ESSENTIAL GUIDE TO

Digital Payments Compliance

jumio

STAYING ON TOP OF DIGITAL PAYMENTS TRENDS

Digital payments are not only a reality — they are the future.

At the same time, digital identity usage is accelerating, with the global digital identity solutions market expected to reach US$147.25 billion by 2032.

This increase in digital payments owes itself to rising identity and authentication fraud, as well as digitization trends with increased integration of biometrics in smartphones. Here are some key insights according to research by Jumio and other industry experts.

CONSUMERS LACK CONFIDENCE

Despite more consumers demanding digital identity solutions for online verification when engaging with companies, they are not confident that all businesses are doing everything they can to protect their online accounts.

1/3 BELIEVE THEIR BANK HAS INCREASED ONLINE IDENTITY VERIFICATION

Only one-third (34%) of consumers worldwide believe their bank has implemented more online identity verification checks since the pandemic to protect them against online fraud and identity theft.

57% FREQUENTLY USE THEIR DIGITAL IDENTITIES ONLINE

Over half (57%) of consumers worldwide now use their digital identity "constantly" or "often" to access their online accounts following the pandemic. Consumers in Singapore reported the highest level of digital identity use (70%) as opposed to those in the UK (50%), the U.S. (52%) and Mexico (55%).

MAJORITY THINK DIGITAL IDENTITY IS IMPORTANT FOR FINANCIAL TRANSACTIONS

Over two-thirds of consumers worldwide (68%) think it's important to use a digital identity to prove they are who they say they are when using a financial service online due to the high monetary transactions involved. A 2022 study revealed that cybercriminals are attacking a wider set of payment methods and driving up the cost of fraud to new highs. The rise of synthetic identities is also identified as the most common source of identity verification issues.

HALF SAY IDENTITY VERIFICATION SHOULD BE A PRIORITY FOR CRYPTO

About 50% of global consumers think crypto companies and cryptocurrency exchanges need to make accurate identity verification a priority. This is because users can trade certain tokens anonymously. The cryptocurrency frenzy is also creating a lucrative environment for fraudsters. Case in point: in just the last decade, users were scammed out of nearly $5 billion in cryptocurrency, with another $3 billion stolen through security breaches.

OVER 2/3 ARE OPEN TO USING ONLINE IDENTITY VERIFICATION

Over two-thirds (68%) of consumers are open to using a digital identity to verify themselves online. Financial services is the main sector, where 43% of consumers agree they would prefer to use a digital identity over a physical ID like a driver's license or passport.

5 TRENDS SHAPING THE FUTURE OF DIGITAL PAYMENTS

1 EMERGING PAYMENT METHODS

The payments landscape has been transformed by new digital methods for making transactions and managing payments. Estimates show an increase of 83% in digital wallet spending by 2025, reaching $10 trillion.

New technologies are also creating the potential for new means of payment to emerge, including tools such as digital currencies, e-wallets and Buy Now Pay Later (BNPL). The value of digital wallet transactions, for instance, is expected to grow 60% by 2026 globally.

2 CRYPTO PAYMENTS

Cryptocurrencies could be a potential game changer as attitudes and perceptions change worldwide. Recent reports show over $12 billion transferred across Bitcoin, Ethereum and Litecoin blockchains daily, representing some 1.5 million transactions per day. Blockchain is getting a lot of attention because it helps combat fraud in crypto payments by providing greater transparency and traceability, but there's also increasing awareness that a robust Know Your Customer (KYC) process is essential.

3 FINANCIAL INCLUSION

Even in developed countries, many people remain underbanked or unbanked. For example, more than 13 million adult EU citizens still lack access to formal financial services, and in some parts of the EU, the percentage of those who remain unbanked is over 30 percent. Organizations must back innovation to tackle exclusion.

Bulgarian fintech iCard uses Jumio Identity Verification to simplify and speed up onboarding while also defending against fraud: "It was important that our online identity verification solution allowed us to strike a balance between identity fraud detection and the ideal user experience that matches our risk configurations and customer base. With Jumio we have less fraud and have significantly increased conversion rates." Gabriela Anastasova, Head of Product Definition, iCard.

4 CROSS-BORDER PAYMENTS

The global cross-border payments market is rapidly growing and is expected to reach $356.5 billion by 2032. This has been driven by trends such as borderless ecommerce and global trade improvements.

For example, Regulation 924/2009 on cross-border payments reduced the cost of all intra-EU payments in euros and unified the single payment market for consumers and businesses. In Asia, several countries are exploring cross-border payment arrangements.

5 INCREASING ONLINE FRAUD AND CYBERATTACKS

Ecommerce losses to online payment fraud have significantly increased and are estimated to reach $362 billion globally between 2023 and 2028.

Protecting transactions is crucial, not only to safeguard merchant revenues but also to reassure customers about the safety of their data and build trust. Customer trust is invaluable, and once lost, it's challenging to regain. The significance of preventing fraud is evident from the fact that 43% of businesses are worried about how ecommerce fraud affects their brand reputation, up from 26% in 2020.

KEY REQUIREMENTS FOR FINANCIAL COMPLIANCE

KNOW YOUR CUSTOMER

The first step in preventing financial crimes is to Know Your Customer (KYC). This means verifying the identity of your new customers when they set up an account with you, ensuring that they are who they say they are.

It also means assessing the risk they pose to your business by screening them against watchlists. For example, if they are a politically exposed person (PEP), you might apply more stringent checks during onboarding and monitor their activity more closely on an ongoing basis, whereas if they are on a sanctions list you would avoid doing business with them altogether.

DATA + BIOMETRICS (RECOMMENDED APPROACH)

Minimally, Know Your Customer compliance needs to include self-reported data such as name, birthdate, address and phone number during the onboarding process. This information is then checked against various data sources including bank records and credit bureaus to prove identity.

While this process validates that such a person or company exists, it does not always prove the applicant is not an imposter.

Biometric identity verification adds a more sophisticated level of security. It requires the user to send current photos of their ID documents and take a selfie to compare to the photo on the ID document. A smartphone and an internet connection are all that is needed. And when combined with advanced liveness detection technology, businesses can ensure the person submitting the ID is indeed physically present. Fraudsters typically abandon the process when asked to provide such authentication forms.

KYC FOR FIAT-TO-CRYPTO

Crypto-to-crypto exchanges often have more relaxed KYC requirements, and many of them require no KYC documentation at all. On the other hand, fiat-to-crypto exchanges typically perform at least some level of KYC. This is because they are dealing with fiat currency, which is recognized as a legal tender by governments. Such exchanges have to conduct business with banks and other traditional financial institutions, most of whom perform their own KYC before conducting business with external entities.

CASE STUDY

Paysafe:

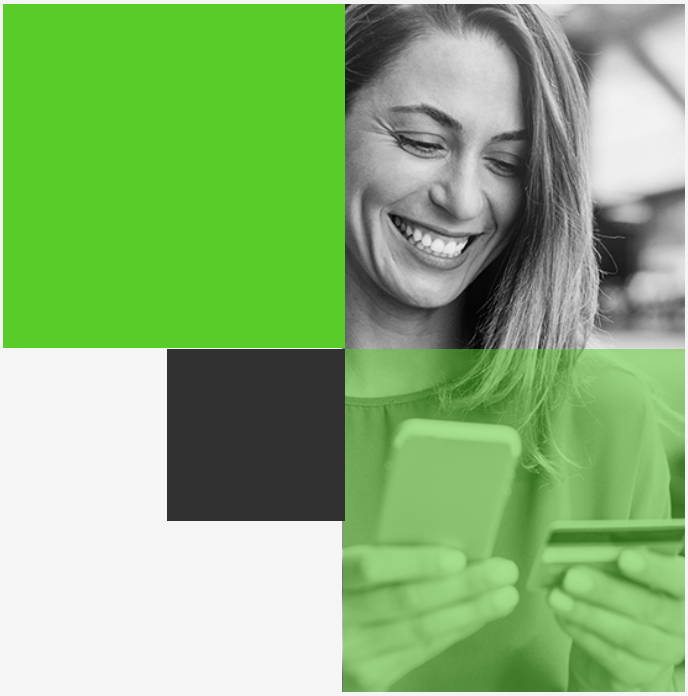
Paysafe, a leading specialized payments platform, needed an automated solution that would enable them to verify customer identities in real time while meeting strict Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance mandates.

Jumio's solutions help Paysafe:

Reduce manual reviews and shorten the customer onboarding process from a day to a few minutes

Improve their customer onboarding experience and conversion

Scale their business geographically through Jumio's global coverage of over 5,000 ID types across more than 200 countries and territories



Read the full case study

ONGOING MONITORING

After you've onboarded a customer, compliance doesn't stop there. You will need to monitor your customers on an ongoing basis. What's more, you will also need to screen the individuals they transact with.

AML screening and ongoing monitoring of new or existing customers is a minimum requirement for any KYC process. This is especially true if third-party payment processors are involved, as these can introduce additional risks, such as anonymity of funds source and beneficiary.

When planning your compliance program, there are several points to take note of.

SPEED AND ACCURACY ARE CRUCIAL

If the person on the other side of the transaction is deemed unsuitable, you must block the transaction with real-time interdiction. However, you must only stop the payments that need to be stopped, or you risk losing legitimate customers. And if you process payments that should have been stopped, you face hefty fines.

This starts with having a sophisticated rule set that triggers the right alerts for your business. Equally important is that the solution uses machine learning to spot patterns and help you tune the rules over time. These help to minimize false positives and increase the catch rates of financial crime.

KEEPING AHEAD OF THE TECHNOLOGY CURVE PUTS YOU AT AN ADVANTAGE

If you do business internationally, cross-border payments can present unique challenges. Complications will arise as you deal with multiple intermediaries across different territories, with variations in data standards and workflows. As a result, 100% automation is extremely difficult, and businesses must rely on highly trained experts to manage cross-border payments. In fact, 2%-5% of cross-border payments are subject to investigation, resulting in a time lag in the payment being completed.

Businesses should use a vendor that can provide a flexible platform designed to swap out the underlying technologies based on the changing business landscape and requirements.

Wire transfers are the most popular cross-border payment method despite high transaction costs and fraud risks. An advanced screening solution can go a long way in identifying and preventing money laundering in wire transfers and other types of fund transfers.

Red flags in funds transfers:

- Many funds transfers are sent in large, round dollar, hundred dollar or thousand dollar amounts.
- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason, or the activity is inconsistent with the customer's business or history.
- Funds transfer activity occurs to or from a financial institution located in a higher-risk jurisdiction distant from the customer's operations.
- Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.
- Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
- Funds transfer activity is unexplained, repetitive or shows unusual patterns.
- Payments or receipts with no apparent links to legitimate contracts, goods or services are received.
- Funds transfers are sent or received from the same person to or from different accounts.
- Funds transfers contain limited content and lack related party information.

OPTIMIZING THE CUSTOMER EXPERIENCE AND PROTECTION

Security is one of the top priorities for consumers when selecting a financial app or brand. Yet, how does one ensure security without compromising on the speed of digital onboarding or opening an online account? How does one make the user experience less disjointed, time-consuming and onerous?

ONGOING AUTHENTICATION

Thanks to advances in verification technologies, more businesses are moving away from traditional methods of authentication such as passwords and knowledge-based authentication, and shifting toward user checks that involve new tools. These include biometric authentication and the increasingly popular proximity badges — contactless cards that can be read without having to insert them into a card reader.

These authentication methods have allowed businesses to improve the customer experience in various ways. For instance, if the organization has already captured biometric data (e.g., a face-based biometric template) during the onboarding process, it only makes sense to repurpose that same data for ongoing authentication.

This means that when a high-risk transaction is initiated (such as a wire transfer or a password reset), the user only needs to retake a selfie and go through a liveness check to quickly unlock their digital identity.

LOW-FRICTION CHECKS

Modern organizations can exploit simple tactics that require no action on the part of the user beyond completing an online application. These include risk signals based on IP address, address verification and phone-based checks.

In the case of IP addresses, another simple check is to determine whether the address of the user's device (phone or computer) matches the physical region of the self-reported information entered on the application.

Many of Jumio's customers correlate these digital attributes with real-world identities to help increase the levels of identity assurance.

When it comes to address verification, one of the simplest checks is to determine whether the physical address exists in the real world and that the applicant resides at that address. Firms can ping third-party databases and credit bureaus in real time without alerting a potential fraudster.

For phone-based checks, several risk signals can be derived from the number provided by the user. Some vendors will send an SMS message to the phone to ensure the phone number provided belongs to the applicant. But there's more information that can be gleaned from the phone number, including the age of the SIM, the IP address and porting information.

DESIGNING THE COMPLIANCE FLOW

Most eKYC solutions tend to be limited in scope, forcing companies to research, purchase, integrate and maintain dozens of different point solutions to meet all their identity verification requirements across the end-user journey. This can be costly in terms of time, resources and money, in addition to creating an unmanageable web of complexity.

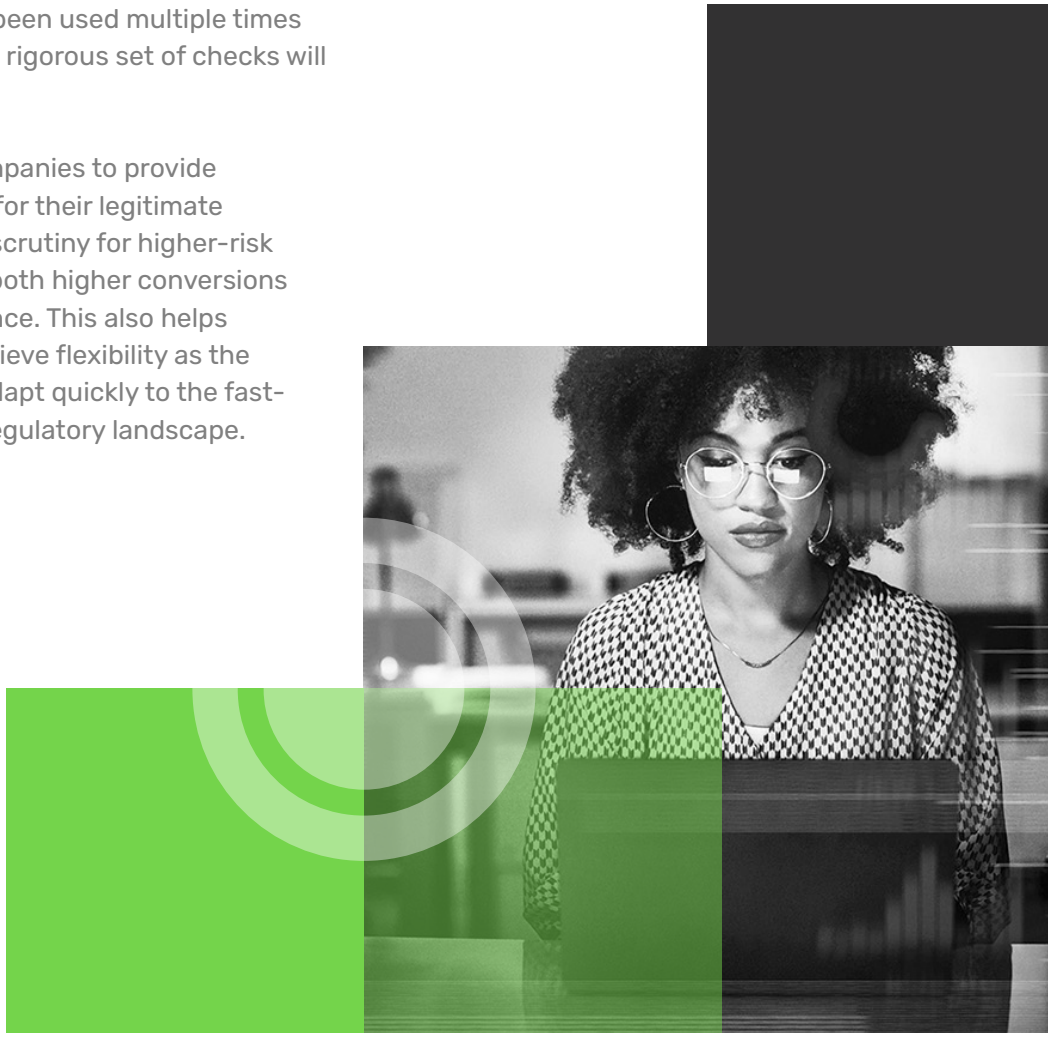
This is why so many companies are now turning to end-to-end identity verification platforms with orchestration.

Orchestration is the ability to run multiple KYC checks and dynamically adjust the workflow based on real-time inputs. For example, your workflow may start with a device check. If the user's smartphone has already been used multiple times to open accounts, a more rigorous set of checks will be initiated.

This approach allows companies to provide a frictionless experience for their legitimate customers and increase scrutiny for higher-risk individuals. The result is both higher conversions and higher fraud deterrence. This also helps improve productivity, achieve flexibility as the business expands, and adapt quickly to the fast-changing business and regulatory landscape.

Orchestration is also useful post-onboarding for continuous authentication and risk-based monitoring. For example, if a customer logs in from an unusual location, simply checking their password may not be enough. Instead, an advanced authentication workflow prompts the user to take a new selfie and compares it to the biometric template that was created from the original selfie they took when they created the account.

Fraudsters constantly evolve, and when a new fraud pattern emerges, businesses must be able to respond immediately. The best identity verification platforms allow business users to modify rules in real time with a straightforward rules editor.



ONE PLATFORM TO RULE THEM ALL

While technically an orchestration tool can allow you to connect to multiple data sources from different vendors in your workflow, a single platform provides huge advantages. This is because:

- You sign a contract and maintain a relationship with only one vendor, which saves companies time and resources.
- Integrations to different data sources are pre-built, making orchestration very straightforward so you can focus on your business instead of fighting fraud.
- When regulations change or if a data source no longer meets your needs, you don't have to worry about finding and implementing a different data source — the platform vendor handles everything for you.

LEVERAGING THE JUMIO PLATFORM: FROM ONBOARDING TO ONGOING MONITORING

Traditionally, financial institutions would need over a dozen solutions to:

- **Verify the user's identity**
- **Check their ID and supporting documentation**
- **Authenticate them on subsequent visits**
- **Perform ongoing screening to make sure they are still suitable to do business with**

This approach is complex, inefficient, expensive — and often does not work. Jumio protects the ecosystems of businesses through the Jumio platform, a unified, end-to-end identity verification, eKYC and AML platform. It offers a range of identity verification and AML services to accurately establish, maintain and reassert trust, from account opening to ongoing monitoring.

If your organization is ready to take the next step toward a safer, identity-centric security strategy, the Jumio platform provides everything you need to orchestrate sophisticated and flexible workflows that can connect to hundreds of data sources — all from a single API.

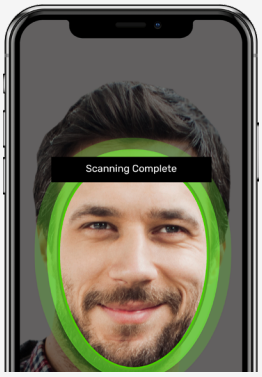
END-TO-END IDENTITY VERIFICATION, EKYC AND AML SOLUTIONS

ONLINE CUSTOMER ONBOARDING

Identity Verification and Risk Signals

- ID & Selfie Verification
- Liveness Detection
- Government Databases
- Device Intelligence
- Phone Number Verification
- Email Verification
- Address Services
- Video Verification

ONGOING MONITORING

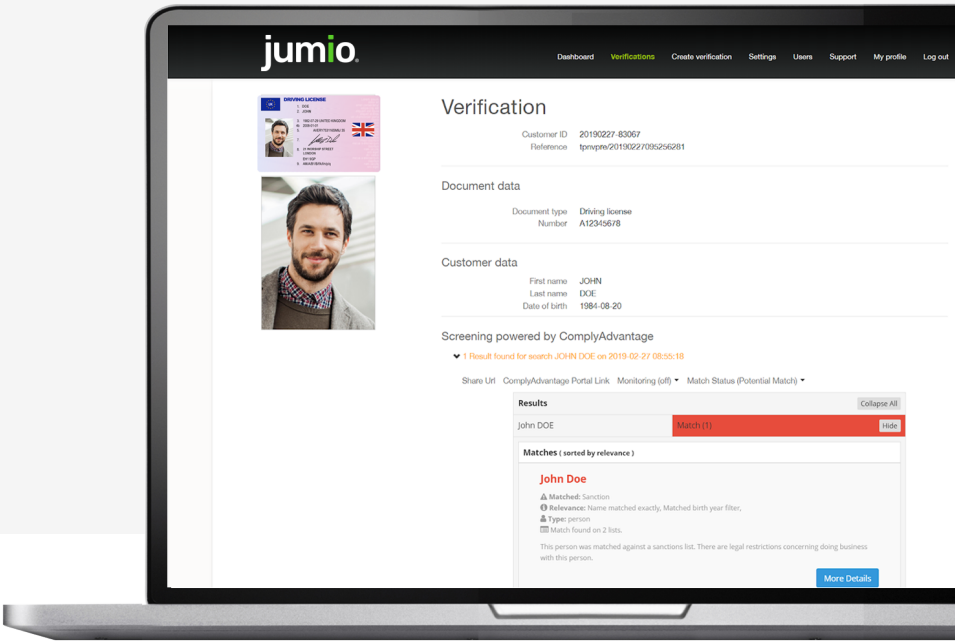


Identity Authentication

- Capture and compare new selfie to the original biometric information created during onboarding
- Perform liveness check

Continuous AML Screening

- Sanctions
- Politically Exposed Persons
- Adverse Media



ABOUT JUMIO

Jumio helps organizations to know and trust their customers online. From account opening to ongoing monitoring, the Jumio platform provides AI-driven identity verification, risk signals and compliance solutions that help you accurately establish, maintain and reassert trust.

Leveraging powerful technology including automation, biometrics, AI/machine learning, liveness detection and no-code orchestration with hundreds of data sources, Jumio helps you fight fraud and financial crime, onboard good customers faster and meet regulatory compliance including KYC and AML. As the industry leader, Jumio has processed more than 1 billion transactions spanning over 200 countries and territories from real-time web and mobile transactions.

Based in Sunnyvale, California, Jumio operates globally with offices and representation in North America, Latin America, Europe, Asia Pacific and the Middle East and has been the recipient of numerous awards for innovation. Jumio is backed by Centana Growth Partners, Great Hill Partners and Millennium Technology Value Partners.

For more information, please visit jumio.com.