Solving the Identity Problem in PSD2 and GDPR

consult hyperion

JUMIO®

Executive Summary

The Second Payment Services Directive—known as PSD2—forces banks across all European Union member states to add two-factor Strong Customer Authentication (SCA) on all remote access to customer accounts. Hidden behind this is a deeper requirement—the need to perform a Strong Customer Identity Verification (SCeID) process on both the initial issuance of the authentication credentials and any subsequent remote re-issuance when credentials are lost.

Failure to implement SCeID, which must also use two-factor authentication, exposes banks and other account servicing institutions to penalties under both PSD2 and the forthcoming General Data Protection Regulation (GDPR). Under GDPR the penalty for not implementing strong processes could be as high as 4% of the previous year's total turnover.

A properly designed SCeID process supports the Customer Due Diligence requirements under the Anti-Money Laundering regulations (AMLD4/AMLD5), simplifying the account creation and digital onboarding processes. It also meets the PSD2 requirement to support two-factor authentication during remote issuance and re-issuance of authentication credentials. If the process is too slow, complex, inaccurate or weak customers will be faced with losing access to their accounts and are more likely to abandon transactions or seek an alternative financial provider. For banks this will lead to loss of business, increased customer dropout rates, regulatory penalties and increased compliance costs.

The aim of this white paper is to examine the links between SCeID and SCA bearing in mind the inter-relationship between PSD2 and GDPR. We outline key requirements for a Strong Customer Identity Verification process that meets the regulatory intent, keeps customers satisfied and addresses the key business needs for payment institutions.

We have produced this white paper to share insight into how this legislation mandates regulated firms to digitally verify customer identity and how Jumio's technology helps to achieve this objective in compliance with PSD2 and GDPR.

consult hyperion JUMIO

Table of Contents

Key Takeaways

PSD2 & GDPR are Changing the European Banking Landscape

PSD2 is forcing payment institutions to open up access to customer account information at the same time as GDPR is increasing the penalties for failing to control that access. All European payment institutions will be affected by these changes. Strong Customer Identity Verification (SCeID) and Strong Customer Authentication (SCA) processes are at the heart of these requirements.

Meet the Challenges Strong Customer Authentication & Identity Verification Bring

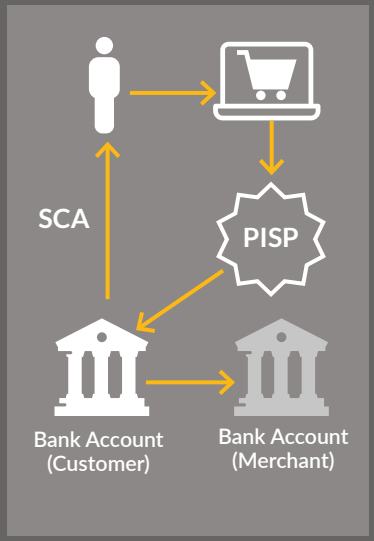
The PSD2 mandate to open an account using two-factor SCA on an irregular basis makes it more likely that customers will lose or forget their credentials—such as their mobile phone or passwords—and will lead to many more reset requests. This reset process exposes payment institutions to criminal attacks, which could lead to penalties under both PSD2 and GDPR. To avoid penalties and keep customers satisfied the credential reset must be built on a remote, strong identity verification process using two alternative authentication credentials.

Create New Value for Your Customers through Strong Customer Identity Verification (SCeID)

A well-designed SCeID process will allow customers to remotely and painlessly perform digital onboarding and to reset their authentication credentials. It will provide a state of the art defence against criminal attacks and will keep customers' transactions safe.

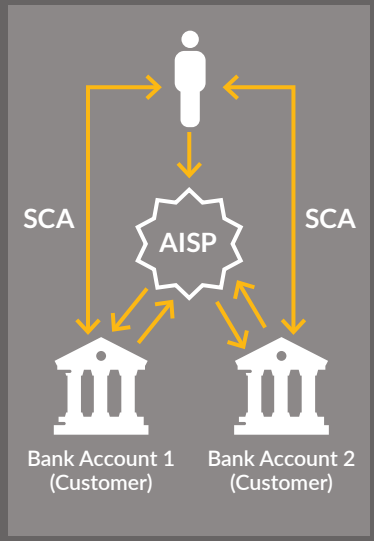
Introduction

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 (see diagram). 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.



Payment Initiation API

Trusted Third Party can initiate a payment directly to a payment account

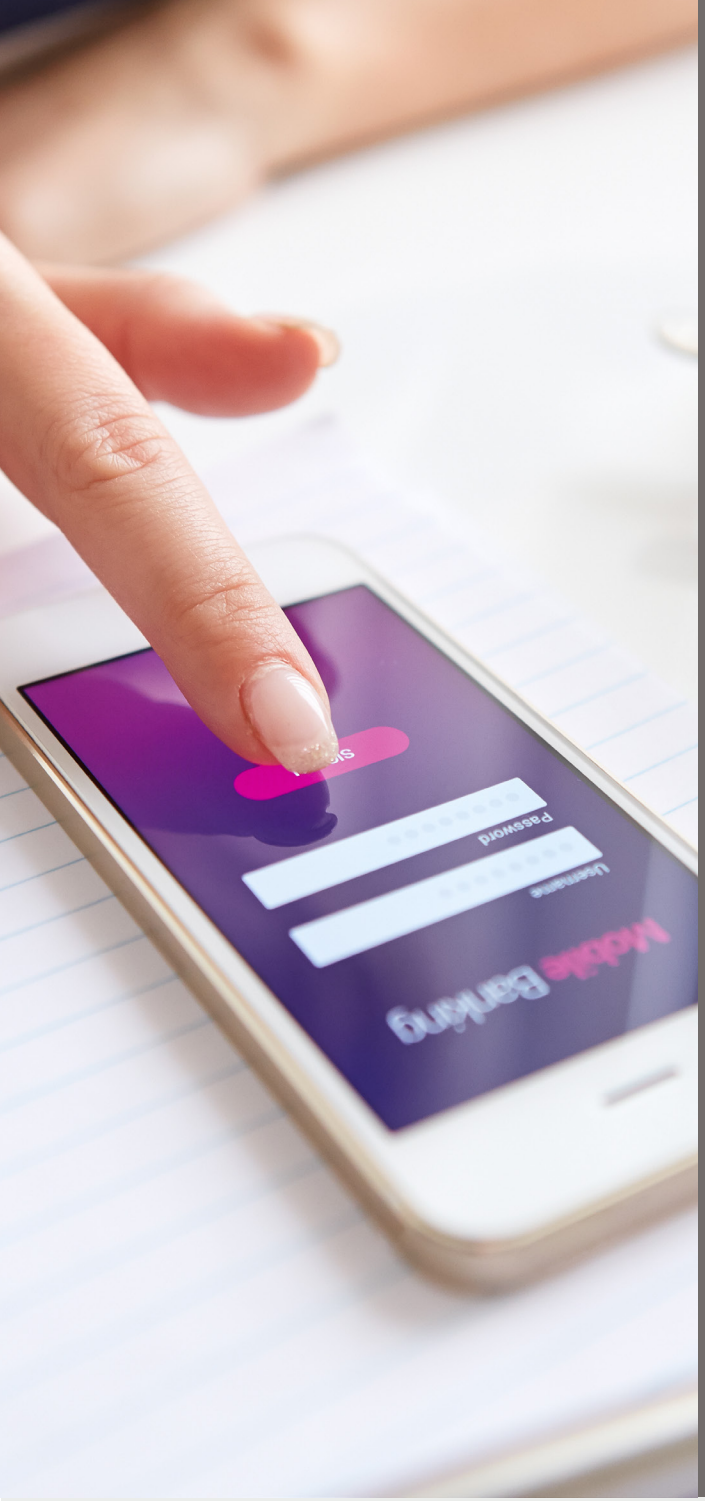


Account Information API

Trusted Third Party can query bank customer account details

Funds Available API

Trusted Third Party can check if funds are available to complete a transaction



We can be sure that making customer account access dependent on two-factor authentication will lead to an increase in customers losing their authentication credentials. For instance, the obvious way of implementing remote two-factor authentication will be through an app on a customer's smartphone, therefore losing, breaking or swapping the device will automatically trigger the need to re-issue 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.

Getting this credential reset process wrong exposes payment institutions to penalties not just under PSD2 but also under the new European General Data Protection Regulations (GDPR). Even a first offence may see penalties of up to 2% of global annual turnover or €10 million, whichever is higher, and there are circumstances under which this could double.

This white paper sets out the challenges that these regulations create for banks and payment institutions around customer identity and authentication, and makes recommendations for an ideal solution that can meet all of these diverse requirements.

Regulatory Context

Summary: The Regulations and Penalties

The specific requirements for PSD2 SCA are detailed in the PSD2 Regulatory Technical Standards (RTS). These specify that all electronic remote access to payment accounts must be based on the use of two or more authentication credentials. Separately, the General Data Protection Regulation (GDPR) governs access to customer data and the consent processes around that use of data, while the ePrivacy Regulation (ePR) extends GDPR to cover all forms of electronic communications.

PSD2 itself will be in force starting January 2018 but the PSD2 RTS on SCA does not apply until 18 months after it is agreed by the European Commission, which has not occurred at the time of publication of this paper. Despite this delay, payment institutions cannot avoid implementing Strong Customer Authentication. If they do they will be liable for penalties under GDPR if fraudsters use the PSD2 Open APIs to access customer account data via weak customer authentication.

PSD2 Jan 2018	GDPR May 2018	ePR (proposed) May 2018	SCA RTS (estimate) Jan 2019
EU-wide regulation Mandates all payment institutions to provide open APIs for account access and payments Requires all remote account access to use 2-factor authentication	EU-wide regulation, global coverage for service providers to EU residents Personal data expanded to include online identifiers Enhanced definition/ restrictive use of consent Enhanced data subject rights Administrative fines of up to £20,000,000/up to 4% of total worldwide annual turnover	Inclusion of over-the-top electronic comms providers Explicit opt-in for direct marketing Enhanced cookie consent Administrative fines of up to £20,000,000/up to 4% of total worldwide annual turnover	Defines specific requirements for PSD2 2-factor authentication Defines rules for exemptions to authentication Defines communication requirements for PSPs Specifies credential reset requirements

PSD2 - Strong Customer Authentication (SCA)

What is PSD2 Strong Customer Authentication?

PSD2 describes SCA as requiring the use of two or more credentials categorised as:

- **Knowledge: Something only the customer knows, such as a password or memorable date.**
- **Possession: Something only the customer possesses, such as a smart phone or hardware fob.**
- **Inherence: Something the customer is, such as a biometric. Behavioural biometrics, such as analysing keystroke patterns, are specifically banned as an authentication factor.**

These factors must be independent, such that a breach of one credential does not cause a breach in the other.

When must Strong Customer Authentication be used?

PSD2 Article 97(1) requires that SCA is used when:

- **The customer makes a remote payment—this can be via a PSD2 API or using a card.**
- **The customer accesses their account remotely or permits a third-party to do so.**
- **Any other situation occurs which could lead to remote, account based fraud—which would include resetting credentials remotely.**

PSD2 allows for exemptions to SCA (see breakout box)—situations in which it is not needed to access accounts remotely—but the approach means that all customers will, from time to time, find that they need to use their two credentials to access their account. There will be many occasions when, if a customer loses access to their credentials, they will be unable to access their account or make a payment.

The RTS makes clear that the SCA process extends beyond pure authentication and must cover an identity verification process that ensures the correct customer is associated with the correct account details (see diagram). The process of remotely linking the customer identity to the authentication credentials must use SCA—but cannot use the regular credentials as these have been lost or forgotten.

In summary—SCA must be used to link a customer's identity to their SCA credentials. This means that if credentials are issued or re-issued remotely then the associated identity verification process must use an alternative set of authentication credentials to those used in the account access process.

PSD2 REQUIREMENT	RTS REQUIREMENT	MEANING
PSD2 Article 4(3) requires that all electronic remote access to payment accounts must be based on the use of two or more authentication credentials categorised as: • knowledge (something only the user knows) • possession (something only the user possesses) • inherence (something the user is)	RTS Article 21: Payment service providers shall ensure that only the payment service user is associated with the personalised security credentials, with the authentication devices and the software in a secure manner	PSD2 requires that only the genuine customer is linked to the authentication credentials
	RTS Article 27: The association via a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software shall be performed using strong customer authentication	PSD2 requires that where authentication credentials are linked to the customer's identity remotely this also uses strong customer authentication

consult hyperion JUMIO

GDPR

GDPR is an updated data protection regulation, effective in European member states from May 2018. It introduces significant penalties for all organisations—not just payment institutions—that fail to protect their customers' data and which do not provide prompt notification of a subsequent data breach. These fines can be up to €20 million or 4% of total worldwide annual revenue:

Article 4(f) of GDPR states:

> **"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')."**

Article 83 indicates that the decision to levy a penalty and the amount to be levied is dependent on a number of criteria including:

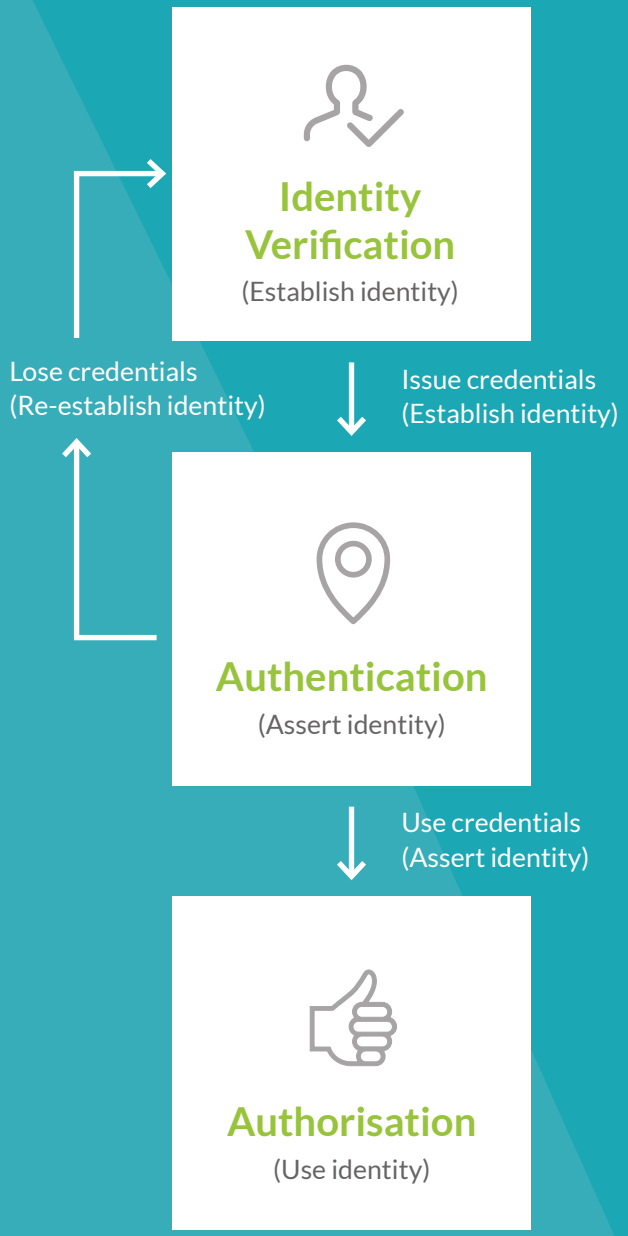
> **"The intentional or negligent character of the infringement."**

Given the requirements around Strong Customer Authentication (SCA) in PSD2 it is likely that a failure to implement this solution according to best principles will attract significant GDPR penalties for financial institution[1].

From this it follows that if a fraudster can gain control of a customer account by resetting their credentials and spoofing the reset process they will have automatically enabled a data breach. At this point the requirements of GDPR come into play.

Clearly this creates a dilemma for payment institutions. They are forced to open up access to accounts through PSD2 but they face significant penalties under GDPR if that access is breached. The option of not opening account access is not available to them: this is, to put it mildly, a significant challenge.

[1] *The new German Federal Data Protection Act "... allows for the sanctioning of individuals, leading to a risk of liability for managers, employees and in-house data protection officers of up to three years imprisonment."*



Digital Identity in the Context of PSD2 and GDPR

So how does the digital identification process link to the authentication process?

In Consult Hyperion's Digital Identity practice we spend a lot of time addressing this question for organisations across multiple sectors, but especially for banks. We have built a three-stage model to explain how the processes are linked—which shows that it's not possible to consider the security of authentication without addressing the security of the identity verification stage.

Digital identity can be divided into three distinct phases:

Identity verification: the 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. This phase also includes establishing authentication credentials that will allow the customer to assert their identity in the future without needing to redo the relatively expensive identification process each time.

Authentication: the process of asserting a previously established identity. Typically this will involve asserting a particular identity (account number or other identifier) and using the previously established authentication credentials to demonstrate ownership of the identity. In the background, contextual information (device, location, time, etc.) will be used to spot high risk and potentially fraudulent activity.

Authorisation: the process of determining what the customer is allowed to do having asserted their identity to a particular level of assurance.

As the model shows, all credential issuance and subsequent re-issuance has to link back to the initial identity of the customer. Critically, the design of the process needs to make it possible for the secondary re-identification process to be done without the initial complex and expensive customer verification process being repeated. For instance, you do not want to make the customer come to a bank branch with their identity documents every time they lose their authentication credentials.

Identity and Authentication within PSD2

In the context of the three-stage identity model the PSD2 RTS (Payment Service Directive 2 Regulatory Technical Standards) explicitly covers Authentication and Authorisation. The Identity Verification process comes under Articles 21 and 27, which specify the processes of associating a digital identity with an account and remotely issuing and re-issuing credentials linked to that identity using Strong Customer Authentication (SCA).

As our three-stage digital identity model shows, using SCA during these steps is essential because weak identification and re-identification processes will negate the strength of the authentication step. If a customer's credentials are wrongly associated with a fraudster then the criminal will be able to perform authenticated transactions on the customer's account.

In financial services the initial identity establishment is often done through a face-to-face Customer Due Diligence or Know Your Customer (KYC) process, but this is complex, time-consuming and not effective in an online environment where the requirement is to re-issue credentials. PSD2 makes clear that identification and re-identification processes may be supported by remote solutions.

To meet the intent of PSD2, the processes to issue and re-issue credentials must be analogous to the remote Customer Due Diligence support processes, must use two alternative SCA credentials and must be largely automated to achieve high levels of throughput and reduce friction.

Additionally, they must achieve very high levels of accuracy, otherwise customers will be locked out of their accounts unnecessarily, or it may be possible for fraudsters to subvert the process.

Strong Customer Authentication Credential Reset Under PSD2

We can see that the PSD2 requirement for widespread use of Strong Customer Authentication (SCA) will inevitably lead to an increase in credential reset requests. We expect that the most common implementation of SCA will use a smart phone (Possession factor) and either a biometric (Inherence factor) or a passcode (Knowledge factor). If the device is lost, broken or stolen the customer will need a means to regain access to their account, often in a remote situation and on a new, unauthenticated device.

Under PSD2 RTS Article 21 banks are only allowed to associate a customer identity with the SCA credentials in a secure facility or, if performed remotely, using two-factor authentication. So, if the customer has lost or forgotten their credentials—for instance, by losing their phone—then they must either use two different factors to support a remote credential re-issuance or must wait for a physical credential re-issuance.

The penalties for breaching this requirement will be determined by national PSD2 legislation, although the form of those penalties is as of yet unknown. However, implementing a weak credential reset process will be a target for criminals, and a breach of this process that exposes customer account data will attract penalties under GDPR.

The intent behind the PSD2 requirements is clear and meets the standard expected in this situation—the credential reset mechanism should be at least as secure as the methods it is resetting: otherwise fraudsters can force a credential reset and then break the reset methods. As these often involve using personal knowledge, this makes the customer's account vulnerable to attacks mounted using social engineering and phishing. The rule is that any strong reset method must revert to the root identity of the customer.

How a Reset Attack Works

STEP 1	fraudster gains access to email accounts via a phishing attack
STEP 2	fraudster analyses email traffic and past emails, identifies financial service providers
STEP 3	fraudster accesses social media accounts, gathers personal information
STEP 4	fraudster triggers a reset on the financial service provider (e.g. “Forgotten password”)
STEP 5	fraudster responds to reset request to email account or contacts customer services with personal details, attacking a weak reset process
STEP 6	fraudster now has control of payment account
STEP 7	fraudster blocks access to email accounts to prevent genuine customer resetting
STEP 8	fraudster starts transferring money out of account

consult hyperion JUMIO

Business Threat of Credential Reset Breaches

The requirements around PSD2 credential reset pose a significant set of problems for both banks and their customers:

1. If the credential reset process is **weak** it exposes payment institutions to attacks and penalties under PSD2 and GDPR. In the latter instances, this may lead to fines of up to 4% of global annual revenues.

2. If the credential reset process is **slow**—for instance requiring face-to-face verification of identity—it will lead to transaction abandonment and the loss of customers migrating to more sophisticated and frictionless providers.

3. If the credential reset process is **inaccurate** it will lead to the customer facing false acceptances—in which fraudsters can take over a customer's account, or false rejection, in which valid customers are locked out of their accounts. This will lead to the loss of customer business and potentially exposure to regulatory penalties.

4. If the credential reset process is **complex** it will inconvenience the customer and significantly add to the ongoing costs of compliance, particularly where high levels of customer service intervention are required. This will increase costs and may lead to loss of customer business.

Requirement	PSD2 requires strong customer identification Significant increase in credential reset as customers forget credentials, lose devices and swap phones			
Problem	Credential reset is slow/ offline	Credential reset is weak	Credential reset is inaccurate	Credential reset is complex
Customer Issue	Customer is inconvenienced	Customer credentials compromised	Customer faces false acceptance/ rejection	Customer is inconvenienced
Bank Issue	Bank loses business	Bank faces PSD2/GDPR penalties	Bank loses business/faces penalties	Bank compliance costs increase significantly
Solution	?	?	?	?

It is clear that the requirements for Strong Customer Identity Verification (SCeID) under PSD2 are not at all trivial—they are significant in terms of compliance costs, future business revenues, customer retention and regulatory penalties. In the final section of this paper we look at the potential solutions to this challenge from both a customer and a banking perspective.

consult hyperion JUMIO

Recommendations

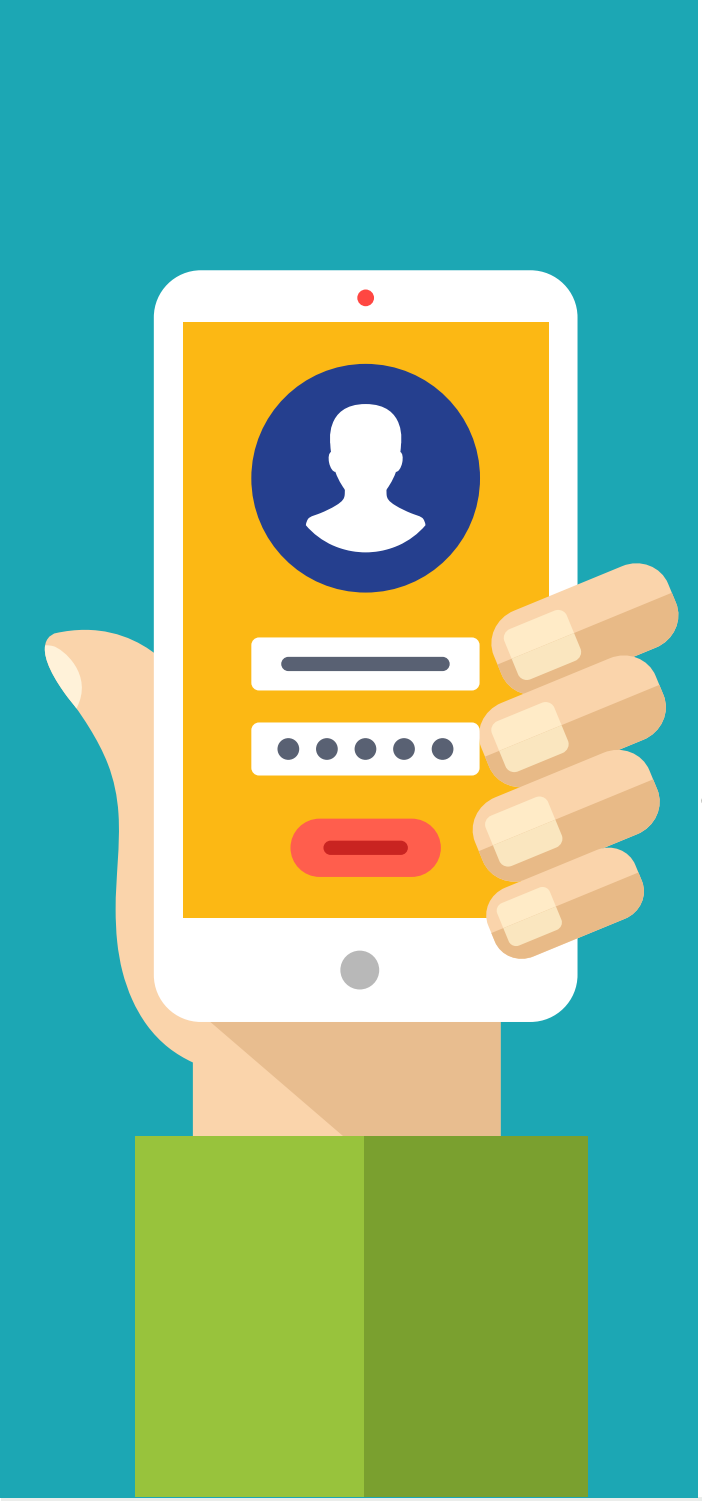
As we have seen the combination of forthcoming European regulations, coupled with the potential impact on customers, is potentially a serious issue for payment institutions. However, it is important to recognise that the regulations are primarily about intent—there is no expectation that a bank can completely stop fraud, only that they take all reasonable precautions to minimise it.

Moreover, the 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." [2]

PSD2: all payment functions that can result in fraud must be protected by two-factor SCA PSD2 Article 4(3)	Customers will lose and forget credentials more often—and need reset more often	Reset must ensure only genuine customer is linked to new credentials PSD2 SCA RTS Article 21	Breaching PSD2 SCA may also breach GDPR by allowing access to customer data GDPR Article 4	Identity proofing using different two factors required, otherwise will be target for fraudsters PSD SCA RTS Article 27	Use government issued identity documents and biometric matching
Exemptions apply but SCA will be required much more often than today	**Increased costs for bank and increased friction for customer**	**"Hidden" PSD2 requirement—but is explicit in intent**	**Significant fine and penalties under GDPR** **GDPR Article 83**	**Online, real-time ID document and verification process**	**Bank grade systems supporting AMLD already exist**

Well designed on-line identity proofing and verification matching service can support 4AMLD, PSD2 and GDPR requirements, reduce costs and improve customer service.

[2] *EBF – Driving Digital Transformation – The EBF blueprint for digital banking and policy change*



Finding solutions that meet these requirements, minimising the compliance costs, ensuring high levels of customer satisfaction and keeping fraud down is a challenge, but we believe that mechanisms to deliver Strong Customer Identity Verification (SCeID) solutions already exist, based on systems that have been developed to assist effective Customer Due Diligence services.

Currently these are the only technologies in operation that can meet the requirements. eIDAS[3], the European regulation on electronic identification, is a possible alternative but this has yet to be fully deployed, is unproven and does not support the full range of PSD2 use cases. For instance, some eIDAS implementations are smart card-based and require access to a reader and PC, which is not much use if all you have is a smartphone.

[3] *"Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC". – EUR LEX Europa, 2017 [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG*

Create New Value for Your Business and Your Customers

Any solution must address the four main problems:

Requirement	PSD2 requires strong customer identification Significant increase in credential reset as customers forget credentials, lose devices and swap phones			
Problem	Credential reset is slow/ offline	Credential reset is weak	Credential reset is inaccurate	Credential reset is complex
Customer Issue	Customer is inconvenienced	Customer credentials compromised	Customer faces false acceptance/ rejection	Customer is inconvenienced
Bank Issue	Bank loses business	Bank faces PSD2/GDPR penalties	Bank loses business/faces penalties	Bank compliance costs increase significantly
Solution	SCeID must be online, real-time	SCeID must use two factor authentication based on real ID	SCeID must have human involvement	SCeID should be a mainly automated service

consult hyperion

JUMIO

1 **If the credential reset process is weak**

Requirement: Use two-factor authentication meeting the requirements of PSD2 Strong Customer Authentication (SCA).

2 **If the credential reset process is slow**

Requirement: The process must be implemented on-line, remotely, and performed as near to real-time as is possible, while not sacrificing the quality of the identity verification process.

3 **If the credential reset process is inaccurate**

Requirement: The process must have an accuracy rate as close to 100%, a level only possible with some human intervention.

4 **If the credential reset process is complex**

Requirement: Be highly automated and incremental to existing payment institution processes in order to minimise the additional costs associated with compliance.

Solving the Reset Challenge

Implementing new systems and solutions to address these four problems will be difficult, as it will potentially open up unknown weaknesses. In the event of a subsequent attack it will be necessary to justify the design decisions made in this process to show that the solutions meet best practice as defined by the industry.

Fortunately, existing technology can address the requirement. Under the various anti-money laundering regulations there is provision for supporting both the initial identification and the secondary re-identification process using remote technology that addresses the critical requirements of the reset process:

> **"Technologies allowing for digital on-boarding should also be considered as equivalent and valid identification methods."**
>
> -EBA (European Banking Federation)[4]

1. **It is strong:** It uses a combination of a government issued identity document which can be verified online via a photograph of the document which is matched in real time to a database (Possession) and a facial biometric which matches a live picture using a webcam or smartphone camera (Inherence) against the identity document photograph.

2. **It is fast:** Document verification against existing documents can be matched in seconds and the facial biometric matching against the document photograph are both fast processes. (Add estimated average time).

3. **It is accurate:** The facial biometric matching must be enhanced by human interaction to ensure a very high level of success. This slows the process down, but improves the accuracy—and under PSD2 and GDPR this is essential.

4. **It is simple:** The entire solution can be globally outsourced, with many existing examples, including the biggest banks in the world, using the same technology to support their Customer Due Diligence processes.

[4] *EBF, Driving the Digital Transformation, The EBF blueprint for digital banking and policy change, p15*

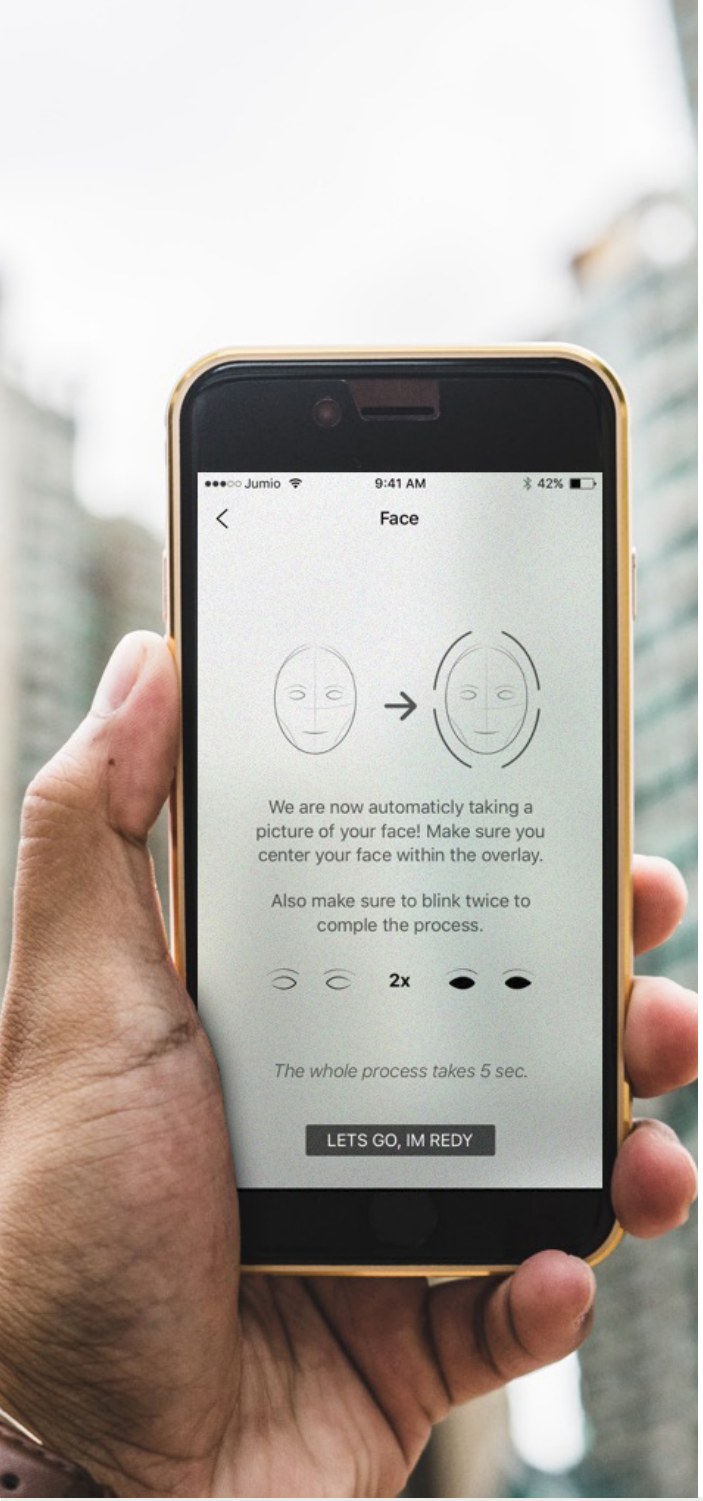
The PSD2 Credential Reset Process

Must be

STRONG	FAST	ACCURATE	SIMPLE
Meets PSD2 SCA	Gets customers transacting quickly	Links the correct customer	Convenient for customer
Uses two factors	On-line and real-time	Uses proven technology and services	Limits additonal compliance costs
Identity document verification (possession) + Live facial biometric matching (inherence)	Real-time online identity document verification + Facial biometric matching in under 90 seconds	High level of accuracy due to human interaction to perform final analysis	Service based model that already meets 4AMLD requirements

Use best in class identity verification service
Solution that meets PSD2 intent and which isolates the GDPT/ePR problem

consult hyperion JUMIO

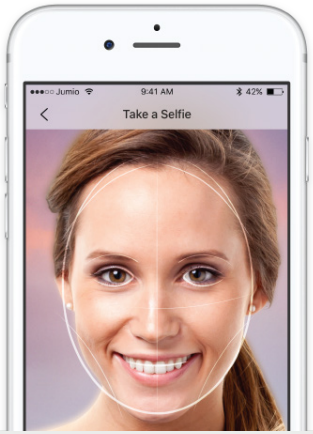


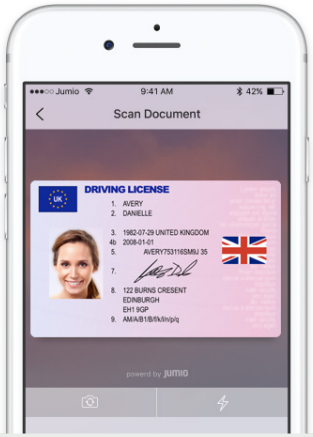
The solution that can deliver on all of these requirements has already been deployed in the financial services industry by Jumio. The leading digital verification company delivers the highest accuracy rates in the digital verification industry in just seconds, compared to the complexity of interacting with a customer service team, which can take up to days or hours.

Jumio's digital verification technology is ideally placed to help regulated entities to deliver customer identity verification for remote transactions. Jumio's Netverify® Trusted Identity as a Service (TIaaS) combines ID Verification, Identity Verification, and Document Verification for a complete solution to establish the real-world identity of a customer. Leveraging advanced technology, such as biometric facial recognition, machine learning and intelligent process automation (IPA), Netverify TIaaS meets KYC and AML regulatory compliance; all while providing an excellent customer experience.

Leading European incumbent and challenger banks have been using Jumio's solution to combat the sophisticated nature of identity crime, improve the identity process, helping banks and other financial institutions further establish digital identities in continuously new legislative scenarios.

If you would like to learn more about how Jumio's Netverify TIaaS can help your firm comply with digital identity requirements within today's legislative scenarios, please email the team at marketing: anamaria.leonte@jumio.com





Conclusions

Identity verification is at the heart of PSD2, and must be supported by a Strong Customer Identity Verification (SCeID) process using two-factor authentication. A failure to implement a Strong Customer Identity Verification will expose payment institutions to liabilities under both PSD2 and GDPR, where the penalties can be as high as 4% of annual global turnover. Existing technology, built to support the KYC requirements associated with anti-money laundering regulations, can be used to support a strong remote identity verification process that protects payments institutions against regulatory and business risks, reduces compliance costs, retains customers and supports increasing market share.

About Consult Hyperion

Consult Hyperion is an independent strategic and technical consultancy based in the UK and US, specialising in secure electronic transactions. We help organisations around the world exploit new technology for secure electronic payments and identity transaction services from mobile payments and “chip and PIN” to contactless ticketing and federated identity. Our aim is to assist customers in reaching their goals in a timely and cost-effective way. We support the deployment of practical solutions using the most appropriate technologies and have globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to transactional systems and applications.

About Jumio

Jumio, the creator of Netverify® Trusted Identity as a Service (TIaaS), 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 like biometric facial recognition and machine learning, Jumio helps customers to meet regulatory compliance including KYC and AML and tie the digital identity to the physical world. Jumio has verified more than 50 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, higher education, retail, travel and online gaming sectors. Based in Palo Alto, Jumio operates globally with offices in the US and Europe, and has been the recipient of numerous awards for innovation. For more information, please visit www.jumio.com.

Appendix

Term	What it stands for	What it is
AISP	Account Information Service Provider	A PSD2 regulated entity, which uses the account information API to an ASPSP to provide services to a consumer. Typically this might involve account information aggregration from multiple ASPSPs.
AMLD	Anti-Money Laundering Directive	EU directive covering anti-money laundering requirements—there are two versions AMLD4 (in effect) and AMLD5 (proposed)
ASPSP	Account Servicing Payment Services Provider	A PSD2 regulated entity, which provides payment accounts to consumers or businesses. Typically this would be a bank, but potentially any institution offering payments. The ASPSP must provide Open APIs for AISPs and PISPs.
EBA	European Banking Association	The European Banking Authority (EBA) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.[5]
eIDAS	Electronic Identification and Signature	EU standard for electronic identity and signature services. Primarily aimed at government services to ensure a common method for accessing these acorss the EU.
ePR	ePrivacy Regulation	EU regulation covering the conditions under which consumers may be contacted electronically.
GDPR	General Data Protection Regulation	EU regulation for data protection standards, specifically covering consumer consent and corporate responses to data breaches

[5] *EBA, 2017, About Us [website] http://www.eba.europa.eu/about-us;jsessionid=271CC20E886D49460D838E763A1E5FD4*

Term	What it stands for	What it is
KYC	Know Your Customer	The process of verifying a customer's identity, otherwise referred to as Customer Due Diligence
Netverify® TIaaS	Netverify Trusted Identity as a Service	Netverify TIaaS is the trusted identity service for financial companies across the globe, helping them to faster and easily verify the identity of their customers online, while also helping them meet KYC and AML requirements.
PISP	Payment Initiation Service Provider	A PSD2 regulated entity which uses the payment initiating API to an APSP to trigger a direct credit transfer from the payer's account to the payee's account.
PSD2	Payment Services Directive II	EU's Second Payment Services Directive. The directive introduces a complex range of rules over and above the original PSD in 2007, reducing fraud through SCA and sponsoring innovation by opening up APIs to ASPSPs and driving down the end-user costs of existing card based payment channels.
RTS	Regulatory Technical Standards	These documents specify detailed technical requirements outlined in regulations. For instance, requirements on the implementation of SCA are provided in an RTS.
SCA	Strong Customer Authentication	As defined in PSD2 and SCA RTS this is two-factor authentication. The permitted factors are Possession, Knowledge and Inherence and the factors used must be independent of each other such that a breach of one does not imply a breach of the other.
SCeID	Strong Customer Identity Verification	Process of verifying a customer's identity by using two independent identification factors, analogous to those used in SCA. The factors used in a PSD2 compliant SCeID must be different to those used in the SCA process.