DIGITAL-FIRST BANKING

TRACKER®

AUGUST 2020

PYMNTS.com | NCR

DIGITAL-FIRST BANKING

TRACKER®

TABLE OF CONTENTS

PYMNTS.com | NCR

ACKNOWLEDGMENT

The Digital-First Banking Tracker® was done in collaboration with NCR Corporation, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE

Digital banking is more popular than ever, with 89 percent of American bank customers using mobile banking apps to manage their accounts. Ninety-four percent of these mobile banking users leverage online banking services at least once a month, and experts predict the usage of digital banking services to increase well into the future. The number of online and mobile banking users is expected to hit at least 3.6 billion by 2024 — a significant portion of the world's population.

Many factors are driving this surge in digital banking use, including increased convenience over visiting bank branches and greater access to banking services for individuals who are otherwise underbanked or lack access to a full array of affordable mainstream banking services. The latest study on underbanked households conducted by the Federal Deposit Insurance Corporation (FDIC) found that 25.2 percent of households in the United States either did not have bank accounts or were underbanked, using financial services that traditional banks did not provide. Digital banking is vital for providing checking accounts, loans, payment cards and other services to these individuals as it is much easier to conduct banking on a computer or smartphone than it is to visit a physical bank branch that may not be conveniently located.

The biggest, most recent factor driving digital banking by far, however, is the ongoing COVID-19 pandemic. Banks are closing physical branches, reducing hours of operation and encouraging customers to use their websites or mobile apps to conduct transactions and reduce face-to-face interactions between bank customers and staff. Services that were once available only at branches, such as loan or credit card applications, are being moved to mobile apps and ATMs. Some of the latter even include videoconference capabilities that connect live tellers with customers in remote locations, providing an alternative to meeting with bank staff in person.

COVID-19 might be a new worry for banks, but cybersecurity has been a concern since the dawn of digital banking. Up to one in five account openings are believed to be fraudulent, with bad actors seeking to steal both

customers' funds and their personal data, such as account numbers, Social Security numbers, payment card data and login credentials. Most financial institutions (FIs) rely on simple passwords to protect their customers, which are more at risk of being exposed in a third-party data breach, but many FIs are exploring more advanced security methods like biometrics and artificial intelligence (AI).

Neither COVID-19 nor digital fraud has shown signs of receding in the U.S. Tools like smart ATMs and AI could prove effective at stemming the tide for now, but these threats will likely be on banks' radars for the foreseeable future.

Digital-first banking developments around the world

COVID-19 is affecting every step of the banking process, including ATMs. Keypads, touchscreens and other physical input methods are potential routes of infection, so banks are turning to contactless methods that interface with users' smartphones instead. One such method is to have customers scan QR codes printed on the machines and then use their own phones to view account balances and request cash withdrawals, significantly reducing the amount of physical contact needed and driving down the risk of infection.

Some ATMs present crucial security gaps, however. A recent study from Portland, Oregon-based hardware security research company Eclypsium found that third-party drivers in ATMs' Windows operating systems could result in a security loophole that allows fraudsters access to cash dispersal, letting them rob the ATMs. Windows developer Microsoft has released security patches that solve this problem, but many ATMs are in remote areas, making hardware upgrades uncommon.

Banks are also taking new steps when it comes to payments security. Six of the United Kingdom's largest banking groups — Barclays Group, HSBC Group, Lloyds Banking Group, Nationwide Building Society, RBS Group and Santander Group — recently adopted the Confirmation of Payee system, which requires payers to enter payees' full names and rejects transactions if they do not match the names on the accounts. This reduces fraudsters' success rates when transferring money to their own accounts.

For more on these stories and other digital-first banking developments, read the Tracker's News and Trends section (p. 12).

The threats facing ITMs and how FIs can secure them

ITMs have innumerable benefits for FI customers, offering a vast array of services that would normally be available only inside a physical branch, such as account openings or loan applications. These public machines can be vulnerable to fraud, however, ranging from physical techniques like card skimming to advanced digital means like identity theft. In this month's Feature Story (p. 8), PYMNTS talked to Jason Powers, senior vice president of administration for Ascend Federal Credit Union, about how the CU protects its ITMs with a combination of physical security safeguards and behind-th e-scenes fraud analysis systems so that members can continue to safely enjoy their benefits.

Deep Dive: Keeping digital-first banking secure with AI, biometrics

Digital fraud and other forms of cybercrimes are a perennial concern for FIs, with bad actors leveraging phishing schemes, identity theft, account takeovers and botnets to try to scam banks and their customers. Keeping customer funds and personal data secure is FIs' top priority, but they must balance ironclad security with facilitating smooth customer experiences. This month's Deep Dive (p. 18) explores how FIs are harnessing customer authentication procedures, such as biometrics, as well as back-end AI systems to weed out fraudsters without discouraging legitimate customers.

EXECUTIVE Insight

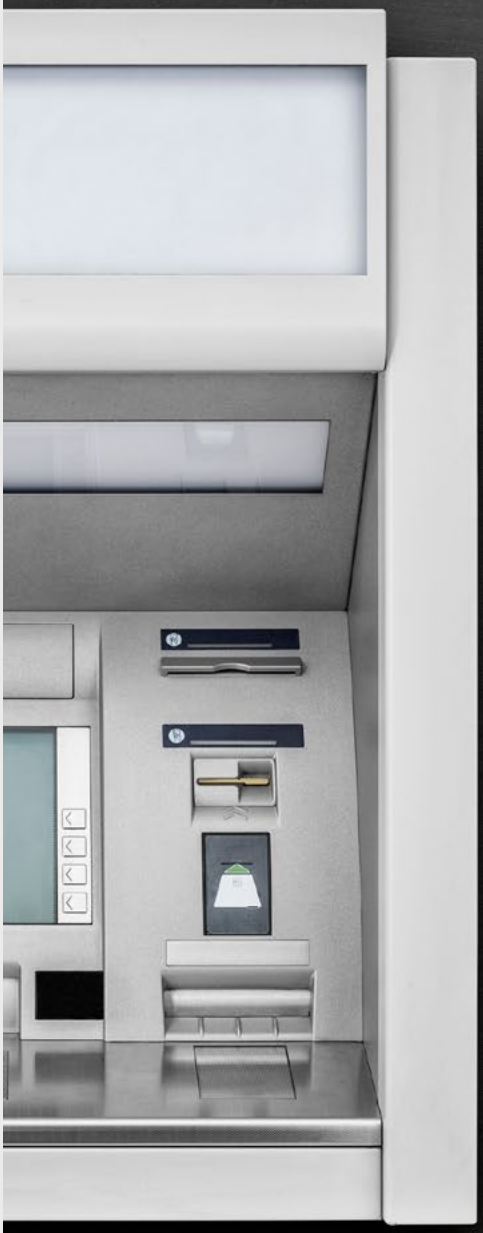
Security is of paramount importance to FIs, but for 87 percent of their customers, a seamless experience is the most important feature of any transaction. How can FIs ensure ironclad security without sacrificing their users' experiences?

"[During] a time of significantly fewer face-to-face interactions in our day-to-day lives, industries across the globe have been working to adapt their services and find ways to improve customer experience and convenience. With that comes a need to balance accessibility and ease of use with providing safe and secure interactions.

For financial institutions, that responsibility is just that much more significant.

Banks and credit unions need to be able to swiftly adapt in this ever-changing [arena] and bring innovative new technologies to market — all while keeping security top-of-mind. But to be agile and quickly implement new capabilities that offer both the convenience consumers crave and the security that's required to keep their accounts secure, it comes down to technology and mindset. For many financial institutions, this means adapting their culture, realigning their business strategies and reevaluating their technology and software to ensure lines of defense are structured and consistent."

Douglas Brown
senior vice president
and general manager
NCR Corporation



5 FIVE FAST FACTS

41%

Share of Europeans unable to access financial services due to the COVID-19 pandemic

$9.97B

Estimated value of the global ATM managed services market by 2027

37%

Share of Canadian FI customers using separate passwords for different accounts

99.9%

Prevention rate of fraud attempts using multifactor authentication

50%

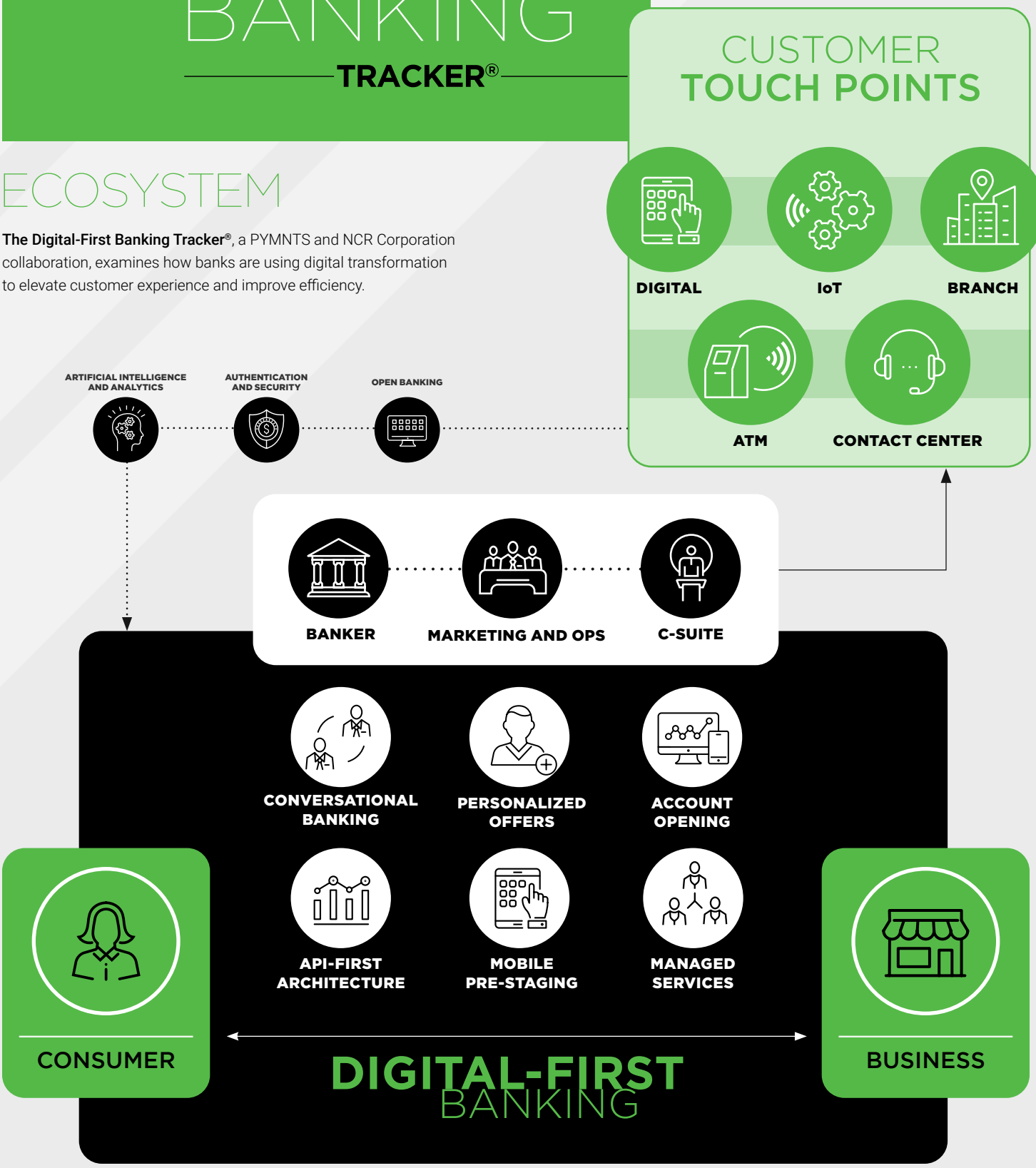
Increase in fraud detection rate for banks that harness artificial intelligence

DIGITAL-FIRST BANKING

TRACKER®

ECOSYSTEM

The Digital-First Banking Tracker®, a PYMNTS and NCR Corporation collaboration, examines how banks are using digital transformation to elevate customer experience and improve efficiency.



FEATURE STORY

ASCEND FEDERAL CREDIT UNION ON PROTECTING THE BENEFITS OF ITMs

Nearly every FI offers ATMs — a crucial piece of technology that allows customers to check account balances and withdraw cash at any time of day without having to visit a physical branch. There are more than 10 billion ATM transactions conducted in the U.S. every year, with the average ATM machine used 300 times a month. This massive popularity is driving many digital-first banks to invest in more advanced interactive teller machines (ITMs), which connect customers with human tellers via videoconference and allow for more sophisticated banking activities beyond cash withdrawal, including card applications and account openings.

One FI deploying ITMs on a wide scale is Tennessee-based Ascend Federal Credit Union, which first began this initiative in 2014. Its 200,000 members have been enjoying a range of improved services ever since, according to the credit union's senior vice president of administration, Jason Powers.

"We needed a way to open several new branches in Nashville," he explained. "But by extending our operating hours and centralizing the management of our tellers, ITMs are the solution that we chose [instead]."

ATMs and ITMs face a range of security threats, however, from smash-and-grab schemes for stealing physical money to identity theft techniques that trick machines into accessing accounts. FIs like Ascend rely on a number of approaches to help secure ITMs and limit their services to legitimate customers, including physical security safeguards and behind-the-scenes fraud analysis systems.

The advantages of ITMs

ITMs offer an array of benefits over traditional teller machines, according to Powers, including accepting loan payments and offering extended teller service hours. Connecting to a live teller rather than interacting with a simple computer interface enables the bank to perform the verification checks necessary for these complicated processes.

"We have a centralized location where our tellers are that works similar to a contact center, except instead of taking telephone calls, it's video calls as members walk up and tap the screen," Powers said. "It's very similar to a traditional teller line with the personal service of a representative on the video chat, and they can conduct almost 90 percent of the transactions they could do inside the branch via the ITM."

Not only is the expanded access to these services convenient for customers; it helps the CU in its back-end processes as well. Ascend and many other CUs have opted to retrofit their drive-thrus with these ITMs rather than have human tellers at booths as they can offer the same services in a fraction of the space. The ITMs also enable FIs to standardize and streamline their employee training processes as having all their video tellers in a single location allows

managers to immediately ascertain which processes are working or need improvement.

"It enables credit unions to centralize the management of that particular teller row, and that centralization condenses the interviewing, hiring and supervision of the service representatives to a smaller group of managers," Powers explained. "This provides greater consistency in coaching the employees, and obviously a much greater consistency and adherence to customer service standards, and diminishes idle time. Instead of having three or four tellers across two or three branches that are idle, you've got one teller who stays busy with the traffic volume."

These perks for both customers and CU management are effective only if the ITMs are safe to use, however. Keeping them secure comes down to a combination of physical security measures and digital fraud detection platforms.

Keeping ITMs secure

Securing ATMs and ITMs can largely be divided into two segments, according to Powers. The first relies on physical security measures to prevent brute-force attacks that enable criminals to physically remove money from cash drawers, including preventing a new technique called "jackpotting," which has been growing more popular in recent months, according to the United States Secret Service. This method involves fraudsters using malware or specialized electronics to hijack ATM systems and control their internal operations, including the ability to spit out cash.

"We have advanced security measures and alarm triggers in place to prevent jackpotting and other types of physical security threats and thefts," Powers said. "[We also have] the latest security methods installed to detect skimmers and shimmers, and stringent identity security protocols, policies and procedures to ensure we are correctly identifying our members to reduce identity theft and fraud."

"Skimmers" and "shimmers" are tools installed on ATMs and ITMs that read customers' cards as they are inserted into the machine, allowing the fraudster to learn their numbers and then use them toward illicit ends. The ATM Industry Association recently reported that 96 percent of ATM operators experienced some form of physical fraud between September 2019 and the year prior, with 91 percent of respondents saying that skimming devices were growing smaller and harder to detect.

Identity fraud is also a massive threat to ATM security, Powers said. Fraudsters armed with stolen account information or payment cards often attempt to access victims' accounts and withdraw funds as these transactions can attract less scrutiny at an ATM compared to a physical bank branch. Many FIs such as Ascend deploy behavioral analysis systems to detect and catch this type of fraud, identifying suspicious transactions that are not typical of the actual customers' whose identities have been stolen.

"We have a fraud analysis system for cards, online banking and checks submitted for payments that allows us to detect transactions, login requests, et cetera, that are not within a member's normal routine so that we can flag for follow-up with account notes," he explained. "The process allows us to be proactive to report fraudulent items to our security department and then to our members. When a member visits a branch or utilizes an ITM, the representative can easily follow up with the member to be certain all is in order."

ITMs can form a core segment of FI customers' financial lifestyles, but only if they are not used as avenues for fraud. Not properly safeguarding these offerings is a surefire way for FIs of all types to lose customers and leave them worse off than when they started.

NEWS &TRENDS

COVID-19'S EFFECTS ON THE BANKING INDUSTRY

41 percent of Europeans unable to access financial services during pandemic

The ongoing COVID-19 pandemic is having massive ramifications for financial markets around the world, with Europe being particularly hard-hit. A recent study of 4,000 bank customers across the EU found that 41 percent of respondents have been unable to obtain financial services due to physical branch closures and a lack of access to digital banking solutions. Many banks across the continent have limited their hours or shuttered their doors completely to reduce the risk of contagion. Digital banking is expected to help close this service gap, but many still lack this option.

Two-thirds of customers surveyed said they expect access to financial services to improve, however, as banks grow more used to offering services in a digital-first banking environment. A large majority of respondents had accounts with digital-first challenger banks, with 70 percent reporting having such accounts and 69 percent saying they offer superior services to those of traditional banks.

KBC Bank reports increased use of digital wallets due to COVID-19

Bank branch closures and reduced hours during the COVID-19 pandemic have resulted in more bank customers than ever using digital service options. Irish digital-first bank KBC Bank reported that customer use of digital wallets increased year over year by 38 percent in June, also marking a 27 percent increase since May. Digital wallet transaction volume rose 18 percent across April, May and June — the height of the pandemic in Ireland — compared with the same period the previous year. The Banking and Payments Federation Ireland noted that June also saw a new height in transaction value, with 20 percent of digital wallet transactions clocking in at more than €30.00 ($35.53 USD), up from 9 percent in June 2019. Average contactless transaction value grew from €11.92 ($14.12 USD) in February to €15.30 ($18.12 USD) in May as consumers increasingly preferred touchless options to avoid the risk of infection.

ATM DEVELOPMENTS

ATMs undergo contactless upgrades to increase safety during pandemic

The COVID-19 pandemic is also forcing banks to rethink their ATM safety protocols as the virus can live on surfaces for days and potentially infect ATM users through physical contact. Many banks are adopting the technology needed to offer contactless ATMs instead, which enable users to conduct transactions with their smartphones. Users scan an ATM-mounted QR code and request cash from their phones, at which point the machine deposits cash for users to take without them having to interact directly with the machine's surface.

Some banking experts believe that ATMs' roles could shift entirely as digital and mobile banking options become more popular and cash usage declines. They could potentially be repurposed to serve as hubs for a variety of financial interactions instead of simple cash dispersal, such as registering for mobile banking, collecting deposits or providing loan advice through video-connected bank tellers.

Faulty Windows drivers to blame for ATM vulnerabilities, research finds

ATMs are common targets for hackers, fraudsters and other bad actors, and many contain a security flaw that could make them extremely vulnerable. A study from Portland, Oregon-based hardware security research company Eclypsium recently found that faulty third-party drivers in Windows operating systems were to blame for security weaknesses, potentially giving fraudsters access to the cash drawers. These drivers come from several third-party vendors and control ATM functions like cash dispersal, which would allow hackers who crack the drivers to withdraw as much money as they please.

Microsoft has released patches and security upgrades to protect against these types of attacks, but it is incumbent on ATM operators to upgrade these systems, which does not happen frequently. Regulations can also slow the upgrading process as any change to security systems must be recertified before the ATM goes into operation again, and banks often do not wish to undergo this time-consuming process.

ATM managed services market expected to hit $9.97 billion globally by 2027

The ATM market is still growing, despite these security and COVID-19 concerns, with a recent report predicting the size of the global ATM managed services industry will reach $9.97 billion by 2027. This equals a significant increase from the market size of $6.11 billion in 2019, representing a compound annual growth rate (CAGR) of 6.5 percent between 2020 and 2027. Experts attribute this growth to a rise in global debit card usage as well as demand for advanced ATM services like account openings and video tellers.

ATMs are particularly popular in the Asia-Pacific region, which accounted for two-fifths of the

global market in 2019. The North American market held only one-quarter of the global share in contrast. The Latin America, Middle East and Africa (LAMEA) market, however, has the highest projected CAGR during the forecast period at 8.1 percent.

NEW DIGITAL-FIRST TECHNOLOGY INTEGRATIONS

UK's six largest banking groups adopt Confirmation of Payee tool

Security and authentication are crucial facets of digital-first banking to ensure that payments arrive safely to the intended recipients without alteration or interception. One tool to help accomplish this is Confirmation of Payee, which was recently adopted by the six largest banking groups in the U.K.: Barclays Group, HSBC Group, Lloyds Banking Group, Nationwide Building Society, RBS Group and Santander Group. Confirmation of Payee works by confirming that the payee's name, as typed by the sender, matches the name on the account, preventing fraudsters from posing as recipients and accepting funds.

The adoption of Confirmation of Payee by these six groups means that 90 percent of all bank transfers in the U.K. will now use this authentication system. TSB plans to adopt it in the fourth quarter of 2020, further increasing uptake.

Deutsche Bank and Google Cloud partner on next-gen financial products

Cloud services are becoming ever more important in the world of digital-first banking, with financial industry players studying and adopting these services to offer new products to their customers. One such example comes from Deutsche Bank, which recently partnered with Google Cloud in a multiyear agreement to accelerate its cloud transition and jointly develop new products. The partnership will allow Deutsche Bank to access Google's data science, AI and machine learning (ML) tools to develop these new offerings, which will be aimed at both consumers and corporate clients.

Potential corporate banking use cases include cash flow forecasting, risk analytics and security solutions, according to Deutsche Bank's CEO, Christian Sewing. Products for private banking customers will focus on smoothing and accelerating interactions between them and bank staff.

Google adds six more FI partners to its upcoming digital banking platform

Google is also making inroads in the digital banking market by adding six partners to its upcoming digital banking platform via Google Pay. These new bank partners include Bank Mobile, BBVA USA, BMO Harris, Coastal Community Bank, First Independence Bank and SEFCU. These partners will be added to its existing roster of Citi and Stanford Federal Credit Union, allowing customers to access digital banking

services through Google Pay when the offering launches. Google's entry into the digital banking space was first revealed in November 2019.

The service will leverage Google's front-end interface along with checking and savings accounts from its partner FIs. The Google app will be co-branded with the customer's bank of choice — a far cry from many of its competitors, which do not generally advertise their banking partners.

US Bank launches smart assistant for digital banking

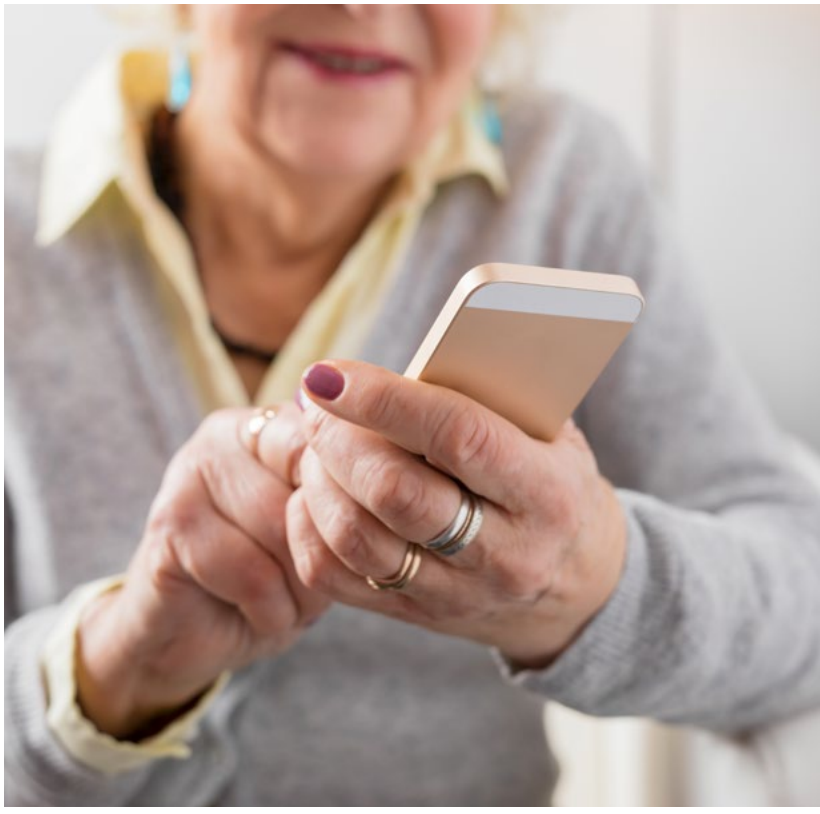
Bank customers are turning to digital banking in record numbers during the COVID-19 pandemic, many for the first time. This transition can be challenging, especially for older customers, which is why U.S. Bank recently launched an AI-based virtual assistant for its mobile banking app. The assistant utilizes natural language recognition so that customers can use voice commands instead of navigating menus. This enables customers to conduct functions like bill pay, fund transfers and transactions more quickly and conveniently, according to the bank.

Three-quarters of service transactions and 46 percent of loan sales are now conducted virtually at U.S. Bank as the pandemic shifts these services away from physical branches. The virtual assistant had been under development for 18 months, but its launch was accelerated in light of the health crisis and the subsequent digital banking surge.

DIGITAL BANKING LAUNCHES

Mozper unveils new digital banking service for Latin American parents and children

It is common for parents and their children to have linked bank accounts in the U.S. and Europe, allowing kids and teenagers financial freedom and securing transactions while letting parents monitor their financial habits. A new service called Mozper recently launched to offer these capabilities to families in Latin America, with its name a mash-up of "money," "prosperity" and "Generation Z." The system will include a debit card and app that both children and parents can access, with Visa providing card processing services.



The offering is aimed at providing financial education for families, something only 30 percent of Latin American financial customers have received, according to Yael Israeli, Mozper's CEO. Israeli unveiled the service in Mexico in late July with plans to expand its availability across the Americas shortly.

Orange Bank launches new mobile banking services in Africa

Another player in the financial industry looking to expand digital banking's footprint is France-based Orange Bank, which recently launched a new digital banking service in Africa. The system is based off Orange Bank's money transfer service that originally began in 2008 and is intended to serve as an alternative to traditional banking apps for individuals who work informal jobs without proof of employment or identification. The automated signup process takes customers' incomes and risk levels into account without the need for these details.

The app will be available initially in Côte d'Ivoire and will need approval by regulator Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) before its planned launches in several other African countries, including Burkina Faso, Mali and Senegal.

Kabbage creates digital checking accounts for SMBs

Small to mid-sized businesses (SMBs) have just as much need for bank accounts as consumers, and like retail customers, business owners and treasurers prefer to do their banking on the go.

Cash flow solutions provider Kabbage recently launched a new offering to this end called Kabbage Checking, which allows SMBs to access digital banking services, including digital wallets, checking accounts and bill payments. The app has no opening fees or maintenance costs but instead offers customers a 1.1 percent annual percentage yield, which Kabbage pays out on a monthly basis.

Kabbage president Kathryn Petralia noted that more than 225,000 SMBs have already signed up for this new service. The company plans on integrating its Kabbage Insights, Kabbage Payments and Kabbage Funding into Kabbage Checking, allowing customers to access all of these features in a single app.

DEEP DIVE

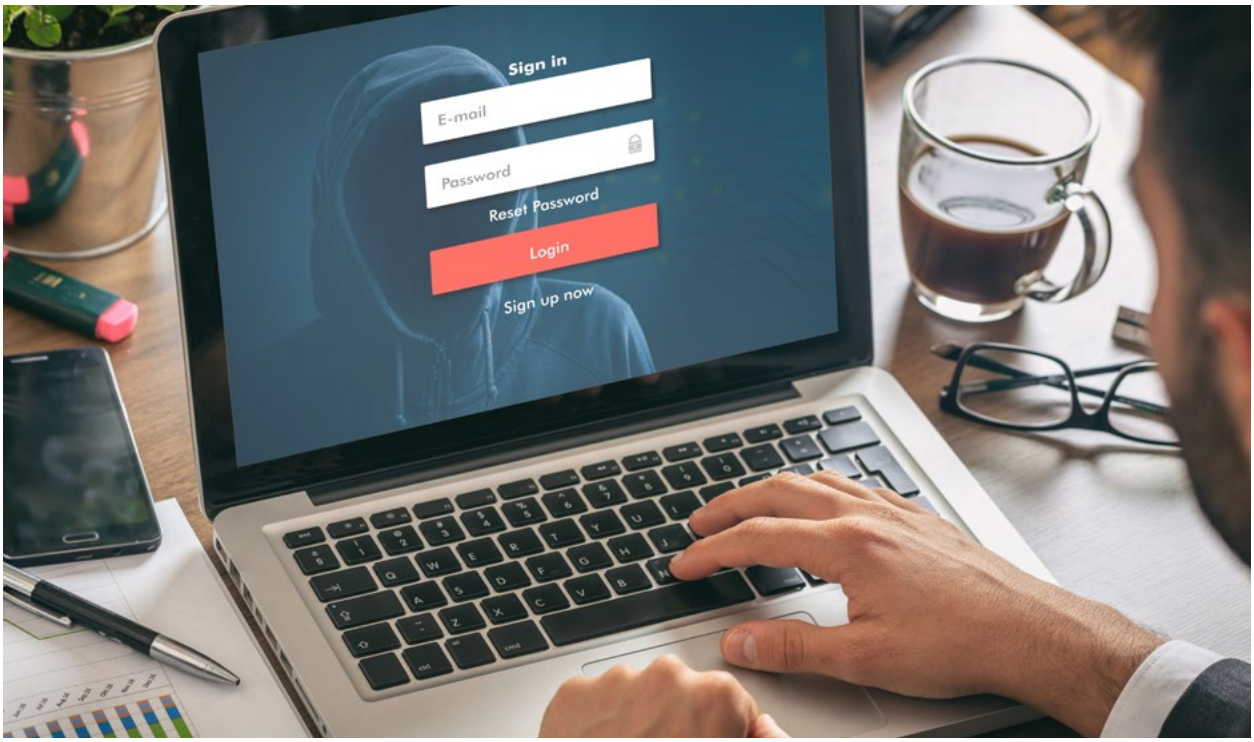
HOW DIGITAL-FIRST BANKS CAN EFFECTIVELY AUTHENTICATE CUSTOMERS, STAMP OUT CYBERCRIME

Cybersecurity is a constant and pressing concern for FIs of all types and sizes, ranging from small community credit unions to multibillion-dollar international banking conglomerates. The World Economic Forum estimates that more than $1 trillion is lost to financial crimes annually, with fraudsters deploying a number of techniques ranging from phishing scams to identity theft to sophisticated botnets. Cybercrime and fraud problems have only been on the upswing in recent years, with one study finding that fraud increased by 30 percent in Q3 2019 alone, with one in five account openings revealed to be fraudulent.

Fighting fraud will require not only diligence on the part of bank staff and customers but also an array of advanced technology. Some of the most effective innovations are authentication tools ensuring that customers are legitimate and AI-based systems that sniff out fraudsters who manage to make it into bank systems. The following Deep Dive explores how these two technologies can drastically reduce bank fraud rates without unduly burdening legitimate customers.

Authenticating customers

The first step to securing customer accounts at digital-first banks involves customer authentication to ensure that the users are who they say they are and not fraudsters attempting to breach accounts with stolen identities. Banks largely use passwords, PINs and other forms of knowledge-based identification, with a PYMNTS study finding that passwords are the most common authentication method used by financial services, eCommerce and healthcare companies. This method is not the most secure, however, in large part due to poor password hygiene on the part of bank customers.



A recent study from data analytics firm FICO found that only 37 percent of bank customers in Canada use separate passwords for different accounts, for example, and 22 percent use two to five passwords among all their online profiles. This represents a massive security risk as a data breach at any one of these accounts could give fraudsters access to any other account that uses the same password.

Banks are instead turning to more secure forms of authentication for their customers' accounts. One of the most common is multifactor authentication (MFA), which relies on input from users besides their passwords, such as numeric codes texted to their mobile devices. These authentication methods can stop potential bad actors cold as the passwords they steal from data breaches are useless on their own. Studies have shown that using MFA can prevent more than 99.9 percent of attacks that rely on stolen credentials, making such solutions an imposing obstacle for hackers armed with pilfered passwords.

One of the problems with MFA, however, is that it requires extra work on the customer's part — a tall order when many customers value seamlessness over security. Some banks are turning to biometric authentication instead, such as a selfie taken on a customer's smartphone. The bank's system would then compare the submitted selfie to a 3D facial-recognition map to ensure users' identities.

Fraudsters have been known to spoof facial-recognition systems by using photos or videos of legitimate users, however, with some systems requiring a likeness certification test to confirm that it is actually the user. The system could request that the user smile or wink during the verification process, for example.

No authentication system is 100 percent effective, but systems that harness AI have shown the most promise in this capacity.

Leveraging AI to hunt down fraudsters

Banks have traditionally used human analysts to study transactions for signs of fraud or other cybercrime, such as unusually high sums, false information on credit card or loan applications or other signs that something could be amiss. The problem with relying on human analysts is that the sheer quantity of transactions that banks process every hour makes it impossible for even a large fraud prevention team to keep up.

Some banks rely on static rules to ease the burden on their analysts, conducting manual reviews only for transactions that have certain red flags of potential fraud. Not only are these rules ineffective — with 45 percent of companies using them reporting that they don't successfully prevent fraud — but they also have very high false positive rates. Sixty percent of companies said they had accidentally blocked legitimate customers with their static rules, and another 60 percent stated that even customers who were not blocked faced friction in the review process.

AI can solve both these problems as it can take thousands of different data points into account and assign transactions a likelihood of fraudulence rather than outright blocking based on individual variables. These systems can also compare legitimate transactions to known fraudulent ones and learn the differences between them, refining their algorithms and applying these lessons toward future transactions. They can do all of this in mere fractions of a second, reducing the burden on human analysts and accelerating the review processes of legitimate transactions so customers can be approved faster. Banks using AI have found that their fraud detection rates have improved by as much as half while their false positive rates have declined by more than 60 percent.

The most effective fraud prevention systems use multiple layers of protection, with ironclad authentication at the point of entry and AI systems to handle bad actors that make it past that point. No fraud system by itself is perfect, but a multisystem approach can drastically reduce the threat of fraud.

about

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.

NCR

NCR Corporation is a leader in banking and commerce solutions, powering incredible experiences that make life easier. With its software, hardware, and portfolio of services, NCR enables transactions across financial, retail, hospitality, travel, telecom and technology industries. NCR is headquartered in Atlanta, Georgia, with 34,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe to this report, please email us at feedback@pymnts.com.

DIGITAL-FIRST BANKING

TRACKER®

DISCLAIMER

The Digital-First Banking Tracker® may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATION`S ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.