NUANCE

Customer engagement in an era of rising fraud

As regional banks transform customer engagement to deliver more simple, personal, self-service experiences, they must contend with a sharp rise in identity fraud.

Contents

The goal of the Nuance 2021 Regional Bank Customer Engagement, Authentication & Fraud Prevention Outlook survey was to understand the use and breadth of customer engagement channels, as well as the ways in which regional banks secure both digital and voice interactions.

As a result, convenience and trust have become strong differentiators in the banking industry and a competitive necessity for regional banks. Larger financial institutions and online-only banks continue to invest in diversifying and personalising customer engagements. These new-generation digital solutions offer customers the ability to communicate and transact with banks wherever and whenever they need via virtual assistants, live chat, and messaging apps, in addition to standard methods like phone calls, emails, and branch/ATM visits.

Another crucial consideration for regional banks is the security of their customers' interactions. Traditional authentication methods like PINs and passwords are viewed as insufficient to stem a growing increase in bank application fraud, account takeovers, and identity theft.

Losses from bank application fraud alone are expected to exceed $4.1 billion by 2023.[1]

To better understand these ongoing trends in customer engagement, authentication and security, Nuance sponsored a December 2020 survey of American Bankers Association (ABA) member banks. The goal of the Nuance 2021 Regional Bank Customer Engagement, Authentication & Fraud Prevention Outlook survey was to understand the use and breadth of customer engagement channels, as well as the ways in which both digital and voice interactions are secured. Nearly 500 ABA member banks, each with more than $1 billion in assets, provided the responses presented throughout this research paper.

Like customers everywhere, regional bank account holders seek frictionless experiences consistent with their other commercial transactions. In response, many regional banks have invested capital over the past five years to provide a variety of voice and digital self-service banking functions. These tools make it easier for customers to bank without visiting a local branch; consequently, customers have come to expect the convenience of banking remotely, whether by phone, website, or mobile app.

A growing need to invest in digital transformation

While many regional banks have introduced new customer engagement channels, the competitive milieu suggests they must set a higher standard. Further investments are needed to provide customers with more choices in selecting preferred channels and seamless experiences across these channels.

Other priorities for customers include the ability to access all their bank products, services and transactions in every channel and to enjoy personal and consistent experiences. By capturing, integrating and preserving customer interactions across all channels, banks can eliminate the frustrating need for customers to repeat information or reauthenticate themselves when switching from one channel to another.

In 2020, banks and credit unions collectively spent approximately $1.9 billion on new banking channels, representing a 6 percent increase from the prior year's expenditure. Spending is expected to increase to nearly $2.1 billion in 2021.[2] More than seven in ten banks (71%) said the key factor driving their investment decisions was "competitive reasons."

80% of customers are apt to switch to a competitor after just one bad digital experience, representing a substantial loss in market share (according to a 2020 study).[3] **The business consequences of not investing in these solutions can be dire.**

Online-only banks up the ante for regional banks

The Nuance Regional Bank survey illuminated why many large banks are investing in more sophisticated and diverse customer engagement solutions. A key factor is growing global competition from online-only banks, putting pressure on traditional brick-and-mortar banks in the U.S.

These nimble competitors are carving inroads into traditional financial institutions' depositor bases by offering frictionless banking solely through digital banking apps. As younger generations place less priority on in-person banking, the online banks' tech-driven platforms are gaining popularity.[4]

Even prior to the pandemic, many banks and credit unions were already shuttering brick-and-mortar branches: Since 2010, more than 9,000 bank branches have been closed.[5] According to Big Four consulting firm Deloitte's 2021 Banking and Markets Outlook, "This new wave of innovation (is) recasting the role of branches (and) accelerating digitisation in almost every sphere of banking."[6]

The Nuance Regional Bank survey affirmed this continued migration away from physical bank branches to support digital customer engagement.

Data from the research speaks volumes —

49% said their primary interest in offering digital banking solutions is reducing operating costs.

43% want to improve customer engagement and experiences.

37% include increasing cross-selling opportunities as a goal.

33% need to meet high customer demand.

Altogether, nearly 90% of the survey respondents cited the importance of digital customer engagement opportunities as "extremely important" or "important." Apprised of the survey findings, Tiffani Montez, a Senior Analyst at market research firm Aite Group specialising in financial institution digital customer engagement strategies, said that banks now understand that their customers are insisting upon digital banking experiences similar to the instant and seamless services they receive in other digital transactions.

Apprised of the survey findings, Tiffani Montez, a Senior Analyst at market research firm Aite Group specialising in financial institution digital customer engagement strategies, said that banks now understand that their customer are insisting upon digital banking experiences similar to the instant and seamless services they receive in other digital transactions.

The pandemic has fueled a rise in such transactions, from single mouse-click product orders to same-day delivery or curb-side product pickup. "Customer stickiness is always about ease, convenience and value," Montez explained. "One of the main reasons why a customer leaves a financial institution is a poor experience, and one of the key reasons they stay is the experiences with a bank's digital engagement solutions."

The need for consistent customer experiences

Survey respondents were also asked about the digital channels through which customers presently engage with the bank. More than seven in ten respondents (71%) communicate primarily through live chat. Other digital channels include virtual assistants/ chatbots (64%), email (55%), mobile apps (40%), social media (39%), and messaging channels like Facebook Messenger, WhatsApp, Apple Business Chat, Google Business Messaging (GBM) and other messaging apps (27%).

Montez expressed surprise that more banks were not further along in offering mobile banking apps to their customers. "The percentage seems quite low, since our research indicates that six in ten bank customers in the U.S. check their accounts an average of two times a week using a mobile application," she said. "We live in a mobile app society today."

Ways consumers communicate with enterprises —

* Like Facebook, Business Chat, Google Business Messaging (GBM) and other messaging apps.

She also considered the percentage of "live chat" engagements to be unusually high, "suggesting that customers using other digital options like mobile apps, virtual assistants and email were unable to find the solution to a problem they had expressed, requiring them to reach out to a human being for help, while staying in the digital channel."

In other words, customers are forced to engage a human being for assistance because their bank's digital channels do not serve their needs. Montez said this inconsistent experience may adversely affect customer retention.

"To make the entire digital engagement more consistent, banks need to capture customer interactions across all channels and integrate them with their back-end processes and workflows. The customer's varied interactions can then be carried forward, without having to re-authenticate the person and re-share information already provided."

— Tiffani Montez, a Senior Analyst, Aite Group

Freedom for customers to select the channel of their choice

Beyond delivering consistent channel experiences, regional banks also must consider the value of liberating customers to transact and communicate through the channel of their choice—not just for the customer's benefit but also for the bank's, Montez said.

"A bank can see how many times consumers bought a particular product offer like a refi or a home equity loan in a particular channel, giving them valuable information on where best to allocate sales and marketing spend," she explained. "The use of AI also can help a regional bank shape the automated responses provided by virtual and live chat / messaging service providers."

These varied considerations have become more important, in part due to the pandemic. Montez agreed that the pandemic's business impact on brick-and-mortar banking has accelerated the need to expand the customer engagement toolset.

44% of retail banking customers used their bank's mobile banking apps more frequently during 2020, according to the study by Deloitte.[7]

"The pandemic has forced many financial institutions to think more proactively about digital customer engagement, given its impact on in-person bank experiences, which have dramatically fallen," she said. "How customers interact with their bank accounts, in terms of moving money, paying bills and managing finances, is the value-add embedded in digital banking."

Regional banks must contend with a rising tide of fraud

As regional banks increase their investments in more sophisticated and diverse customer interactions, they must ensure that transactions are secure. Unfortunately, hastily thrown-together digital engagement solutions are often vulnerable to bank application fraud, account takeovers, and new account fraud, among other crimes.[8]

In addition, the COVID-19 pandemic has fueled a rise in fraud perpetrated against regional banks and their customers by disrupting normal operations and making customers leery of visiting bank branches.[9] This compels greater reliance on digital banking alternatives and contact centre assistance, both growing vectors of fraud.

Bank employees forced by the pandemic to work at home and outside the traditional contact centre environment are vulnerable to phishing scams and social engineering designed to provide fraudsters with access to customer accounts.

Another factor contributing to the rise in fraud in 2020 is economic instability. High unemployment increases the risk that financially vulnerable people will turn to fraud as a last-ditch means of generating capital. This risk has not decreased in 2021 as the pandemic rages on.[10]

In short, regional banks must not overlook the importance of investing in authentication and fraud prevention solutions as they seek to enhance and broaden their digital engagement platform.

Customer authentication is the first step in fraud prevention

The Nuance Regional Bank survey also solicited responses from banks on their current authentication and fraud prevention measures.

When asked what concerns them most about weak customer authentication factors, nearly four in 10 cited the risk of customer account takeovers, followed by new account fraud (32%), and customer identity theft (20%). By contrast, only 9% of the respondents expressed concern over a data breach.

Many bank security professionals struggle to mount an effective response to fraud, said Trace Fooshée, Senior Analyst at Aite Group. "It's very hard to prove the person at the other end of the line is in fact who they say they are without being intrusive," he explained.

Customer authentication that relies on personal information is particularly vulnerable to exploitation. Fraudsters can easily purchase the stolen personal information of bank account holders on the dark web, and then use that information in order to trick a contact centre agent into granting them access to a customers' accounts.

"Such identity deceptions are typically executed using social engineering techniques," Fooshée explained. "All the fraudster needs to do is be fairly good at convincing a customer service agent to surrender information. With a bit of charisma and emotional intelligence, it's not very difficult."

The findings align with research performed by Trace Fooshée, Senior Analyst at Aite Group and a specialist in fraud at financial institutions. "New account fraud and account takeovers are the most common and rapidly growing forms of fraud attacks against banks, making them the biggest concerns of bank security teams," said Fooshée. "In both situations, customer authentication is the first step in fraud prevention."The pandemic has fueled a rise in such transactions, from single mouse-click product orders to same-day delivery or curb-side product pickup. "Customer stickiness is always about ease, convenience and value," Montez explained. "One of the main reasons why a customer leaves a financial institution is a poor experience, and one of the key reasons they stay is the experiences with a bank's digital engagement solutions."

Both digital and voice channels are vulnerable. In digital channels, fraudsters attack "across all of them, and often," said Fooshée. "They're counting on the bank having a relatively siloed approach to managing the channels, with stronger controls in one channel but less robust controls in another."

Through digital channels, a fraudster can use stolen account credentials to gain access to a victim's accounts. Once inside, they may drain funds, open and use new lines of credit, or otherwise abuse the victim's identity.

282% increase in account takeover attacks between Q2 2019 and Q2 2020.[11]

"Since the pace of data breaches shows no signs of slowing, account takeover attacks will remain a significant source of anxiety for bank security teams for years," Fooshée said.

Even worse, a single successful attack can be quickly automated and scaled to ensnare more account holders into the fraud. "Once a workable attack pattern is developed, hackers use automated bots programmed to canvas the web and automatically enter in the stolen credentials of other account holders to access their digital accounts," Fooshée said.

He equated the fraud strategy to gamblers in Las Vegas working the slot machines. "On a very scalable basis, people keep pumping quarters into the slot, trying their luck to hit pay dirt," he explained. "Fraudsters are doing something very similar. But whereas fraudsters must get it right just once to profit, bank security teams must get it right all the time. And that requires the use of very sophisticated customer authentication tools."

Fighting fraud with the swiss cheese strategy

To size up these capabilities at present, the Nuance 2021 Regional Bank Customer Engagement, Authentication & Fraud Prevention Outlook survey asked banks which customer authentication tools they were currently using to enhance security. More than 60% use on-device biometrics, such as fingerprinting or facial recognition, in which biometric data are processed, stored and analysed in a secure location on the customer's device.

Other security solutions included the use of PINs and passwords (over 50%), enterprise biometrics solutions, in which biometric data is processed, stored and analysed in the cloud (over 40%), and SMS one-time passwords, whereby a numeric code is sent to a mobile number.

To reduce the incidence of a successful attack, Fooshée said these varied security solutions should be used in combination: The more layers of security, the better the chance to detect anomalies indicative of a possible attack.

Reliance on PINs and passwords alone, for example, is the equivalent of a single slice of swiss cheese, making it an inefficient way of authenticating customer for fraud detection purposes.

> "Protecting against financial criminals is all about layers of security. You want to pile one slice of swiss cheese on top of other slices of swiss cheese, so there aren't enough holes left for fraudsters to pierce."
>
> — Trace Fooshée, Senior Analyst at Aite Group

In a follow-up question, the survey respondents were asked which types of biometrics they presently use to detect and prevent fraud. Nearly six in ten said they use behavioural biometrics, followed by voice biometrics (45%).

These findings align with Fooshée's research. "We've found that biometrics solutions that assess behavioural patterns, such as how long it takes to fill out a bank deposit application form, are particularly good at identifying fraud," he said. "Two to three minutes is a good indication it's likely a human being, whereas less than a second is a good indication otherwise."

Voice biometrics are widely recognised as an effective way to detect fraudsters while streamlining authentication. They work by analysing the hundreds of physical factors and speech delivery elements that go into a person's voice. Within seconds, a voice biometrics system can authenticate a legitimate customer or identify a known fraudster with extremely high accuracy.

Lastly, conversational biometrics are a novel and highly effective form of fraud detection and prevention. A conversational biometrics engine the grammar, word choice, and language patterns of a given piece of text. This can be useful in live chat and other messaging channels, as well as in contact centres.

"Phone calls to customer service reps at a bank are a low-tech route of entry, since the criminal doesn't need to know how to program bots to launch a scalable attack," Fooshée said. "In this regard, conversational biometrics that detect common ruses and scripts are effective at identifying fraudsters in the act."

A win-win combination of digital customer engagement and security

In these unprecedented times, the importance of personalised, frictionless and secure digital customer engagement cannot be overstated. There is ample evidence to suggest that regional bank investments across all customer engagement channels, including an emphasis on authentication and fraud prevention, will reap dividends in the years ahead in the form of more satisfied customer—a critical consideration during this period of intensifying competition.

LEARN MORE

Visit Nuance or email us at cxexperts@nuance.com.

1 Application Fraud: Accelerating Attacks and Compelling Investment Opportunities, November 2020, Aite Group.
2 U.S. Digital Banking Engagement Platforms: Market Overview. December 2020, Aite Group.
3 2020 Zendesk Member Experience Trends Report.
4 "Nimble Online Banks Go After Brick-and-Mortar Behemoths." Perspectives. Dell Technologies, April 1, 2019.
5 "Thousands of Bank Branches are Closing, Just Not at These Banks." Wall Street Journal, June 15, 2018.
6 2021 Banking and Capital Markets Outlook. Deloitte. December 2020.
7 Ibid.
8 Key Trends Driving Fraud Transformation in 2021 and Beyond. December 2020 Aite Group.
9 Ibid.
10 Ibid.
11 Account Takeover Fraud and the Growing Burden on Business. Digital Trust & Safety Index. September 2020.

About Nuance Communications, Inc.
Nuance Communications (Nuance) is a technology pioneer with market leadership in conversational AI and ambient intelligence. A full-service partner trusted by 77 percent of U.S. hospitals and 85 percent of the Fortune 100 companies worldwide, Nuance creates intuitive solutions that amplify people's ability to help others.

ENT_4284_01_WP_UK, Sep 24, 2021