Building a Better Approach to BNPL Fraud

Vanguard Report

May 2022

Commissioned by

callsign®

451 Research

S&P Global
Market Intelligence

About the Authors

Jordan McKee

Principal Research Analyst, Customer Experience & Commerce

Jordan McKee is a Principal Research Analyst for Customer Experience & Commerce, leading the coverage of the payments ecosystem at 451 Research, a part of S&P Global Market Intelligence. He focuses on the digital transformation of the commerce value chain, with an emphasis on the major trends and technologies impacting payment networks, issuing and acquiring banks, payment processors and other payments industry stakeholders. His research helps vendors and enterprises assess and address the implications of the ongoing digitization of the shopping journey.

McKayla Wooldridge

Associate Analyst, Customer Experience & Commerce

McKayla Wooldridge is an Associate Analyst for Customer Experience & Commerce at 451 Research, part S&P Global Market Intelligence. McKayla's coverage focuses on digital payments and various topics within the fintech ecosystem.

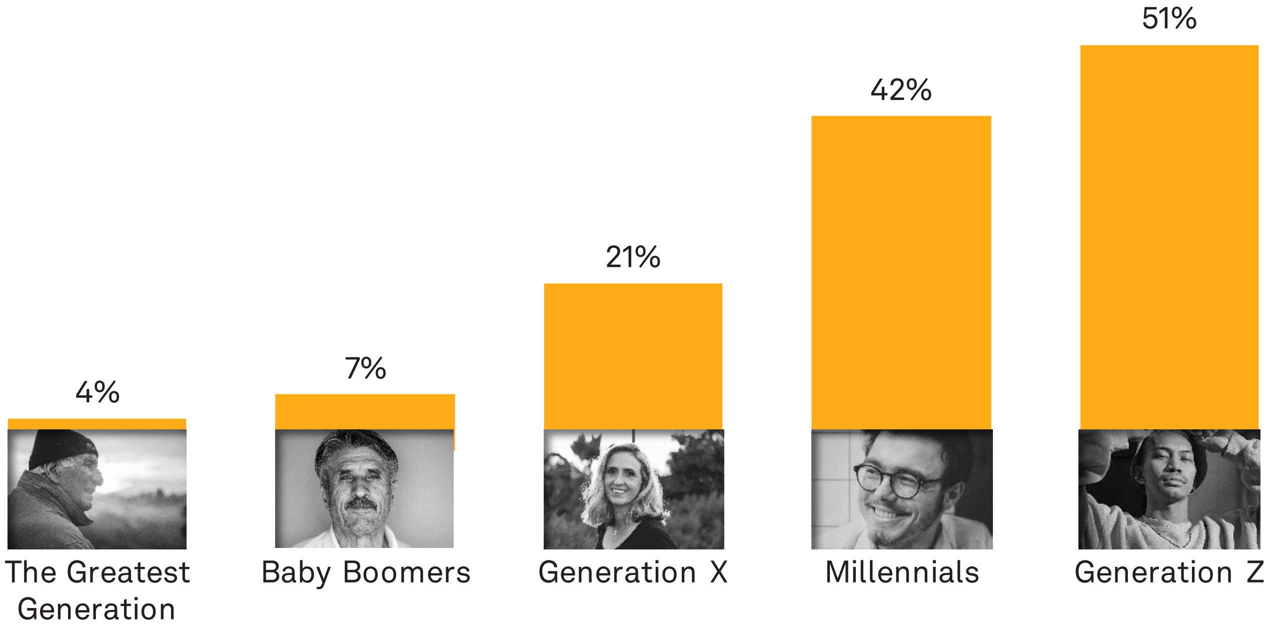
Introduction

Buy now, pay later (BNPL) is rapidly gaining momentum in many markets around the world. More than 100 BNPL providers have emerged globally, igniting a land-grab for merchant and consumer adoption. In the U.S. alone, one in four consumers (26%) have used BNPL at least once in the past six months, rising to 51% of Gen Z and 42% of millennial shoppers, according to 451 Research's Q3 2021 Voice of the Connected User Landscape (VoCUL) survey.

As is always the case in payments, with growth comes fraud. BNPL providers are quickly finding that their account opening flows are being targeted by fraudsters. Concerningly, the emphasis on user-base expansion and rapid scale has led many BNPL providers to prioritize growth over fraud prevention, leaving multiple blind spots and entry points for exploitation. This has exacerbated the problem and left the door open to losses and, inevitably, regulatory scrutiny.

Getting a handle on BNPL fraud during a period of accelerated growth requires a strategy that doesn't compromise the user experience. Focusing on digital identity is imperative to better understand user intent and the risk level associated with each interaction, while minimizing friction. Without a complete understanding of the identity behind each user, BNPL providers will be challenged to fend off growing instances of new account fraud and account takeovers (ATOs).

Figure 1: Consumer BNPL Usage Over the Past Six Months



Q: In the past six months, how many times – if any – have you used a "buy now, pay later" service to make a purchase (e.g., Afterpay, Klarna)?
Base: All respondents (n=1,299)
Source: 451 Research's Voice of the Connected User Landscape: Connected Customer, Quantifying the Customer Experience 2021

The Take

As the BNPL market accelerates, fraudulent activity and losses will follow. While the financial repercussions are problematic, the long-term consequences are even more concerning. Fraud jeopardizes consumer trust and may ultimately undermine the long-term potential of the BNPL ecosystem. Furthermore, the growth – and fraud challenges – associated with BNPL are inviting regulatory scrutiny, including from the Consumer Financial Protection Bureau in the U.S. and the Financial Conduct Authority in the U.K. BNPL providers need to shore up fraud prevention and account opening processes before regulators begin to take more drastic action.

Aside from improving consumer education on security best practices, BNPL providers must take steps to enhance their understanding of the identity associated with each user interaction and the extent to which it can be trusted. Layering in approaches such as device fingerprinting, behavioral biometrics and location analysis helps to build a more comprehensive understanding of the risk level associated with each user. Through a deeper understanding of users' digital identities, BNPL providers can make more informed and accurate decisions during onboarding, login and payment. Aside from stopping fraud, this can also help to drive down false decline rates.

Ultimately, leveraging identity data in conjunction with a digital identity network puts BNPL providers in a position to better secure the end-to-end customer journey without compromising the user experience. BNPL providers should consider aligning themselves with partners that have built robust identity networks because they will be in a strong position to compare user attributes to similar attributes – and associated outcomes – previously seen across their network.

Unpacking BNPL Fraud

Fraud has become a growing concern with BNPL. There are two primary factors that make BNPL an attractive target for fraudsters:

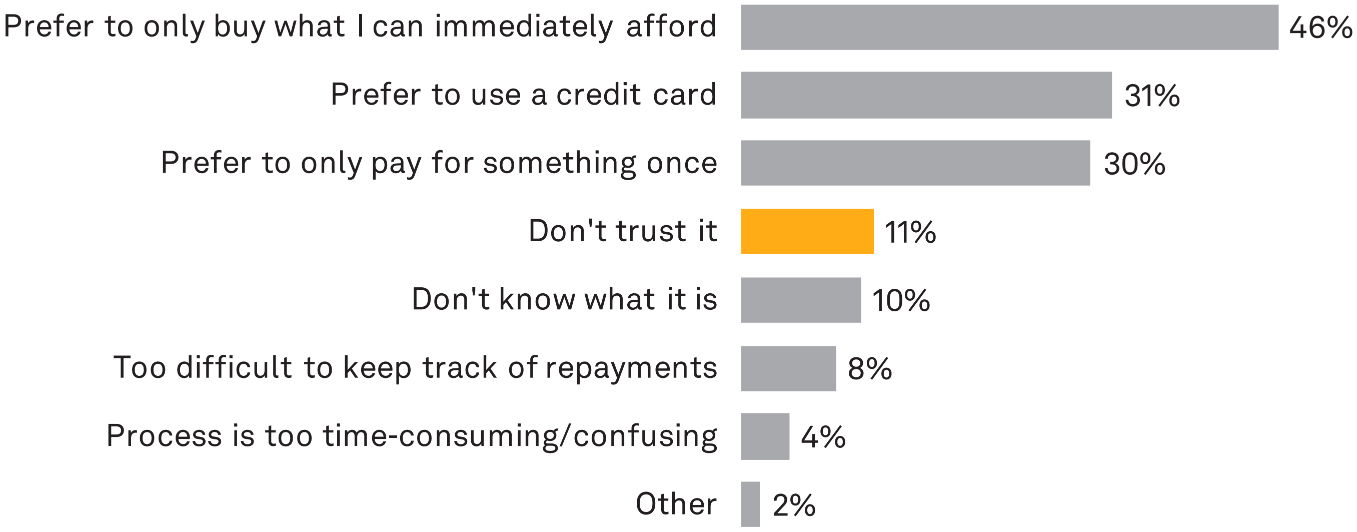
- **Simplicity of account opening:** BNPL providers pride themselves on the ability for users to create accounts quickly with limited personal information. There is generally no credit check (many BNPL users have thin-file or no-file credit histories), and providers often fear being too stringent during onboarding to avoid turning new users away at a time when scale is critical. Adding to the challenge, criminals can often go undetected using the same information to open multiple accounts across multiple BNPL providers.
- **Deferred payments:** BNPL providers generally only take a portion of the total payment amount up front. This leaves the door open for bad actors to make one payment and disappear. Since payments are smaller and often spread out over six to eight weeks, a cardholder whose card is being fraudulently used in a BNPL account may not notice for an extended time, and long after the fraudster has caused significant financial damage.

Most BNPL fraud is occurring at the account opening stage, where fraudsters are exploiting poorly protected application processes. Limited information collection and lack of credit checks have resulted in a breeding ground for new account fraud and synthetic identity fraud. This has created an attractive way for fraudsters to leverage stolen payment credentials obtained through data dumps on the dark web.

Account takeovers represent another pertinent issue. Because charges only occur every several weeks, it may take longer for consumers to realize their account has been taken over. Adding to the challenge, Gen Z consumers – the most widespread users of BNPL services – have the worst online security hygiene of any generation, with 1 in 10 stating they do nothing to protect their personal information online, according to our Q2 2021 VoCUL Trust & Privacy survey.

Both new account fraud and ATOs result in chargebacks for BNPL providers. The negative implications of this are many, including chargeback fees, losses, operational distractions and higher processing rates the BNPL provider must pay to its payment service provider (thus reducing its margins). Failure to prevent fraud also undermines consumer trust – a factor that already ranks as a top five inhibitor to BNPL adoption, according to 451 Research's Q3 2021 VoCUL survey. Further, excessive fraud may also result in damage to BNPL providers' merchant relationships, given the propensity of consumers to place the fraud blame on the merchant, regardless of which party is at fault. It's also plausible that unsavory BNPL users may abuse merchants' business policies (e.g., return abuse), driving up their operational costs.

Figure 2: Adoption Inhibitors for BNPL



Q: Why have you never used buy now, pay later? (Check all that apply)
Base: Respondents who never used “buy now, pay later” (n=560)
Source: 451 Research’s Voice of the Connected User Landscape: Connected Customer, Quantifying the Customer Experience 2021

The true challenge for BNPL providers comes in ramping up fraud-prevention processes without compromising their user experience and approval rates. Successful execution requires establishing a level of trust in each interaction at each customer touchpoint.

Trust is predicated on an understanding of identity. Harnessing a combination of identity signals (e.g., geolocation, account age, trusted ID, login velocity), augmented with device fingerprinting and behavioral biometrics inputs, enables BNPL providers to make more informed decisions during onboarding, login and payment. Incorporating user behavior inputs (e.g., has the user ever spent this much before? Shopped at this merchant? Been associated with this IP address?) is also imperative to identify ATO scenarios.

Digital identity networks help BNPL providers take action on identity data. They help to establish trust by determining the behavior and outcome associated with the same (or similar) combination of identity attributes that have appeared elsewhere in the network. For example, if an email address or mobile device has been used with combinations of different identifiers (e.g., address, phone number) and behaviors at other businesses, this may be flagged as suspicious identity. Similarly, a U.S.-issued debit card added to a new BNPL account from a user with a Brazilian IP address could be indicative of new account fraud.

A key benefit of an identity-based approach to fraud is precision targeting of individual instances of suspicious or abusive behavior. This helps preserve the user experience for good customers by ensuring friction is only introduced when risk levels warrant it. For instance, a login with a suspicious identity can be stepped up with behavioral biometric inputs (e.g., keystroke analysis), which are less intrusive for the user and can help prevent fraud stemming from stolen account credentials (e.g., passwords, traditional PINs) and SMS one-time passwords (e.g., via phishing, SIM swapping). Digital identity has similar applicability for merchants. BNPL providers can use digital identity to help their merchants better identify repeat abusers of business policies (e.g., returns) and dynamically present them with more stringent policies (e.g., no free returns).

Conclusion

For BNPL providers to build sustainable, long-term growth, they must start by creating trusted interactions at every step of the customer journey, from account opening to login to payment. Failure to generate trust will increase regulatory pressure and compromise their customer relationships, bottom line and market potential.

With much of BNPL fraud occurring at account opening, BNPL providers need to develop a more complete view of each user interaction. Given that data collection is limited during enrollment, BNPL providers must rely on digital identifiers to build a more robust view of the level of risk associated with each interaction. Behavioral biometrics and device fingerprinting harnessed in conjunction with digital identity networks help to build more complete views of user risk and intent.

Ultimately, a deeper understanding of digital identity puts BNPL providers in a position to make more accurate decisions (reducing losses and false declines), while ensuring that legitimate users' journeys are streamlined and uninterrupted (helping drive loyalty and improved customer experiences). As a starting point, BNPL providers should consider aligning with partners that have tools to compile insights on their users' identities and make determinations on the risk levels associated with those identities.

callsign®

This report was commissioned by Callsign, which makes digital life smoother and safer by helping organizations establish and preserve digital trust so that people can get on with their digital lives. If you'd like to read more on this topic, the following report looks at the consequences of fraud for BNPL services, how it affects consumer trust and the impact it has across BNPL providers, merchants and banks.

Visit https://www.callsign.com/knowledge-insights/bnpl-research-report-2022 to download the report, or email charlie@callsign.com to talk to Callsign directly.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.