FSOs must proactively detect and prevent fraud, reduce and attrition; improving CX directly impacts the organization's bottom line.

To put CX front and center, financial institutions must leverage the right tools and capabilities to proactively detect and prevent fraud and safeguard the customer journey. The role of fraud prevention and CX in the customer lifecycle to shifting fraud prevention from risk mitigation to business enabler will support those financial institutions which continuously pave a path forward for a superior CX.

To accomplish this, financial institutions must begin the journey to creating a holistic view of customer risk; this includes a singular platform for data, analytics, decisioning, and operations. To be an agile fraud fighter, a financial institution needs data agility and the ability to deliver seamlessly into its enterprise fraud management system to enrich fraud analytics and decisioning with greater accuracy to stop fraud in real-time. This applies to its disparate data sources and point solutions and the customer journey to connect data from the account application to the transaction monitoring.

Intelligent AI may sound redundant, but not all AI is intelligent. Intelligence is earned, not built, and as AI becomes commoditized, the value of the industry expertise and quantity of quality data built into intelligence will become increasingly valuable. For example, in detecting sophisticated identity fraud, financial institutions must rely on advanced machine learning applications that understand customer patterns and continuously learn, discover, and adapt to detect anomalous activity and prevent complex fraud attacks quickly. In addition, continuous monitoring of customer interaction builds trust through accurate, real-time, and holistic fraud detection and prevention.

The newest enterprise fraud management solutions driven by AI and cloud-driven platforms will allow data-driven adaptive intelligence to protect customers and enable financial institutions to thrive in this new economy. Accomplishing this reduces the emotional toll of fraud on customers and elevates their experiences – paving the way for new revenue-generating opportunities for financial institutions.

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, 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, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com