DIGITAL-FIRST BANKING TRACKER®

AUGUST 2022

PYMNTS.com | NCR

Read the previous edition

JUNE/JULY 2022

Digital-First Banking Tracker®

DIGITAL-FIRST BANKING TRACKER®

PYMNTS.com | NCR

ACKNOWLEDGMENT

The Digital-First Banking Tracker® was produced in collaboration with NCR, 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.

TABLE OF CONTENTS

EDITOR'S LETTER

As more consumers see the benefits of digital banking, financial institutions (FIs) are under more pressure than ever to deliver not merely convenient but also safe digital experiences for consumers to rely on. Concerns about data security are reaching an all-time high, and with good reason. Data breaches hit unprecedented levels in 2021, with the personally identifiable information (PII) of approximately 300 million victims exposed, and identity fraud grew by 79%. These concerns underlie an apparent paradox: More than 80% of consumers in a recent PYMNTS survey said they use digital methods to connect with their banks, yet just 7% of consumers use a digital-only bank.

Digital banking services are now offered against a field of competitors that is almost boundless, with even community and local banks no longer dependent on geography to gain and retain customers. The multitude of familiar digital banking options alone might explain consumers' low usage of digital-only entities. A closer inspection, however, suggests that a lack of trust is at the heart of consumers' resistance to primary engagement with digital-only banking services. Nearly 50% of consumers, in fact, cite data security worries as a specific deterrent to banking primarily with a digital-only financial services provider.

Despite this anxiety, technological solutions are making significant progress in data security, with such strategies as behavioral and physical biometrics and password-less authentication allowing companies to identify users with close to 100% accuracy. Artificial intelligence (AI) and machine learning (ML) algorithms offer another promising solution for data security by improving fraud detection.

The success of digital-first banking hinges on consumers' trust in digital financial channels. It will require continued investment in emerging technologies as well as outreach and education to convince consumers of digital banking's security and ease of use.

This edition of the Digital-First Banking Tracker®, a PYMNTS and NCR collaboration, takes a deep look at data security in digital-first and digital-only banking, including how technology makes it more difficult to breach security and how raising consumer awareness of this could generate more widespread trust and acceptance.

Thought Leadership Team

PYMNTS.com

Feature Story

BM Technologies On

Managing Digital Security And The Customer Experience

REGARDLESS OF WHERE THEY OPERATE IN THE SPACE, MODERN FINANCIAL SERVICES COMPANIES NEED TO BE ABLE TO LEVERAGE DATA AND LEADING-EDGE TECHNOLOGY TO DELIVER MORE WITH LESS, ACCORDING TO JAMIE DONAHUE, CHIEF TECHNOLOGY OFFICER AT BANKING-AS-A-SERVICE (BAAS) PROVIDER BM TECHNOLOGIES (BMTX).

While digital-native firms, from crypto exchanges to digital banks, have transformed the financial world in this regard, even the most digitally adept firms contend with sophisticated online criminals exploiting the same technology to perpetrate identity theft, launder money and commit a number of financial crimes.

Many tools are available to firms for creating a secure environment, from automation and multifactor authentication to biometric monitoring. At the same time, firms must balance security against minimizing friction in the customer experience. Even then, some friction can actually help with customer satisfaction, as friction represents the visible side of security.

KEEPING THE CUSTOMER SATISFIED

“The main challenge at BMTX is the constant balance of creating the most secure environment while maintaining a frictionless experience to build trust with our clients,” Donahue said. “If you overrotate, the experience can become clunky and hinder adoption.”

BMTX’s response to that challenge starts with the user experience, he said. When working on security solutions, the company’s teams work backward from how customers will experience a security implementation. “[This approach is] longer, but we believe it’s worth the effort in the end,” Donahue said.

Technology also helps, and Donahue said that BMTX employs AI, ML and automation to create a layered strategy that ensures the platform as a whole is secure. That does not just mean secure authentication procedures: AI and ML play a critical role in fraud monitoring, bringing capabilities that human interaction cannot match.

“Our deployment of these technologies has accelerated our time to market and improved operational resiliency,” he said. “We have found that AI and ML are extremely powerful when used synergistically to solve efficiencies in our operations.”

A UNIVERSAL CHALLENGE

While digital-native financial services companies may be at the forefront of many innovations in data security and digital fraud prevention, they are at no greater risk than traditional FIs, Donahue said. As a result, any public perception of traditional FIs having an advantage in the data security space is misguided.

“Traditional brick-and-mortar institutions have many digital vectors they service their clients and partners through,” he said. “The financial services industry is digital, even for the ‘non-FinTech’ players.”

As a result, financial services companies such as BMTX can have an advantage against some security threats. Digital threats are top-of-mind for such companies and have been from the day they turned the lights on. Unlike brick-and-mortar institutions, they are not learning to address threats in a new environment but are instead adapting to evolving threats in their native space.

SEEKING OUT THE BEST SOLUTIONS

While BMTX has the digital DNA that comes from its foundation as a cloud-based BaaS provider, not every technology it uses is developed in-house, Donahue said. The focus for BMTX is on finding and employing the best solution available, whether that means it is a BMTX solution or something purchased from another company. That also means creating and adopting the best application programming interfaces (APIs) for a given need.

“We believe that success in the new digital age in financial services will be highly dependent upon two factors: our ability to integrate and embed our functionality into other ecosystems, [and ensuring] our platform is able to seamlessly integrate with partners to bring a wide breadth of services to our clients.”

Working well with others does not mean just other businesses, either. Donahue said that good relationships with regulators can help financial services companies stay on top of the latest concerns and developments, and regulators can be a great source of information.

Whether it comes to working with partners, customers or regulators, financial services companies need to be aware of developments in their space as well as open to collaboration that improves their end products.

“If you want to go fast, go alone. If you want to go far, go together,” Donahue concluded.

Q&A

DOUG BROWN
President

NCR

How do data security, fraud and trust concerns influence consumer attitudes toward digital-only banks?

Most digital-only banks don't have years of built-up brand trust and track record that they can fall back on as a key component of their offering. For digital-only banks, they have to rely on messaging and emphasize how they are protecting the privacy of current (and prospective) customers. It's also critical they walk the walk. The leeway for a slip-up — even minor — is much smaller.

Is addressing these concerns simply a question of better messaging, and if so, how can digital-only and digital-first FIs win the trust of potential customers?

It has to go beyond messaging. It's the first step, especially for FIs with less reputation, but it has to go further. Transparency is a key component to that messaging and building that trust: Don't just tell me in fancy marketing speak; actually show me how you're going to protect my privacy and keep my money safe.

Consumers want an experience that is quick and convenient and are often willing to sacrifice some security measures, such as multifactor authentication, if it means they can quickly access the tools they need. How do FIs or FinTechs balance providing the best security while still providing a great customer experience?

It's an extremely fine line and one that FIs and FinTechs are battling every day. As stated previously, transparency and communication are key components. One key component to making sure consumers are getting the experience they expect but also keeping them safe is by adopting new security measures and technology as they come out.

Looking to the future, what strategies do you believe will prove the most successful in helping FIs protect the security of customer data while minimizing frictions?

Biometrics can go a long way in that effort, allowing FIs to add in additional layers of security without adding friction. Biometrics goes beyond just fingerprint or facial recognition. Behavioral data from how fast you navigate common activities to how hard you press on the screen can all play into providing security without sacrificing experience.

PYMNTS Intelligence

Why Data Security Is Key To Consumer Trust In Digital-Only Banking

THE ACCELERATED DIGITAL TRANSITION THAT ACCOMPANIED THE PANDEMIC HAS CONTRIBUTED TO GREATER RELIANCE ON DIGITAL BANKING TOOLS.

While 48% of surveyed consumers still use branches, just 11% say branches are their primary banking method, in contrast with 41% who bank primarily using mobile apps. More than 80% of consumers connect with their accounts digitally, including 26% who most often access their accounts with a computer. At the same time, just 7% of consumers use a digital-only bank. This is possible because digital banking access has become nearly ubiquitous, regardless of the type of FI.

Digital banking is available to consumers from a wide variety of FIs, FinTechs and neobanks, with even the most local institutions no longer restricted by geography when it comes to gaining and retaining customers. As such, all digital banking services are offered against a field of competitors that is nearly limitless. With so many digital options from which to choose, digital-only entities' low usage may not appear to be surprising. A deeper inspection, however, reveals that data security concerns are driving down consumers' primary usage of digital-only banking, with 47% citing this factor as a deterrent to banking primarily with a digital-only provider.

This month, PYMNTS Intelligence takes a closer look at data security in digital-first banking, including how technology makes it more difficult to breach security and how raising consumer awareness of digital security measures could generate greater trust.

FIGURE 1:

How consumers engage with their bank accounts

Share of consumers who engage with bank accounts in select ways, by most-used method and overall usage

Source: PYMNTS.com
Digital Banking, September 2021

N = 2,225: Complete sample, fielded July 1, 2021 - July 7, 2021

TECHNOLOGY PROGRESS IN DATA SECURITY

Consumers' concerns about digital data security are well-founded. Data breaches reached unprecedented levels in 2021, with the PII of approximately 300 million victims exposed, while identity fraud grew by 79%. With all this happening, 62% of United States consumers say they are either very or extremely concerned about the danger data breaches pose.

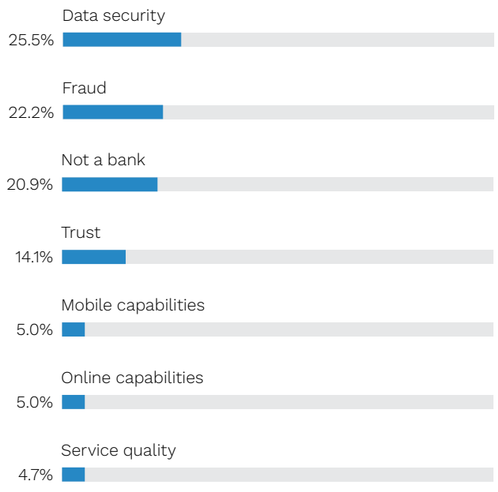
Nevertheless, technological solutions are making substantial progress in data security. Overall, 92% of data breaches are related to cyberattacks, and several startups are addressing this problem through behavioral biometrics. By combining multiple behavioral characteristics, companies can create a behavioral biometric profile that is nearly 100% accurate in distinguishing fraudsters from legitimate users. At the same time, behavioral biometrics do not have to be the only factor securing user data against breaches but can contribute to improved accuracy of anti-fraud stacks that include physical biometrics plus passwordless authentication.

AI algorithms offer another promising solution for data security by improving fraud detection. Anti-money laundering (AML) and know your customer (KYC) fraud detection are among the top use cases seeing the greatest investment. The number of FIs deploying AI for fraud detection jumped from 10% to 31% in 2022, and 75% of acquiring banks use AI to detect card transaction fraud. Along with ML, AI is one of the main technologies utilized to enhance data security without downgrading the user experience.

FIGURE 2:

Reasons consumers opt against using digital-only banking services

Share of consumers citing most important reason for not using digital-only banking services



Source: PYMNTS.com
Digital Banking, September 2021

N = 2,225: Complete sample, fielded July 1, 2021 - July 7, 2021

CONSUMER TRUST IN DIGITAL DATA SECURITY

PYMNTS' research points to data security as a leading concern among those consumers who say they have little or no interest in digital-only banking. This concern is especially high among baby boomers and seniors, one-third of whom cite security as a reason to opt against digital-only banking services. Moreover, 26% of all survey respondents who were uninterested in digital-only banking ranked data security as their top reason for this lack of interest. Despite this, there is still strong interest in digital-only banking among younger consumers, with 42% of bridge millennials and 41% of millennials very or extremely interested in having primary accounts with digital-only banks. Convincing consumers of digital-only accounts' security is likely the key to making the most of this interest, however. Offering at least one security-enhancing feature was the single most important factor inspiring consumers' trust in a financial services provider, at 83%.

PYMNTS' research further suggests that one way to gain consumers' trust in digital-only banking is through the use of advanced security techniques such as biometrics and passwordless login. Sixty percent of surveyed consumers said that having information about how their transactions are secured has a very or extremely big impact on their trust, and 44% said the same about the ability to log in without passwords. While 40% of consumers want easy onboarding in their online banking platforms, 30% demand biometric logins and 19% prefer no-password logins.

Digital-only banking service providers have a powerful opportunity to expand their presence in the banking market if they can demonstrate data security as well as ease of use. A failure to convince consumers of a digital-only platform's security, however, could hinder its acceptance.

NEWS & TRENDS

CONSUMER CONCERNS AND COMFORT WITH DIGITAL BANKING

EUROPEAN CONSUMERS AFRAID OF HOW FINANCIAL DATA IS ACCESSED, REPORT FINDS

Data mistrust may be compromising growth in digital economies, according to a recent report. More than two-thirds of consumers in Europe are unsure about who has access to their personal financial data, even as most of them are concerned about the security of their online activities. The report, based on a survey of 6,000 consumers in five European countries, suggests that this lack of knowledge is giving rise to a widespread lack of trust between consumers and organizations.

Some notable findings include that 72% of consumers are worried about technology's role in spreading misinformation, yet just 10% think that governments and businesses are transparent about how they use these technologies. Nearly half of consumers surveyed said that technological progress is necessary to improve their well-being, but 58% have growing concerns about the security of their digital footprints. In financial services, many consumers are also signaling that they miss the human touch. While 40% believe in-person financial services are waning, 29% would switch banks simply because theirs was not fully available online, and 33% would trust an app to manage all their finances, even though it generated greater returns. Finally, 65% of respondents said they expect financial services organizations to continue to offer in-person service. The report noted that realizing technology's full potential will require industries to take a proactive role in helping consumers understand and gain confidence in data privacy protection.

COMFORT LOGGING IN TO FINANCIAL SERVICES WITHOUT A PASSWORD IS INCREASING, STUDY FINDS

Logging in to financial services accounts may be changing as consumers have grown comfortable with new login methods that remove the requirement to memorize long and increasingly complicated passwords. A recent PYMNTS report found that 61% of consumers would be willing to do away with passwords as an authentication option for their accounts. In addition, nearly half of the 2,719 consumers surveyed said they believe that passwords will soon be completely eradicated.

As financial providers switch to newer, more advanced authentication methods such as biometrics, consumers are showing more trust in letting go of passwords. According to the report, 45% of consumers said they were comfortable with the security provided by non-password login methods. Their trust level changes depending on the devices they use to log in, however. Approximately 60% of consumers who use multiple options — including both mobile and desktop-based devices — to access financial accounts are comfortable not using passwords, and roughly half of those who use mobile devices alone are comfortable using non-password methods.

CANADIAN FIs LACK IN SATISFYING DIGITAL BANKING SERVICES, REPORT FINDS

Canadian consumers are less satisfied with the digital banking experiences offered by their FIs, according to a survey of more than 8,000 consumers, owing much to financial stress and lack of personalization. The report found that of those consumers who physically visit FI branches, 65% said they had a positive personal relationship with their banks, but just half of those who do their banking primarily online or on mobile channels said the same. This, the report noted, indicates that banks in Canada are not providing the same level of personalized service in digital banking as they do in branches.

The report said that low customer adoption of spending analysis and budgeting tools gives a clue to the need for more personalization, as these tools raise satisfaction across the board and can provide consumers with the personalized information they need to keep a better eye on their finances. Half of consumers surveyed said they were financially "healthy," while nearly one-third were financially vulnerable. Another 11% said they were "overextended" in their financial situations.

ONE-THIRD OF CONSUMERS PREFER DENTAL VISITS TO INTERACTING WITH THEIR BANKS AFTER NEGATIVE EXPERIENCES

A trip to the bank is supposed to be more pleasant than a dental checkup, but a new report suggests otherwise, finding that one-third of consumers would rather go to the dentist than converse with their FIs after a negative experience. Subpar customer support and digital experiences are increasingly becoming a frustration for bank customers, and the survey of 1,000 U.S. consumers found that good customer support is one of the biggest priorities for them when interacting with their banks.

Much of consumers' satisfaction with customer support hinges on the use of their preferred communication channels. The survey found that nearly 90% of customers want to be able to use digital tools such as SMS, chat apps and social media to connect with their banks. Customer satisfaction decreases with slow or unclear communication, and speed was found to be one of the most favored features, with SMS the preferred channel for that reason. Nearly half of respondents said they prefer text messaging over emails or phone calls to receive alerts from their FIs.

DIGITAL SECURITY AND **FRAUD TRENDS**

£583M ($701M USD) LOST TO APP FRAUD IN U.K. IN 2021, REPORT FINDS

Authorized push payment (APP) fraud, which tricks victims into providing real-time payments to fraudulent actors, rose dramatically in the United Kingdom in 2021, according to a recent report, resulting in losses of more than £583 million ($701 million USD). Nearly 40% of that total, or £215 million ($259 million USD), was lost to impersonation scams, and £172 million ($207 million USD) was lost to investment scams.

APP fraud generally takes the form of scams on social media, dating apps and purchase platforms such as auction websites that ask for money to be paid in real time, which is then quickly transferred to numerous "mule" accounts before being cashed out. Often, the money is difficult to trace and recover. In addition, current legislation does not offer legal protection to victims for the recovery of money lost through APP scams if the victim authorized the payment. A 2019 law called the APP Voluntary Code was passed to help hold payment service providers (PSPs) accountable if the victims met certain standards. In 2020, the law helped to recover some £147 million ($179 million USD), the report noted, representing about 47% of documented APP losses.

BANKS NO LONGER TOP TARGET FOR CYBERATTACKS BUT STILL AT GREAT RISK

The stability of the global financial system relies on the safety of the networks it operates on, and while a new report found that financial services dropped from being the top target of cyberattacks in 2021, the industry is still highly vulnerable to ransomware and other attacks. From 2015 through 2020, finance and insurance was the most attacked industry, with 70% of attacks on banks, while approximately one-third targeted insurance and other financial organizations. Last year, manufacturing took over as the industry most attacked, surpassing the financial services and insurance industries.

While the drop in attack status was attributed to improved security standards at financial organizations, fraudulent actors continue to look for ways to outsmart the safeguards. Ransomware and phishing remain the most frequent forms of cyberattack, with nearly three-quarters of firms having experienced ransomware attacks that caused 63% to pay ransoms to unlock networks. Business mergers and acquisitions are increasingly being used to target compromised systems, the report noted, with public information such as stock valuations serving as incentives for the attacks.

DIGITAL-FIRST BANKING

TRACKER®

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 in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

ABOUT

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 or comments, or if you would like to subscribe to this report, please email us at feedback@pymnts.com.

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 LIMITATIONS 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.