How address verification benefits digital identity verification in fintech

loqate
GBG

Contents

Fintech: Payments and crypto

The payments industry is exceptionally heavily regulated in many different ways.

Payments companies need to ensure that their systems are not being used for terrorist financing or money laundering elements. Therefore, practices that enable AML (Anti-money Laundering) and KYC (Know Your Customer) compliance are essential in this area.

For crypto wallets and exchanges, this is also incredibly important, particularly given the perception that cryptocurrency's anonymity can be used to mask fraudulent and criminal activities.

Outside of this, the ever-present threat is fraud, with there being endless fraud risks, such as account takeover fraud for wallets or scammers trying to convince users to make fraudulent payments. These highly complex pressures mean that digital identity verification is vital in this sector and must be considered a priority.

Address verification adds a layer that can and should be imbedded into the identity verification flow to enhance and improve the ability to verify and further mitigate risk. In fact, as more and more customers purchase online, an increasing number of merchants requiring the credit card number, name on the card, Card Verification Value (CVV) code, zip code and/or full address.

Especially relevant when a physical card is not present, a verified address helps to increase the chances that the customer is the actual cardholder. Address verification helps add an extra layer of security.

AVC: Address verification produces an AVC or Address Verification Code that provides levels of verification from micro delivery-point match to a more macro level or street or city or state that matches customer information with the information on file with the card issuer.

Payment companies can set the level of approve or decline based on their custom risk tolerance levels using the AVC.

Industry identity verification situation, why address matters

The payments industry faces a problematic identity verification situation, given how ubiquitous payments are.

Payments are a part of all our daily lives, whether these are scheduled payments through banks, card payments online, in-person payments via cash, QR codes, contactless card or mobile, or even crypto payments. Given the absolute ubiquity of payments, ensuring that fraud is minimized via digital identity is a highly challenging proposition.

Payments companies need to ensure that they follow KYC regulations and identify the customers using their services. Challenges have multiplied as payment services have multiplied to include elements such as digital wallets, which can contain multiple payment methods. What was a simple proposition, where a bank account was generally the source of payments and managed by the bank, has spiraled into a system where payments can come from any source, massively complicating matters.

The digital nature of these payment types means that identity also needs to be verified digitally. Suppose a user loses their mobile device, for example. In that case, wallet services need to ensure that the device cannot authorize transactions immediately without additional checks.

Providing a secure experience to the user will be a major driver for using services such as mobile wallets, which can leverage address data, biometrics and other elements. These services must employ the maximum level of digital identity verification possible to meet user expectations. Address verification should be integrated into the digital identify verification process to deliver both an added security layer to prevent fraud and help deliver greater customer experiences by making it easy to enter and capture a verified address during onboarding.

Providing a secure experience requires a balancing act versus friction. Getting this balance right is difficult and requires leveraging the correct verification tools and strategies. By creating a robust yet user-friendly onboarding process, payment services can create a competitive differentiator. However, there is risk in not doing this correctly. Ineffective identity verification processes can lead to losses in new customer acquisition and friction during the onboarding experience. This is critical, as this does not create an excellent first impression for the potential user relative to engagement and trust, which is highly important for all industries in this rapidly digitizing payments world.

Industry use cases & considerations

There are several different use cases and considerations for payments and crypto in digital identity verification where address verification can add value. These are explored below.

Onboarding for payments services

Digital payments services, such as cryptocurrency exchanges and digital wallets need to onboard and verify users in a purely digital way. This means doing all the required elements, such as KYC, AML, checking against sanctions lists, etc., in a digital-only environment, which can be challenging.

This means needing to design a UX that is inclusive of digital identity verification at its core, with access to multiple verification layers that can be deployed in each required scenario. Address capture or type-ahead auto-complete can be integrated into any single address field to remove friction and limit errors at the point of new data creation. In three keystrokes or less, address capture will suggest a complete and accurate address to the user and autocomplete it in relevant fields as part of onboarding for a payment service.

Data diversity and consortium networks

Central to the requirement for effective digital identity verification is data diversity – payments and crypto vendors must be able to access enough data to know that user onboarding information and their behavior is unusual. Incorporating other identity verification data sources, such as an address, is essential, as the more indicators are used, the more robust the system is compared to a traditional system reliant on credit checks, which can be breached.

The other consideration is data transparency – data must be sourced and explained, as a critical requirement for ongoing regulatory compliance, and justify decisions to customers. Data sources used as part of the identity verification process must be known to be accurate and verified, trustworthy.

This is where the idea of consortium networks, where data is shared between a large network of interconnected parties, becomes highly important, as they enable new account openings at different institutions to benefit from fraud data and learnings elsewhere in the ecosystem; securing the whole market more effectively. No customer or business record is complete without an address, making address data a perfect checkpoint between institutions.

Ongoing verification

Onboarding is an important element of fraud prevention, but ongoing verification is necessary, which is the authentication part of the equation. Opening a fraudulent account is a risk, but account takeover of an existing account is also a significant risk, as payment accounts have access to make payments and view transaction history and payment details.

The requirement is for payments vendors to design strategies that ensure that verification is carried out continuously. This could be when an unusual transaction is made, or when a new payment method is set up, or in any number of given scenarios. Address verification, where an address is parsed, matched, formatted, transliterated and enriched by appending key elements such as geocode coordinates can play an ongoing key role.

Address verification capability embedded into the backend system of a payment service enables ongoing management of millions of records stored across multiple date entities. Customer data decays at a rate of 30% per year and needs to be continuously managed to maintain it as a reliable and trusted layer of the identity verification flow.

New payment types

This market is in a state of rapid evolution – payments have not stayed stationary. New payment types, such as cryptocurrency, Open banking payments, or biometric cards present new challenges compared to older payment systems.

As such, payments vendors need the flexibility to deal with changes in the market, rather than just having fixed tools that support current use cases. Next generation address verification capabilities built on modern deployment architectures can easily be integrated into any application and environment that new payment types may use.

Pain points for identity verification

As with any industry, there are specific pain points in payments and crypto around digital identity verification where address verification can add value. These will be outlined below.

Integrating with existing infrastructure

To date, much of the payment industry's technical infrastructure is highly complex. Also, the main difficulty is that payment systems are always inflight: payments are being made all the time. Services cannot be interrupted to update how systems work, meaning that integrations have to be well tested and easy to deploy.

Due to these challenges, models which focus on easy to integrate APIs and dashboards that can make changes, rather than relying on code changes, will reap the biggest rewards in the payments vertical. Modern global address verification solutions that are installable and SaaS based products that are easily deployable, cloud agnostic and highly performant (example: deployed via Helm Charts on any Kubernetes (K8s) based environments) are optimal for integrating into existing infrastructures.

The rise of synthetic identity fraud

Of all the fraud types currently prominent, synthetic identity is the biggest concern for payments vendors. Synthetic identity, fueled by a very high level of data breaches, can bombard verification systems with plausible looking identities, meaning that verification strategies need to advance in order to secure against this risk.

Over time, the use of machine learning will be increasingly critical in combatting synthetic identity fraud, which is important, given that synthetic identity will attract increasing attention from regulators. Combining identification methods that include address verification with powerful machine learning-based analytics is the best way to offset this risk and secure the highest risk transactions.

Using machine learning in the right way

The use of ML (Machine Learning), as opposed to the general term of AI (Artificial Intelligence), is highly important within payments. The scale of payments being made over time means that ML is the only way to cope with these requirements.

This is a problem when many ML models in use today are difficult to understand when it comes to reasons for making decisions. Therefore, the inability to explain decision-making has been a limiting factor for the use of automation within any heavily regulated industry.

This means that using ML within the payments sector requires a careful approach, which balances these needs and still leverages rules-based systems combined with human intelligence. Aside from ML bias which is both a regulatory and brand risk, there are dangers in using vendors who utilize 'ML-only' technology, specifically related to the governance of changes to the ML decision engine.

When the model changes, these changes are applied to the engine itself, impacting multiple customers across multiple industries, resulting in false positives and more fraud. This said, the application of AI and ML to supporting data services such as address verification can yield benefits without exposing the entire identity workflow to risk. For example, modern address verification capabilities will use AI and ML to help recognize, parse and standardize addresses, yielding improved verification rates, speed and throughput.

Cryptocurrency and identity verification requirements

In the payments industry, adding cryptocurrency into the equation can be an additional challenge. Cryptocurrency is undoubtedly still in its early stages, with its best use cases still emerging.

Cryptocurrency payments services must be backed by robust identity verification to ensure that it can still comply with AML and KYC regulations. As such, the introduction of digital identity verification into crypto wallets and exchanges is an essential requirement. Adding a layer that includes address verification enhances the capability and efficacy to identify and prevent fraud.

Industry-specific needs and settings

Payments have highly specific requirements based on the scale and the trends that are influencing them. These will be examined here.

The need to support massive scale and diversity

Digital payments are more diverse than ever, with payments being leveraged in every conceivable corner of the digital economy. As such, digital identity verification must be suitable for all these use cases.

This means that not only do systems need to be capable of handling massive scale, they also need to be able to cater to different requirements. Having a truly global solution is critical to meeting cross-border needs at scale. In the case of address data, being able to integrate one (1) API to enable verification across 250 countries/territories/possessions, 6500 spoken languages and 130 different address formats is critical to supporting required scale and diversity.

To ensure effective verification, the best way to operate is to utilize multiple layers of identity verification together, in an effectively orchestrated platform. This will enable an improved anti-fraud performance, while enabling transparency around which layer of fraud verification has been triggered, which is important for transparency.

Of critical importance here is customizability – by being able to tune the different verification layers and how they interact, banks can gradually improve fraud detection, while allowing more good business in by reducing fraud.

The need to prevent account takeover fraud

Digital wallets are becoming increasingly central to the financial lives of numerous users worldwide, meaning that if fraudsters take them over, this can lead to severe challenges.

In practice, this means having a combination of verification methods and a wide-ranging level of data diversity. If this is lacking, payments vendors can miss the fraud signals they need to prevent fraud techniques, such as account takeover fraud. It also highlights how critical behavioral checks and ongoing verification are in the payments and crypto space. Here again, having a global address verification layer as part of fraud prevention provides an added point of security.

Future outlook and requirements

Prediction is that payments and cryptocurrency will be an essential market for digital identity verification introduction and innovation over the next 12-24 months.

Payments is such a diverse and complex area that serves so many interests. If vendors fail to implement robust systems based on more than just point solutions for identity document scanning, they will struggle to deal with evolving fraudster tactics.

For this reason, we will see the continued fusing of physical and digital attributes for verification, such as taking name, address, date of birth, etc. It will also be fusing it with IP detection, email and mobile analytics, enabling better decisions to be made. Only by taking a multi-layered, customizable approach will banks achieve the best anti-fraud and customer experience outcomes.

Partner with Loqate to integrate global address capture and verification solutions

Loqate enables its fintech partners to integrate and leverage its global address verification APIs into their identity verification and customer onboarding applications to deliver enhanced capabilities and superior CX.

Our partner program is designed to allow our partners to offer, build or enhance their solutions across a variety of applications. Fintech partners can bolster their identity verification and fraud prevention capabilities while delivering frictionless onboarding experiences for their customers by leveraging our market-leading address verification, address capture predictive type-ahead technology, geocoding, email and phone verification products.

The world's leading global software companies integrate Loqate's solutions into their applications or resell our solutions worldwide. Read how NCR benefits from partnering with Loqate.

To learn more about our offerings or discuss your requireme contact our Partner Team.

loqate
GBG