Online Customer Identity Verification Program

COMPLIANCE MADE SIMPLE

An Essential Guide to Simplify Your Compliance with 7 Key Requirements

JUMIO

Welcome to consumer protection in the digital age.

The lines between the digital and physical world are officially blurry. According to a 2018 Pew Research study, one-in-four Americans say they are online 'almost constantly' and three-quarters of Americans go online at least daily. Consumers are doing everything from catching a ride, sending money to a friend, opening a bank account, renting a vacation home, and so much more, all with a few clicks and swipes.

Along the way, consumers are leaving a digital trail of information that can and will be used against them if in the wrong hands. In fact, the convergence of offline and online has opened up entire new pathways for fraudsters, money launderers, and identity thieves to assume another person's identity and wreak havoc on innocent people, companies, and even entire industries.

Consequently, there is a rising tide of concern that the people you do business with and the people you connect through your business are authentic—that they are who they claim to be. The concern has been highlighted in several recent high profile cases including the congressional hearing into Facebook's data collection and sharing practices, the Wells Fargo account opening scandal, and the massive Equifax breach.

Enter online identity verification.

Online customer identity verification providers have come on the scene with increasing urgency to help ensure trust and safety among customers and users of online services across a spectrum of industries. The role of online identity verification is to tie your customers' digital identities (who they claim to be) to their real world identities (who they are in real life). This "match" is key to building a strong online brand, preventing fraud, and converting good customers.

Companies have utilized a range of approaches to achieve a desired level of confidence in the identities of their customers. For some, confirming a valid government-issued ID (passport, driver's license) is enough and can be accomplished using the camera on a smartphone or computer. Other companies are comfortable with two-factor authentication or knowledge based authentication (KBA). Still others demand a more thorough identity verification (including ID checks, supporting documentation, and biometric verification).

On one hand, each layer of trust and safety brings a layer of confidence, fraud prevention, and risk reduction. On the other hand, each layer requires online users to divulge more information that, if not handled appropriately, could later be used by scammers to assume their identities.

Enter regulators.

Lawmakers have long been involved with regulations intended to protect the financial system. KYC (Know Your Customer) and AML (Anti-Money Laundering) are among the most notable. But today, they face a growing chorus of concern over consumer privacy and data protection online. In the course of capturing and verifying identity information, companies expose a range of personal identifying information (PII). This information, and the consumers who own it, demands protection.

About this whitepaper:

This whitepaper outlines some of the key regulations you'll need to consider as you subject your customers and online users to ID, identity, or document verification processes. It will also run through considerations to help you choose the right identity verification provider with the systems and processes in place to support and enable your compliance.

What we'll cover:

1. General Data Protection Regulation (GDPR)
2. California Consumer Privacy Act (CCPA)
3. Know Your Customer (KYC)
4. Anti-Money Laundering (AML)
5. 4th Anti-Money Laundering Directive
6. Revised Payment Service Directive (PSD2)
7. Payment Card Industry (PCI-DSS) Compliance

Let's get started.

1. General Data Protection Regulation (GDPR)

What is it?

GDPR is a regulation that requires businesses to protect the personal data and privacy of EU citizens. It came into effect May 28, 2018 and covers how data is collected, stored, processed, and destroyed.

Does it apply to you?

If an organization is based in the EU or conducts business with EU citizens, GDPR applies. Unfortunately, countless organizations, both inside and outside the EU, are still unaware that GDPR applies to them and their third-party solution providers, known as data processors, who handle personal data. According to an Ovum report, about two-thirds of U.S. companies believe GDPR will require them to rethink their strategy in Europe. In fact, 85% of those surveyed see the GDPR putting them at a competitive disadvantage with European companies.

How is your online identity verification program impacted?

Gemma Rogers, co-founder of Fintrail compliance consultancy, explains, “While it is the duty of all companies to ensure they properly protect and manage the data of EU citizens, this is especially important for companies offering identity verification solutions. Data processors in this space handle vast amounts of sensitive, personal data that, while integral to ensuring customers are who they say they are, can also be exploited or mishandled.

At the same time, the best data processors in identity verification can not only meet GDPR requirements, but also help collectors reduce their compliance burden. This is why GDPR compliance is so important in the identity space. Data collectors need to make sure their processors, especially in the identity verification space, are being held accountable to a high standard when it comes to GDPR, in both the letter and spirit of the law.”

For many industries, companies have to establish trust in digital identity verification solutions that can guarantee “the person claiming a particular identity is in fact the person to whom the identity was assigned.” But, this imposes strict requirements on the vendor that is managing sensitive personal information, including images of government-issued IDs, biometric and other personal information.

GDPR Article 5 addresses principles relating to processing of personal data. It includes this statement:

> **“Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”**

Beyond the secure handling of PII data, GDPR mandates additional considerations when the outcome of that verification results in an “automatic refusal of an online credit application or e-recruiting practices.” Fully automated verification solutions that fail to give the data subject the right to “to obtain human intervention on the part of the (data) controller, to express his or her point of view and to contest the decision” (Article 22(3) GDPR) are not allowed under GDPR.

What should you look for in a compliant identity verification solution?

Given the important intersection between identity verification and GDPR compliance, it is important to understand what to look for in an online identity verification solution.

1. Human Review

GDPR gives data subjects (i.e., your online customers) the right not to be subject to decisions solely based on automated processing that produce ‘legal effects’ or other significant effects. As increasingly more online verifications are carried out by algorithms, concerns have been raised about the lack of transparency behind the technology, which leaves individuals with little understanding of how decisions are made about them.

2. Compliant Machine Learning

Many identity verification vendors aggregate data across multiple customers to develop their machine learning algorithms. With GDPR, vendors can only develop specific AI models trained on the data of a given customer and cannot leverage data from other business customers to create more comprehensive models.

3. Data Retention

GDPR requires that personal data should be ‘limited to what is necessary for the purposes for which they are processed,’ and requires personal data storage being ‘limited to a strict minimum.’

4. Breach Notification

GDPR requires data processors to notify the controller ‘without undue delay’ once aware of a data breach. Most identity verification vendors don’t have established or tested processes in place for data breach notifications.

5. Data Encryption

GDPR requires data processors to have ‘appropriate’ measures to ensure security of personal data, including encryption, ensuring confidentiality, restoring data access and regular auditing/testing.

2. California Consumer Privacy Act (CCPA)

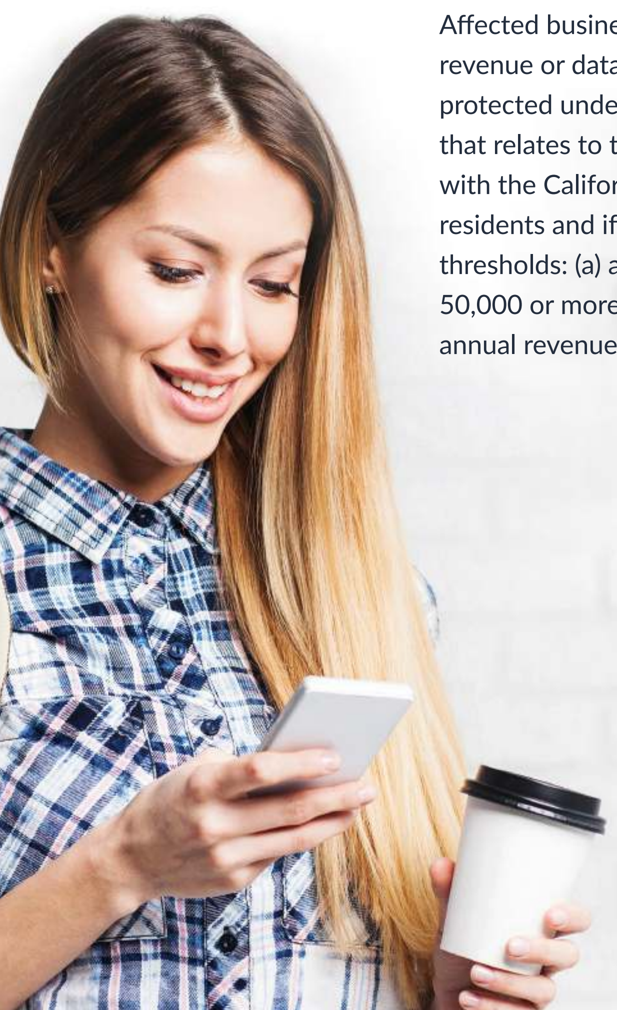
What is it?

A new law—the California Consumer Privacy Act, A.B. 375—affords California residents an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected. Among other novel protections, the law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a "readily useable format" that enables its transfer to third parties without hindrance.

While the law, which is set to come into effect at the start of 2020, technically applies only to California residents, it will most likely have much broader implications. **In fact, it will likely be the strictest data privacy law in the United States, and will require data privacy protections and requirements similar to or broader than those imposed by the European Union General Data Protection Regulation that became effective on May 25, 2018.** Consider that most major companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some Californian customers.

Does it apply to you?

Affected businesses are for-profit entities doing business in California that meet certain revenue or data collection volume requirements. Principally, all California residents are protected under the California Consumer Privacy Act with respect to any information that relates to them. This means that companies around the world have to comply with the California Consumer Privacy Act if they receive personal data from California residents and if they—or their parent company or a subsidiary—exceed one of three thresholds: (a) annual gross revenues of $25 million; (b) obtains personal information of 50,000 or more California residents, households or devices annually; or (c) 50% or more annual revenue from selling California residents' personal information.



How is your online identity verification program impacted?

Because many forms of identity verification collect personal information including information on government-issued IDs, biometric information, and/or pictures of consumers, these solutions are bound to comply with CCPA. The CCPA broadly defines personal information to cover types of information not traditionally considered personal information in the United States, including:

- IP addresses
- Email addresses
- Records of purchasing or consuming histories or tendencies
- Browsing history and search history
- Geolocation data
- Audio, visual, or thermal information
- Professional or employment information
- Education information

What should you look for in a compliant identity verification solution?

CCPA-compliant solutions should be transparent about the types of personal data collected as part of the identity verification process. Your chosen identity verification solution must be able to equip their business customers with a complete list of the personal data collected and it must be able to manage consumer requests for deletion of personal data after the identity verification has been performed. And clearly, your chosen solution should not be re-selling consumer data without prior acknowledgment and businesses should seek written confirmation that consumer data is kept strictly confidential.

Like GDPR, CCPA-compliant solutions should store PII data securely and have predetermined data retention policies in place to assure the timely deletion of that data. Compliant solutions should have the ability to manually override retention policies and have consumer data deleted upon written request. Identity verification solutions that are already PCI-DSS compliant have a significant head start because of the security and data protection mandates they must meet and vet with independent auditors. Likewise, any solution that is already GDPR compliant should be able to tick most, if not all, of the compliance mandates of CCPA.

3. Know Your Customer (KYC)

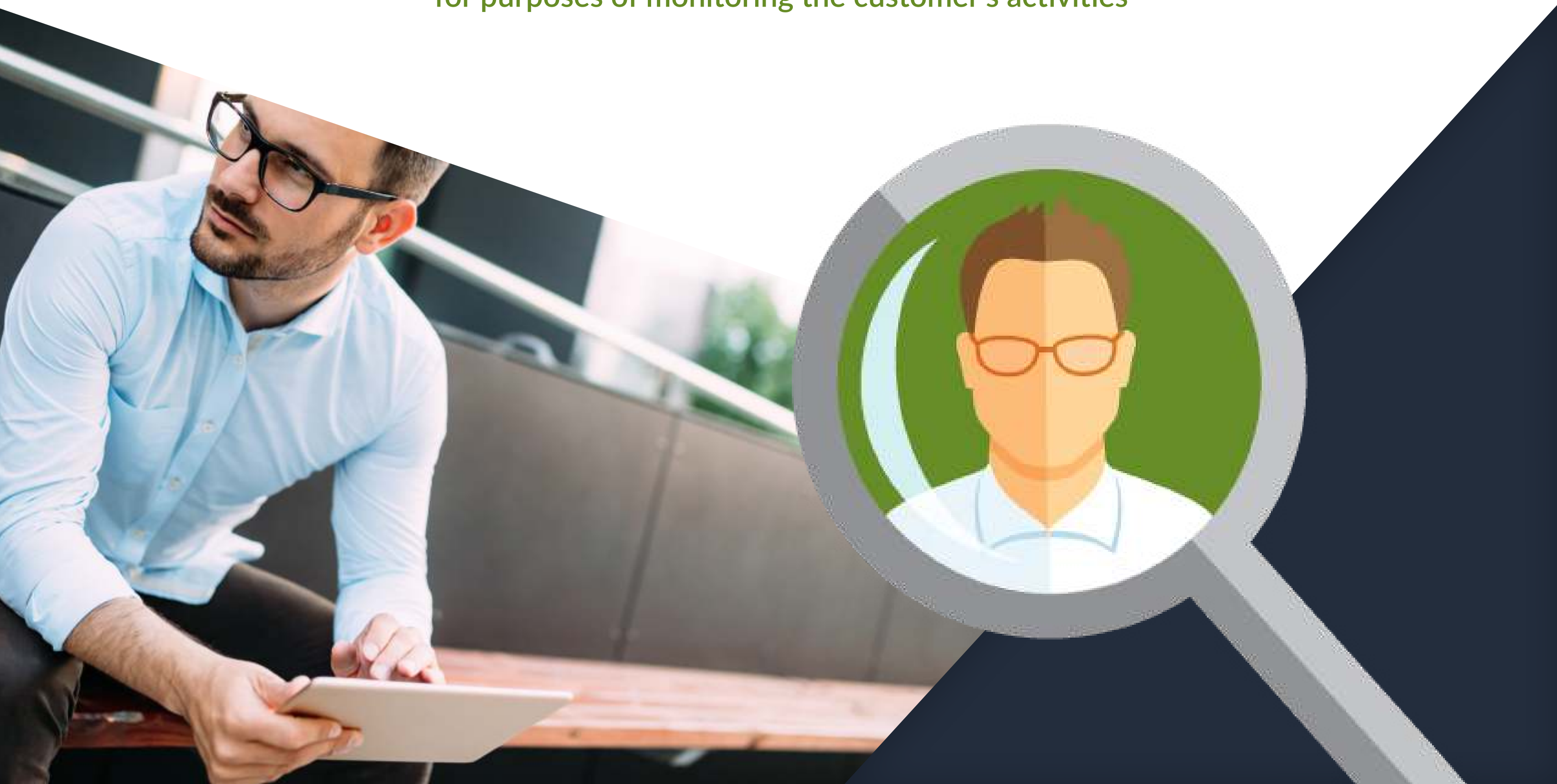
What is it?

The process of knowing your customer, otherwise referred to as KYC, refers to the process of verifying the identity of your customers, either before or during the time that they start doing business with you. The term KYC also references the regulated bank customer identity verification practices to assess and monitor customer risk and a legal requirement to comply that are intended to prevent banks from being used for money laundering activities.

If you're a financial institution, you can face possible fines, sanctions and bad publicity if you do business with a money launderer or terrorist. More importantly, it's a fundamental practice to protect your financial institution from fraud and losses due to illegal funds and transactions.

"KYC" refers to the steps taken by a financial institution (or business) to:

- ✓ **Establish customer identity**
- ✓ **Understand the nature of the customer's activities (primary goal is to satisfy that the source of the customer's funds is legitimate)**
- ✓ **Assess money laundering risks associated with that customer for purposes of monitoring the customer's activities**



Does it apply to you?

Regulations are becoming increasingly strict for financial institutions to better verify customer identities during the opening and maintaining of accounts. KYC rules require “reasonable diligence” to know (and retain) the essential facts concerning every customer. Whether you are technically subject to KYC regulation or not, companies of all sizes are embracing KYC practices to protect themselves and their customers.

How is your online identity verification program impacted?

How do you know someone is who they say they are?

Consider these stats. According to 2018 Identity Fraud: Fraud Enters a New Era of Complexity from Javelin Strategy & Research, in 2017, there were 16.7 million victims of identity fraud, a record high that followed a previous record the year before. Criminals are engaging in complex identity fraud schemes that are leaving record numbers of victims in their wake.

The amount stolen hit $16.8 billion last year as 30% of U.S. consumers were notified of a data breach last year, an increase of 12 percent from 2016.

But, this is not just a U.S. phenomena.

Identity fraud in the UK hit a record high of 174,523 incidents last year—and the vast majority of it happened online. Separate research (Source: Top10VPN.com, March 2018) found that fraudsters operating on the dark web could buy a person’s entire identity for just £820.

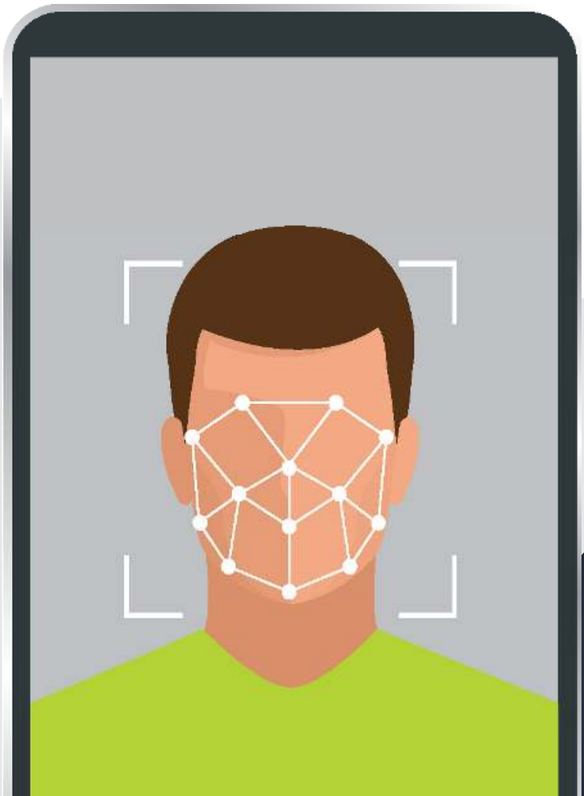
The customer identification program (CIP) mandates that any individual conducting financial transactions have their identity verified. As a provision in the USA Patriot Act, it's designed to limit money laundering, terrorism funding, corruption and other illegal activities. A critical element to a successful CIP is a risk assessment, both on the institutional level and on procedures for each account. While the CIP provides guidance, it's up to the individual institution to determine the exact level of risk and policy for that risk level.

It's not enough to just check your customer once, you need to have a program that knows your customer on an ongoing basis. The ongoing monitoring function includes oversight of financial transactions and accounts based on thresholds developed as part of a customer's risk profile. Historically, regulations had called for a risk-based assessment, however, as of January 1, 2017, the New York Department of Financial Services (NYDFS) requires specific measures of transaction monitoring and filtering.

While customers want the account opening process to be fast, easy, and online, financial institutions are grappling with how to offer this experience while meeting stringent KYC and related AML compliance requirements. Unfortunately, the typical approach of knowledge based authentication has come under fire as highly-publicized breaches and rising account opening fraud has the industry looking for a better way.

What should you look for in a compliant identity verification solution?

To help meet your KYC obligations you need an identity verification solution that can deliver both convenience to your customers and protection for your business. To do so, look for mobile and web-enabled solutions that leverage on-device technology, biometrics (such as facial recognition with liveness detection), compliant machine learning, and identity experts to achieve accurate identity results within a seamless digital environment your customers want.



4. Anti-Money Laundering (AML)

What is it?

Anti-money laundering (AML) describes the legal controls that require financial institutions and other regulated entities to prevent, detect, and report money laundering activities. Anti money laundering (AML) refers to a set of procedures, laws and regulations designed to stop the practice of generating income through illegal actions. Though anti-money laundering laws cover a relatively limited number of transactions and criminal behaviors, their implications are far-reaching.

Does it apply to you?

AML regulations require financial institutions issuing credit or allowing customers to open accounts to complete due-diligence procedures to ensure they are not aiding in money laundering activities. It's up to financial institutions that issue credit or allow customers to open accounts to investigate customers to ensure they are not taking part in a money laundering scheme. They must verify where large sums of money originated, monitor suspicious activities and report material cash transactions.

How is your online identity verification program impacted?

Online identity verification is the starting point for AML compliance in a digital world. If the EU's Fourth Anti-Money Laundering Directive is any indication, governing bodies are becoming more comfortable with, and some would suggest even encouraging of, the use of digital customer identity verification. The European Commission recognizes, "Accurate identification and verification of data of natural and legal persons is essential for fighting money laundering or terrorist financing. Latest technical developments in the digitalization of transactions and payments enable a secure remote or electronic identification."

According to Gov.UK, organizations must perform due diligence by carrying out checks on their business and customers, and maintain records to help prevent money laundering. Customer due diligence means taking steps to identify your customers and checking they are who they say they are. In practice, this means obtaining a customer's name, photograph on an official document which confirms their identity, and residential address and date of birth. The best way to do this is to ask for a government issued document like a passport, along with utility bills, bank statements and other official documents.

What should you look for in a compliant identity verification solution?

AML and KYC go hand in hand when it comes to the role of online identity verification. To help meet your obligations you need a solution that is convenient for your customers and delivers a high level of assurance that your customers are who they say they are. To do so, look for mobile and web-enabled solutions that leverage on-device technology, biometrics (such as facial recognition with liveness detection), compliant machine learning, and identity experts.

In addition to ID and identity verification, organizations should look for identity verification solutions that can also establish proof of address by extracting data from bank statements or utility bills. These document verification solutions, when combined with identity verification, provide an extra layer of assurance during the account set-up (customer onboarding) process that can help you meet the stringent requirements of AML.

5. 4th Anti-Money Laundering Directive

What is it?

The European Union's Fourth Anti-Money Laundering Directive went into effect in June 2017 with the purpose of removing any ambiguities in the previous legislation and improving the consistency of anti-money laundering (AML) and counter terrorist financing (CTF) rules across all EU Member States. The Directive includes some fundamental changes to the anti-money laundering procedures, including changes to CDD, a central register for beneficial owners and a focus on risk assessments.

The main modification points to note are:

- ✓ **Emphasis on ultimate beneficial ownership and enhanced customer due diligence**
- ✓ **Expanded definition of a politically exposed person to domestic PEPs**
- ✓ **Cash payment threshold lowered to €10,000 (US$11,250)**
- ✓ **Expanded to include the entire gambling sector beyond just casinos**
- ✓ **Enhanced risk-based approach, requiring evidence-based measures**

However, with proper preparation and training, the transition to the new regime should be seamless for most firms. The rules for politically-exposed persons ("PEPs") are no longer limited to persons outside the UK. Local PEPs will now be subject to the same scrutiny as foreign PEPs. The Directive puts a heavy emphasis on employing a risk-based approach to money laundering at every level. It directs states to commission national risk assessments, firms to develop risk-based policies, and practitioners to conduct CDD in a risk-based manner.

Does it apply to you?

The Directive applies to organizations within EU member states. It emphasizes ultimate beneficial ownership and enhanced customer due diligence. Affected corporations and legal entities must maintain accurate and current information on ultimate beneficial ownership. They must provide that information to the government and it will be held by each member state in a central register that will be accessible to banks, law firms and "any person or organisation that can demonstrate a legitimate interest."

How is your online identity verification program impacted?

As you might expect, once again, compliance starts with knowing your customer (KYC). The new rules allow companies to verify customers remotely using electronic means. In fact, the Directive promotes and encourages the use of electronic ID verification:

> " ... in particular with regard to notified electronic identification schemes and means that offer high-level secure tools and provide a benchmark against which assessing the identification methods set up at a national level may be checked."
>
> European Money Laundering Directive 4.1

What should you look for in an AML compliant identity verification solution?

Refer to the KYC and AML sections above.

6. Revised Payment Service Directive (PSD2)

What is it?

PSD2 is the second iteration of the Payment Services Directive (PSD) implemented by the European Union and it affects both individual consumers and businesses. PSD2 enables bank customers to use third-party providers to manage their finances. The regulation went live in January 2018 and has implications for all companies in Europe that deal with payments, ranging from how to regulate the emergence of Third Party Providers (TPPs) to the need for strong customer authentication (SCA).

Under PSD2 "account servicing payment service providers"—primarily banks—are forced to open up three sets of APIs giving registered third-parties access to customer accounts. The customer must give permission to the bank using two-factor authentication, a process PSD2 refers to as "Strong Customer Authentication" (SCA), before the third-party is allowed access. Most access to customer accounts, including card payments, is covered under this process—sometimes even when the customer is directly querying their own account details.

Does it apply to you?

The rules and guidelines of PSD2 applies to modern payment services, including banks, credit unions, fintech companies, and payment companies (e.g., third party payment service providers, account servicing payment service providers, and payment information service providers) based in the European Union.

How is your online identity verification program impacted?

PSD2 sets out very specific standards for secure electronic identity verification, in order to keep customers' funds and personal identities safe. The European Banking Federation encourages trust in digital identity verification tools that can guarantee "the person claiming a particular identity is in fact the person to whom the identity was assigned."

One of the key requirements of the revised Payment Services Directive (PSD2) is that banks must add two-factor Strong Customer Authentication (SCA) for all remote access to customer accounts. This means that when authentication is required, two of three factors will be applied: something the customer is, something the customer has and something the customer knows. Clearly, identity verification will be critical as part of this, and when customers forget or lose a key component, banks will need to ask them to re-identify themselves.

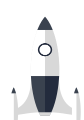
As many businesses are already seeing, customer account access dependent on two-factor authentication leads to an increase in customers losing their authentication credentials. What is often missed in the new regulation is that PSD2 requires this credential reset process to also use two-factor authentication, and needs the end customer to use two different authentication factors to those utilised in the account access process for the Open APIs. The credential reset process means the customer has to re-identify themselves to their bank using a Strong Customer Identity Verification (SCeID) process to verify or re-verify their identity.

Both SCA and SCeID are mandated by PSD2, although the latter is not well understood. Failure to implement these capabilities exposes banks to penalties under PSD2 as set by national regulators. However, a failure to implement these capabilities properly may also expose banks to potential loss of sensitive customer data and, under the General Data Protection Regulation (GDPR), this opens up the possibility of fines of up to 2% of global annual turnover.

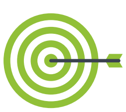
What should you look for in a compliant identity verification solution?

According to a report from Consult Hyperion and Jumio, a compliant PSD2 credential reset process should have the following characteristics:

Strong:
Use two factors of identity document verification to demonstrate that the consumer is in possession of their ID and live facial biometric matching to establish the person behind the transaction matches the person holding the ID.



Fast:
Online and near real-time process to get customers transacting quickly.



Accurate:
Deliver a high level of accuracy using proven technologies and services.

Simple:
Convenient for the customer, while limiting additional compliance costs for the business.

7. Payment Card Industry (PCI-DSS) Compliance

What is it?

PCI DSS compliance requires adherence to a set of specific security standards that were developed to protect sensitive card information during and after a financial transaction and “to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.”

Does it apply to you?

PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. That is, the standard applies to all organizations, which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands. PCI defines a 12-step process that vendors need to adhere to show that they are taking the necessary steps to avoid online access or compromise to their card processing data. Failure to achieve PCI compliance could cause a retailer to face substantial penalties, which can exceed $500,000, depending on the volume of transactions processed.

How is your online identity verification program impacted?

While it is not mandatory for online identity verification providers to comply with PCI DSS, consider the value of the data they are handling—legitimate government issued IDs (e.g., passports and driver's licenses). These images can fetch up to $20 on the dark web. Black market dealers can inflict considerable damage armed with valid driver's licenses and passports, including opening new credit cards or getting a major loan in the victim's name. This means that online identity verification vendors are sitting on a treasure trove of valuable PII information which must be managed appropriately and strictly protected from potential data breaches.

What should you look for in a compliant identity verification solution?

Plain and simply, ask and verify that your identity verification provider has a valid PCI-DSS Level 1 certificate. In doing so, this will give you the assurance that their practices are up to date and validated by a reliable third party.

How Jumio Can Help

GDPR Compliance

Jumio is GDPR compliant and can help companies meet their GDPR obligations.

GDPR categorizes data holders into two groups: processors and controllers.

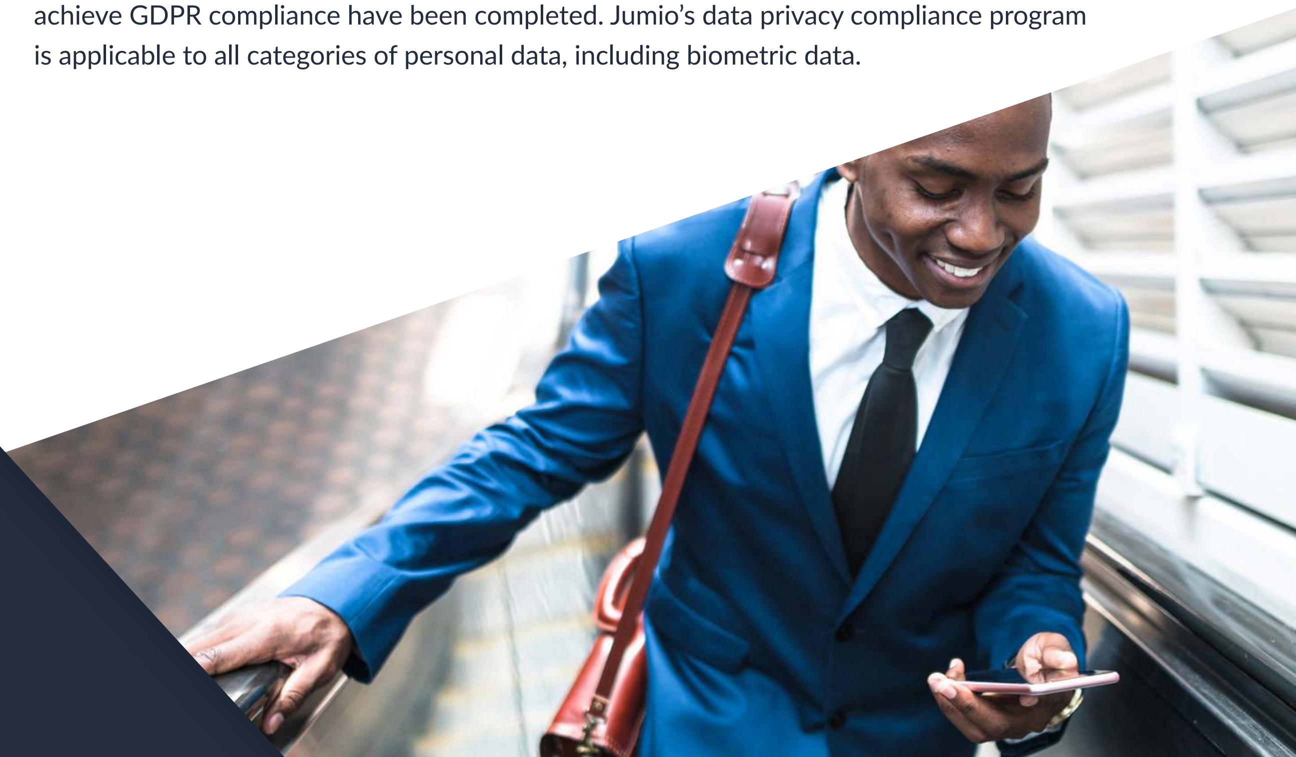
Controllers collect, process, store, and basically "own" the data and the relationship with EU citizens.

Processors are essentially subcontractors of controllers who may process, store, and utilize EU citizen data on behalf of a controller.

There are additional required measures, processes, and documentation requirements for controllers. Jumio is considered a data processor.

Moreover, Jumio is also PCI-DSS compliant. This means that we've adopted a strict set of security standards designed to ensure that identity and PII-related information are encrypted, stored and maintained in a secure and vetted environment.

Statement of Compliance: Jumio uses the European data privacy directives as the baseline for its data privacy compliance globally. Effective February 1, 2018 all necessary steps to achieve GDPR compliance have been completed. Jumio's data privacy compliance program is applicable to all categories of personal data, including biometric data.



California Consumer Privacy Act

Jumio enables any business that captures data from California residents with the requisite data security, transparency and retention policies to comply with CCPA. Jumio will never sell consumer data to third parties. Just as importantly, Jumio stores and protects consumer data, captured during the identity verification process, under PCI-DSS's strict data security requirements.

Jumio has the ability to delete any data captured during the online identity verification process, including information captured from government-issued IDs, biometric information, and selfie images. Business customers can enforce strict data retention periods or have the identity information deleted automatically after a verification decision has been rendered.

Know Your Customer

Jumio enables financial organizations to fulfil their KYC (Know Your Customer) obligations with fast and accurate online ID and identity verification. Our solutions have helped banks and other financial institutions replace slow, ineffective, and manual KYC processes with more automated solutions that can be embedded within the online account setup and onboarding experience.

Anti-Money Laundering

Jumio's online identity verification solutions are among the most cost-effective ways of responding to the demands of their ever mobile-centric and technically savvy customers with an easy to use and secure identity authentication experience. Additionally, Jumio's solutions help banks and other financial institutions support the ongoing AML on a global scale since our identity verification solutions are already in compliance with the most comprehensive regulations. Jumio also offers document verification services that extracts address information from utility statements and bank statements which provides an extra layer of identity assurance.

4th Anti-Money Laundering Directive

Jumio enables European merchants, financial institutions and other obligated entities with the online verification tools needed to comply with AMLD 4.1. Jumio's online identification solutions allows for quicker, cost-effective, and seamless identification processes, while retaining the risk reduction and compliance requirements the financial industry demands. Our identity solutions replace the cumbersome paper bound procedures of outdated, manual high-touch methods with new digital data techniques and procedures.

Revised Payment Service Directive (PSD2)

Jumio's online identification solutions enable EU banks to incorporate the necessary PSD2 safeguards to ensure that each customer's identity is verified before each interaction with a third-party service provider. PSD2 requires that EU banks have a process of establishing the identity of the customer including determining to an appropriate level of assurance certain information (attributes) such as name, address and date of birth. Jumio helps these banks establish authentication credentials that allow their customers to assert their identity in the future without needing to redo the relatively expensive identification process each time.

Payment Card Industry (PCI-DSS) Compliance

Jumio is PCI DSS Level 1 compliant and regularly conducts security audits, vulnerability scans and penetration tests to ensure compliance with security best practices and standards. To demonstrate PCI compliance a yearly on-site validation assessment by a QSA is carried out. Jumio carries the security controls established to achieve PCI compliance over to PII data which is of comparable sensitivity and has extended the scope of such controls to cover and protect all systems used to transmit/process/store PII data.

Because Jumio has complied with PCI-DSS strict security standards, our customers can have greater confidence that their data—be it credit card, PII, or government-issued IDs—is handled in a secure manner throughout its lifetime. Jumio extracts, redacts (masks), and stores merchant's credit card information while adhering to PCI DSS, reducing customers' internal processing and operational costs.

Trusted Identity as a Service (TIaaS)

Across industries, companies are finding that establishing trust and safety goes hand in hand with having a strong customer identity verification process.

The processes you enable to verify the identities of your users and customers must be secure, accurate, and compliant while also contributing to a smooth and seamless onboarding experience. While it may feel impossible to achieve all of these goals, the fact is, customers expect it. Your customers want to engage with companies that have strong measures in place to deter fraud and protect personal privacy, but not at the expense of a fast and easy customer experience.

The Identity Verification Triangle

Customers

- Trust & safety
- Privacy
- Ease and speed of use

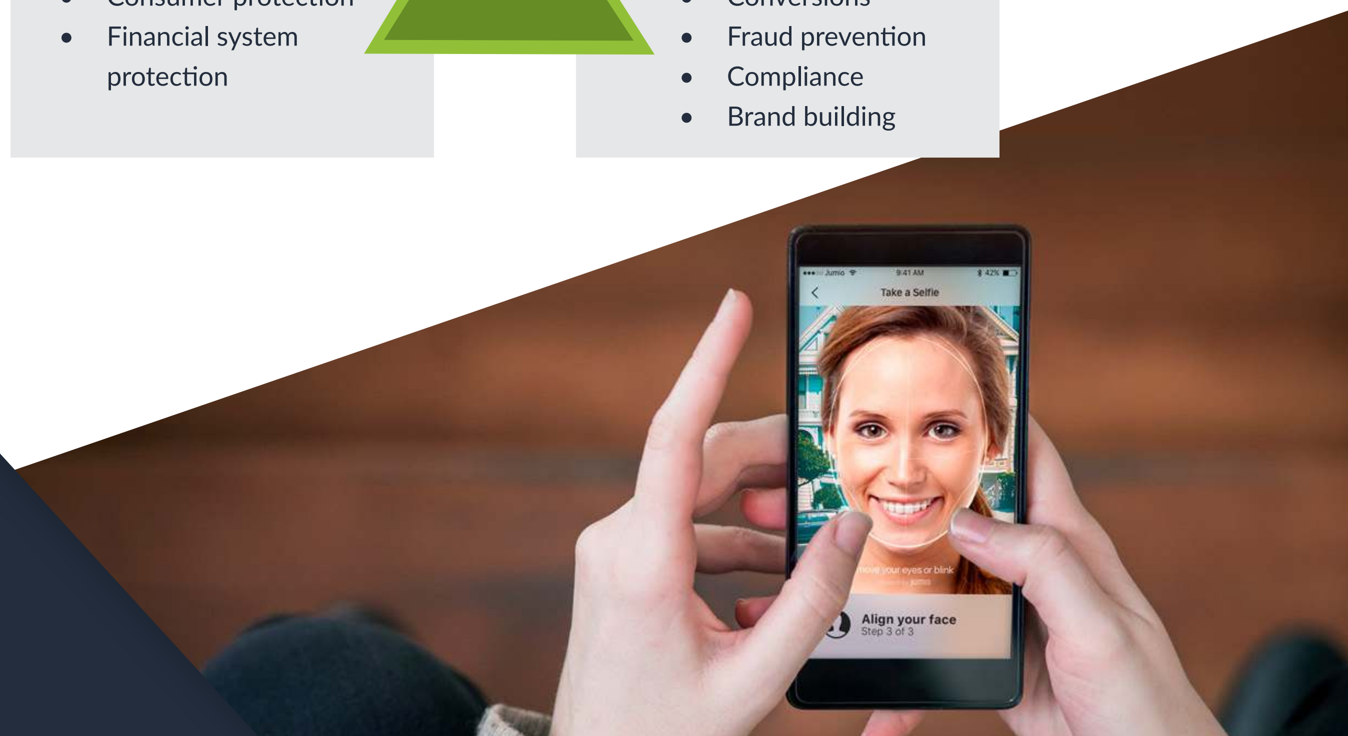
TIaaS

Regulators

- Consumer protection
- Financial system protection

Businesses

- Conversions
- Fraud prevention
- Compliance
- Brand building



NETVERIFY®

Trusted Identity as Service

Jumio offers Trusted Identity as a Service through its Netverify suite of products. Netverify enables businesses to increase customer conversions while providing a seamless customer experience and reducing fraud. By combining the three core pillars of ID Verification, Identity Verification and Document Verification, businesses now have a complete solution that allows them to establish the real-world identity of the consumer.

Leveraging advanced technology including augmented AI, biometric facial recognition, machine learning, and human review, Jumio helps organizations to meet regulatory compliance including KYC, AML and GDPR and definitively establish the digital identity of their customers. Jumio has verified more than 130 million identities issued by over 200 countries from real time web and mobile transactions. Jumio's solutions are used by leading companies in the financial services, sharing economy, cryptocurrency, retail, travel and online gaming sectors.

JUMIO®

When Identity Matters

Learn more at jumio.com