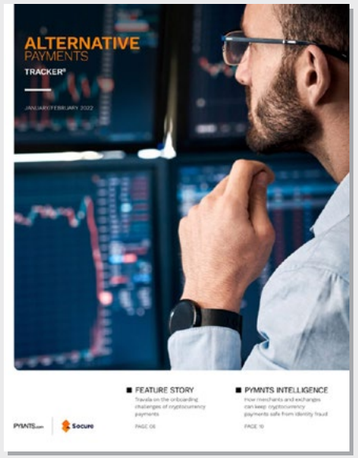
ALTERNATIVE PAYMENTS TRACKER®

MARCH 2022

PYMNTS.com | Socure

Read the previous edition



JANUARY/FEBRUARY 2022

Alternative Payments Tracker®

ALTERNATIVE PAYMENTS TRACKER®

PYMNTS.com | Socure

ACKNOWLEDGMENT

The Alternative Payments Tracker® was produced in collaboration with Socure, 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

Consumers have quickly come to prefer digital solutions and channels to fulfill their banking, shopping and other payment needs in the pandemic's wake. Recent PYMNTS data found that 60% of United States consumers prefer to bank via mobile apps, with just 11% of individuals surveyed stating they use physical branches as their primary banking channel.

These changing habits also inspire consumers to experiment with digital payment methods and solutions outside the traditional banking sphere, including cryptocurrencies, mobile wallets and buy now, pay later (BNPL) methods, which grant them financial flexibility as well as digital convenience. A September 2021 study found that 31% of consumers had increased their use of FinTech apps since the pandemic's onset, indicating a growing comfort with mobile payment and financial services. Black Friday and Cyber Monday sales for the past year also showed BNPL usage skyrocketing in the U.S., with installment payment provider Klarna reporting a 141% increase in U.S. sales during that period, compared to that same time in 2020. Transactions on cryptocurrency platforms surged 567% year over year for a total of $15.8 trillion in 2021, indicating consumers' and businesses' increased willingness to engage with digital currencies.

Staying on top of consumers' changing preferences is critical for merchants, but businesses supporting these alternative payment methods must adequately protect these solutions against fraudsters. Cybercrime rates swelled alongside the digital economy in 2021, with one recent report finding that 80% of global cybersecurity leaders now consider ransomware a threat to public safety. Cryptocurrency has captured fraudsters' attention as well, with crypto-related fraud losses ballooning 79% year over year. BNPL-focused fraud has seen a similar increase, rising 66% between 2020 and 2021 as account takeover (ATO) attempts, phishing and other scams became increasingly popular on such platforms.

Protecting against rising fraud while supporting consumers' preferred alternative payment methods is a top priority, especially as they begin to demand stronger data protection. As schemes that rely on stolen user credentials proliferate, implementing identity authentication measures that do not rely on passwords and usernames to verify users' identities is a critical means of shoring up security.

This edition of Alternative Payments Tracker®, a PYMNTS and Socure collaboration, looks closely at the mounting concerns regarding emerging payment methods' security and data privacy. It also examines how upgrading identity authentication measures can help payment providers and merchants keep pace with developing fraud and cybersecurity threats.

Thought Leadership Team

PYMNTS.com

Feature Story

Why Identity Verification And Fraud Protection Are Key To **Alternative Payments' Growth**

THE PANDEMIC-DRIVEN DIGITAL SHIFT PROMPTED MANY CONSUMERS TO TRY NEW PAYMENT ALTERNATIVES WHEN SHOPPING ONLINE,

including mobile wallets and budget-friendly BNPL methods. Supporting alternative payments such as BNPL offers merchants an important opportunity to increase customer acquisition, according to Mike Jia, growth director for eCommerce platform CASETiFY, a phone case and accessory retailer. CASETiFY supports a variety of alternative payment methods, including mobile wallets Apple Pay and PayPal, and the company is currently working with installment payment service Klarna to provide BNPL solutions to CASETiFY customers.

"We hear a lot of requests from our existing fans talking about how they would love to pay in installments," Jia told PYMNTS in a recent interview. "They would love to buy higher basket sizes if only they [could make] monthly [payments]."

Enabling these capabilities promises significant growth, but digital identity verification has become increasingly critical as alternative payments' popularity extends to fraudsters as well. A surge in BNPL usage, for example, resulted in a concomitant rise in BNPL fraud between 2020 and 2021. This means that seizing this opportunity will require merchants to bulk up with robust fraud protection in advance.

ALTERNATIVE PAYMENTS AND ONLINE IDENTITY VERIFICATION

Identity verification in eCommerce is challenging, however, as convenience comes first for today's digital shoppers. Consumers want payments to be as easy and seamless as possible, Jia said, especially as more online shopping moves to mobile devices. They are migrating not only to alternative payment methods but also to shopping channels in which all their pertinent details are already on hand and just waiting for them to click "buy."

"We have noticed a lot of users have been requesting one-click checkouts, where all their information is saved," he said. "At one tap of a button, they can buy what they want, so that's something we're working [on] on our side."

This convenience can make it easier for enterprising fraudsters, too, unless retailers take proper precautions, but doing so can be difficult for merchants, especially when it comes to distinguishing between legitimate users of alternative payment solutions and fraudsters who aim to impersonate or infiltrate legitimate consumer identities. Many BNPL and mobile wallet options are not subject to the same level of regulatory or privacy standards as more traditional methods such as debit and credit cards, making it easier for fraudsters to access previously stolen credentials and pose as legitimate users via these alternative options.

Merchants must also keep pace with how mobile phone providers such as Apple are tightening privacy requirements to provide both seamless and safe experiences, Jia pointed out. Apple recently upgraded its data sharing rules in a bid to prioritize user privacy, meaning that much of the consumer data to which retailers recently had access is now obscured, he said. The move has also prompted more consumers to pay attention to how their payment details are being secured against digital fraud.

"Security is something that's always been top-of-mind for consumers, but especially after these recent privacy changes [have led to more] awareness in this space, we're getting a lot more feedback about how important it is that people know their credit cards are hashed and that they're secure," he said.

Implementing robust digital identity verification measures to protect emerging payment methods and channels is likely to become more important as consumers' online payment habits continue to evolve. Solutions that enable seamless and highly accurate verification not only protect consumers but also could help enable a better overall customer experience and therefore improve brand loyalty. Retailers wishing to grow via these channels thus need to be proactive about applying these solutions to alternative payment methods.

PREPARING FOR NEXT-GEN eCOMMERCE

Digital-first merchants can and should create more space for alternative payment methods that offer consumers greater financial flexibility. The success of subscription models, for example, showcases a consumer perspective that merchants should be considering, Jia said.

"We've seen a lot of subscription-based services and providers come out, so that might change the way consumers are thinking about transactions and payments in general," he explained. "It's much easier to have installments that [one] pays on a monthly basis as opposed to one big sum."

Emerging alternative payment methods such as BNPL require new and unique solutions for identity verification and fraud assessment so that merchants can support a safe, secure and convenient end-to-end commerce experience. Meeting consumers' new expectations for easy monthly payments may become eCommerce merchants' top priority in the next few years. Retailers must ensure strong digital identity verification and fraud protection no matter the payment method to make the most of this opportunity.

PYMNTS Intelligence

How Robust Identity Authentication Can Help FinTechs Meet Growing Cybersecurity Challenges

Today's consumers are tapping nontraditional banking and payment solutions more often, turning to neobanks or alternative payment solutions such as mobile wallets to conduct many of their routine transactions. BNPL alternatives have become the fastest-growing eCommerce payment method, for example, with PayPal reporting a 400% year-over-year jump in users of its BNPL solution during the Black Friday and Cyber Monday sales period in 2021. Research also points to rising usage of digital-only banks, including online bank Chime, which now boasts more than 13 million U.S. customers, up from 7 million at the start of 2020.

These emerging solutions can offer users convenience and speed, resulting in greater customer engagement and satisfaction, but their advantages can hide cybersecurity gaps that make them attractive targets for bad actors. The boom in BNPL usage, for example, coincides with a 66% surge in BNPL fraud between 2020 and 2021.

A lack of proper security or data privacy standards can ultimately erode trust and lead to customer dissatisfaction and abandonment, making it essential for alternative payment providers to upgrade their fraud protection measures accordingly. This month, PYMNTS scrutinizes the security weaknesses plaguing alternative payment methods. We also examine how adopting innovative and robust identity authentication solutions can help payment providers protect against increasing cybersecurity threats and fraud.

ALTERNATIVE PAYMENTS AND GROWING SECURITY CONCERNS

More and more consumers rely on digital channels for everything from banking to entertainment, and fraudsters are dogging their steps. According to one recent study, U.S. data breaches rose 38% from Q1 2021 to Q2 2021. Quarter over quarter, phishing and ransomware attacks remain the top two sources of stolen personal details, such as emails, passwords or usernames. These breaches feed the growing problem of ATO attacks, in which fraudsters use stolen credentials to mimic legitimate customers.

Despite having reputations as savvy innovators, many emerging and alternative payment services show security lapses. One recent report found that FinTechs such as neobanks and robo-advisers have an average fraud rate of approximately 0.30% on their platforms — nearly double the average 0.15% to 0.20% reported for traditional credit cards and triple the average of less than 0.10% for debit cards. Alternative payment methods such as BNPL

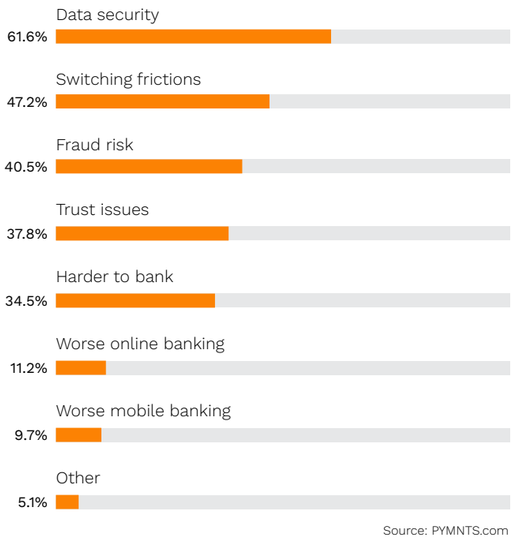
and cryptocurrency are also seeing higher levels of fraud as their solutions become more popular, leading to an erosion of consumer trust in fledgling services. A September 2021 PYMNTS report found that 25% of consumers cited data security concerns as the main reason for not using a digital or virtual-only financial institution (FI). Forty-seven percent named data security worries as their top deterrent to switching to digital-only entities provided by large-scale financial organizations.

Concerns regarding fraud are especially critical for digital-first entities, as legacy authentication methods remain prevalent even as they are proving less and less viable in protecting customers against breaches. Recent PYMNTS data showed that most consumers still prefer to use either credentials or static usernames and passwords to access their online accounts, despite rising security concerns. The research also showed that most consumers are open to using more secure, modern verification solutions, including two-factor authentication (2FA) and biometrics, offering FinTechs a pivotal opportunity to recoup and keep consumers' trust.

FIGURE 1:

Reasons for not switching primary banking services

Respondents who are "slightly" or "not at all" interested in making their primary bank a digital-only bank provided by a large organization



Source: PYMNTS.com

Share of consumers cited data security concerns as the main reason for not using a digital or virtual-only financial institution

Identity authentication solutions that tap new technologies such as AI or ML offer payment providers and merchants ways to keep their platforms secure while maintaining the seamless, personalized experiences their customers seek. Geolocation or biometric identifiers can help verify consumers' identities without adding unnecessary customer frictions. They also enable providers to rely less heavily on credit data to verify new users, a must for BNPL or mobile wallet providers with user bases that may include customers with limited credit histories.

Alternative payment providers have ridden the crest of the pandemic wave to become formidable players in the payments market, but one too many security shortcomings could topple their success. Providers and merchants looking to maintain longtime user loyalty should swiftly adopt cutting-edge authentication measures to oust fraudsters and keep their digital-first users transacting smoothly and securely.

NEWS & TRENDS

CRYPTOCURRENCIES AND FRAUD CONCERNS

RISE OF DECENTRALIZED FINANCE LEADS TO UPTICK IN CRYPTO SCAMS, LOSSES

Cryptocurrency-based scams became prolific in 2021, with fraudsters taking a collective of $14 billion — a record high for such losses. Digital currency crimes, driven by scams and theft, rose 79% year over year in 2021, according to one recent study, which also pointed to the growing popularity of decentralized finance (DeFi) in the crypto industry as a contributing factor.

DeFi refers to cryptocurrency platforms that are replacing legacy banks and legal intermediaries with "smart contracts," or bits of code that help support transactions. DeFi transaction volume skyrocketed 912% in 2021, the report found. Patching the security flaws on DeFi networks or implementing other cybersecurity and identification measures on cryptocurrency exchanges is thus becoming critical to keeping funds secure.

FI EXECS REPORT CRYPTO DATA SECURITY CONCERNS, LACK OF UNDERSTANDING

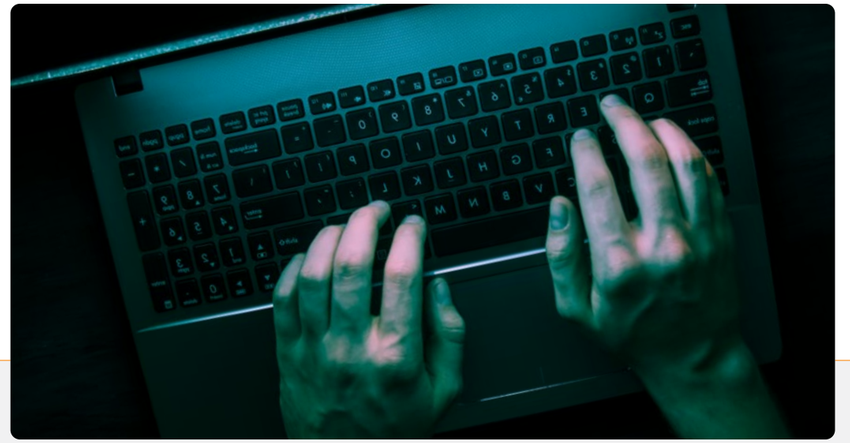
Players in the greater financial industry also report worries regarding cryptocurrency's safety. This factor could be contributing to legacy institutions' slow adoption of blockchain or crypto-related payment platforms or systems. One recent PYMNTS study found that 29% of FI executives cited data security as one of the primary barriers preventing them from adopting or creating such products. In addition, 27% of executives reported a lack of understanding of blockchain and cryptocurrency services, indicating that digital currency has several strides to make before reaching the financial mainstream. Education on cryptocurrency and solutions for bolstering its security appears to be essential for the sector to continue to advance.

ALTERNATIVE PAYMENTS FRAUD

EXPERTS URGE CONSUMERS TO BE VIGILANT OF RISING P2P PAYMENT APP FRAUD

Peer-to-peer (P2P) mobile payment apps are becoming integral parts of consumers' daily lives as the solutions prove convenient for everything from splitting restaurant tabs to paying large bills such as rent. Increased usage has made apps a favorite target of fraudsters, however, and financial experts are warning U.S. consumers to be wary of app scams.

Joe Fitter, a financial expert at the Kelley School of Business at Indiana University, recently explained that fraudsters sometimes pose as legitimate bank officials to message app users about suspicious bank transfers. These bad actors do this to try to trick customers into sending their financial and personal details to resecure their accounts. They can then use this information to access the accounts and attached funds. Implementing tighter security and identity verification measures such as 2FA is one way to oust these fraudsters and reassure legitimate users of P2P apps' safety.



BNPL FRAUD EXPANDS AS CONSUMER COMFORT, USAGE RISES

Consumers are also growing more comfortable with BNPL services as the installment payment solutions become more widely available. One recent report noted that mobile wallet provider PayPal saw a 400% jump in U.S. users of its BNPL solution, launched in August 2020, during the 2021 Black Friday and Cyber Monday retail period. Fellow BNPL provider Klarna reported a 141% rise in U.S. sales during the same time frame. These and other services are helping to make BNPL the fastest-growing digital payment method and consumer favorite for larger or more expensive purchases such as holiday gifts.

Fraudsters have followed consumers onto such platforms, however, with BNPL fraud growing 66% between 2020 and 2021. BNPL providers often do not conduct the routine credit and other financial checks that banking apps do, leaving openings for bad actors to pose as legitimate customers before making off with stolen funds or items. ATO attacks are also becoming a bigger concern for such platforms, with ATO attempt rates spiking during the 2021 holiday season.

BNPL FRAUD LOSSES WILL CONTINUE TO GROW, EXPERTS PREDICT

Finding robust fraud protection and identity authentication solutions should be top-of-mind for BNPL providers, as security and fraud protection experts expect the industry will continue to see growth in fraud volumes. Mike Cook, vice president of commercialization in fraud solutions for ID authentication platform Socure, recently predicted that BNPL providers will experience even greater fraud losses in 2022, with industry players looking to shore up their fraud protection measures as a result. Cook anticipates other forms of fraud will also increase throughout the year, including a bump in impostor scams, bot attacks and identity theft. Warding against all these forms of fraud is critical for alternative payment providers to stay competitive and keep customer and financial data secure.

CONSUMER TRUST IN FINTECH APPS GROWS, BUT DATA PRIVACY QUESTIONS ABOUND

BNPL, mobile wallet services and other alternative payment providers must watch how consumer behaviors shift to ensure that their customers remain engaged. One recent study showed that consumers are becoming more trusting of FinTech apps, especially regarding their digital security. Approximately 73% of individuals surveyed said they believe their personal data is private and secure on such apps. Many consumers lacked clarity around the apps' data privacy standards, however, with just 24% saying they were aware that FinTech apps could share their personal data with third parties. The report also found that 70% of users did not know FinTech apps could access their bank account numbers.

This lack of consumer awareness of data policy could undermine users' trust, especially as online fraud worries continue to grow. The study found that just 23% of users were aware that apps could keep personal data after it is deleted, for example, but 55% reported they would be uncomfortable with apps doing so. Shining a light on data privacy and security is therefore essential for the continued growth of FinTech apps.

Securing Alternative Payments

PYMNTS.com | Socure

How AI-supported identity authentication solutions can keep alternative payment methods secure

Consumers are turning to alternative payment methods such as BNPL or mobile wallet solutions more frequently, but with fraudsters following suit, how can merchants and payment providers keep such methods safe and seamless?

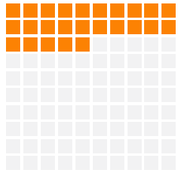
Digital-first consumers are becoming more security-conscious.

Consumers are growing more concerned about online security as digital transactions and fraud increase.

60%
Portion of consumers who would prefer to authenticate **using 2FA periodically for additional security**

10%
Share of consumers who reported fraud attacks **connected to their online credit or debit cards**

25%
Portion of consumers who cited data privacy worries as **their top reason for not signing up with a digital-only bank**

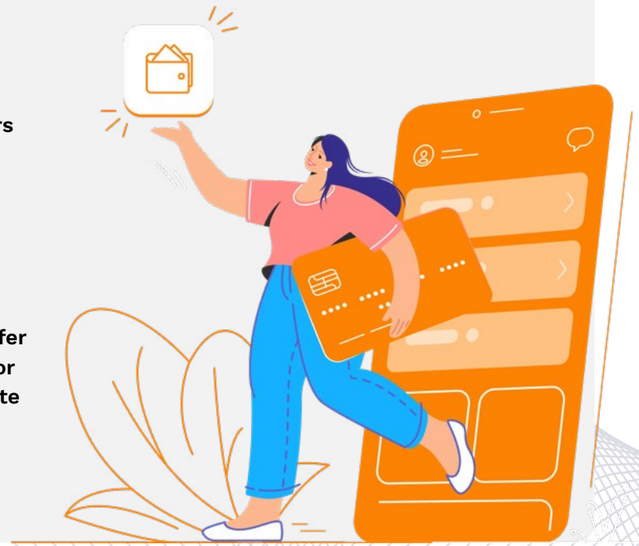


Mobile alternative payment use is creeping upward.

Consumers are turning to mobile banking apps or alternative payment solutions such as BNPL more often, but they are still relying on outdated, static authentication measures.

60%
Portion of U.S. consumers who prefer to bank via mobile apps

Most consumers still prefer to use static passwords or usernames to authenticate their digital accounts.



Upgrading security is vital for merchants and payment providers to keep users' trust.

Improving identity authentication or security measures in a way that matches users' expectations is critical for merchants and payment providers to keep alternative payments safe and seamless.

47%
Share of individuals who cited data security worries as the reason why they would not switch their primary banks to digital-only entities

73%
Share of consumers who want to select the identity authentication methods they use

ALTERNATIVE PAYMENTS TRACKER®

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 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.

Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from email, phone, address, IP, device, velocity and the broader internet to verify identities in real time. The company has more than 750 customers across the financial services, gaming, healthcare, telecom and e-commerce industries, including four of the top five banks, seven of the top 10 card issuers, three of the top MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers and more than 100 of the largest FinTechs. Marquee customers include Chime, SoFi, Varo Money, Public, Stash and DraftKings. Socure customers have become investors in the company, including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, Voyager and Synchrony. Additional investors include Accel, funds and accounts advised by T. Rowe Price Associates, Inc., Bain Capital Ventures, Tiger Global, Commerce Ventures, Flint Capital, Scale Venture Partners, Sorenson, Two Sigma Ventures and others.

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