Is Buy Now, Pay Later a Fraudster's New Best Friend?

Editor's Note: This guest blog post is written by Alexander Hall, principal at Dispute Defense Consulting and a reformed fraudster.

Business trends are constantly emerging and evolving. Starting in 2020, we all witnessed a categorical shift from in-store to ecommerce due to the Covid pandemic. Next, we saw crypto becoming more accessible via familiar channels, the most notable of which being PayPal. This was followed by crypto for payment with merchants, followed by NFTs exploding onto the scene. Now we are seeing loads of data relevant to buy now, pay later (BNPL). New service providers are offering it as their primary function, and merchants are excited to add another payment method to their array of options.

Here are some key things everyone should know about BNPL …

What Is BNPL?

Simply put, "buy now, pay later" is a payment method. I've outlined the user experience for a typical ecommerce merchant employing BNPL here:

1. The customer builds a cart on the merchant site and proceeds to checkout, selecting "buy now, pay later" as their payment method.
2. A new window pops up, asking the user to create an account with the BNPL service provider.
3. The user provides the requested information (e.g., personal information such as name, address, phone number, email, etc.) and establishes an account with the BNPL service provider.
4. The total amount of the order is split into payments. Some providers require the first payment at this point.
5. The merchant fulfills the order, and the user makes the payments directly to the service provider.

The customer-facing part of the process is to interact with. It offers a great value to consumers by allowing them to make large purchases with manageable payment arrangements. It's similar to financing but without the credit check.

Behind the scenes, there are many moving pieces that set this payment method apart from the others.

For example, unlike traditional transactions, the funds that the merchant receives for these orders do not come from the customer at all. When an order is placed, the BNPL provider sends the full amount to the merchant and bills the customer directly for the payments. This is very important to note for two reasons:

1. Chargebacks/disputes are received by the provider. Not the merchant.
2. Unpaid bills are between the provider and customer.

Both items have impacts on the relationship between the merchant and provider, which can result in warnings, limitations and even termination of service.

We've covered the perspective of the user and the merchant. Now let's move onto how fraudsters attack this payment method and what merchants can do to protect themselves.

Fraud Vulnerabilities at Play With BNPL

1. Establishing accounts leveraging stolen identity information and making first payment with stolen payment information.

In this method, the fraudster would use a set of verifiable identity information aggregated from any number of sources to create the two accounts. One at the merchant and another with the provider. The fraudster goes through the process, and uses a stolen card to make the first requisite payment.

A fraudster who works with identity information typically has limited options available when it comes to using sets of identity information with low credit scores (low-value profiles).

Typically, high-value profiles are manipulated over time and can result in high-dollar credit lines/financing, while low-value profiles are used to open accounts for depositing checks, wire transfers, setting up third-party accounts for money laundering and more. BNPL has opened a new door, allowing fraudsters to use these low-value profiles in a way that can be easily monetized.

2. Account takeovers (ATOs) for accounts with stored payment information.

In this method, the fraudster would exploit the disconnect between departments/systems to use a set of data obtained through one of their channels, along with social engineering in order to gain access to an account and enact transactions.

This can be accomplished in several ways.

- By logging into active accounts using recycled login credentials found in a set of data obtained through a breach.
- By contacting customer service directly and gaining access by providing identity information, meeting all the requirements of a change and updating contact information.
- By attempting to log in using accurate credentials and scamming the account holder to obtain the one-time password or two-factor authorization code.
- By making a new account and employing a different tactic at the customer service level resulting in old accounts being deactivated. This would be effective at the merchant level in order to leverage stored payment information on the provider's platform.
- … and the list goes on from there.

How Can We Limit Exposure to These Methods?

We need to put conscious thought toward one idea here.

Identity information is just as important to the user as it is to the merchant, as it is to the service provider, as it is to the fraudster. The entire premise of this payment method is to leverage identity information in order to offer payments for purchases that otherwise wouldn't be available to a customer.

So, it's important to identify our challenges and provide our teams with insight and tools that can identify suspicious activity. Our challenges exist at several touch points across the customer experience journey. A journey that is now being stretched across two loosely connected systems (the merchant's platform and the provider's platform).

What we need is something that can adapt, be implemented at different points, be referred to for chargebacks and provide expansive global data for accurate determinations and winning representations.

Payment data doesn't come into play until the card info is entered into the system of the service provider. That's too far down the line. Device ID Data works at all the touchpoints but doesn't paint a full enough picture. Asking a customer to provide documents is high friction and time consuming.

The answer is expansive personal identifiable information (PII).

What Makes PII Effective for Prevention?

When compared to other sets of data, PII is more expansive. Thousands of pieces of information can relate to a single identity, ranging from social media, phone numbers, emails, IP address geolocation, known associations such as family members and friends, street addresses and more. Additionally, PII can be leveraged at every touchpoint across the customer journey.

As I mentioned above, the gap between the merchant and the provider is important to note. This means that the merchant has less of a chance to make any determinations prior to allowing the user to move forward with their BNPL purchase. A few strategy items to consider are:

- Suspicious accounts do not have access to the BNPL option. This forces questionable accounts to complete their orders exclusively within the merchant system, which allows analysts to monitor their actions closely.
- Escalate certain suspicious actions to a team for research.
- Customer service can leverage these data sets through manual searches and see the information necessary to grant different requests. This is empowering against social engineering.
- Identify ATOs through historical geolocation. This works for identifying that a woman is at her parents' house for the weekend, as well as it works for seeing the fraudster in Ohio trying to access an account from California.

Every merchant's goal is to strike the balance between securing their operation and offering as little friction as possible to their customers. Expansive global data sets provide the accuracy that is required—especially in today's environment where potentially risky new payment methods such as BNPL are gaining popularity.

Merchants wanting to securely employ new and popular payment methods such as BNPL need to look beyond traditional fraud-prevention methods. Effective use of identity information across the customer journey is key. Learn how our identity trust solutions can help.