iovation®
A TransUnion® Company

INDUSTRY WHITE PAPER

Gain Market Advantage by Elegantly Solving for SCA Requirements Under PSD2

Maximize SCA Exemptions,
Reduce Friction for Customers

Table Of Contents

Introduction

The EU Payment Services Directive (PSD2), presents any business that processes online payments or provides account related services in the European Economic Area (EEA) with the challenge of balancing the Strong Customer Authentication (SCA) requirements with a seamless buyer's journey. This is problematic because consumers are increasingly sensitive to any added friction and are voting with their feet. An estimated 70% of consumers abandon online forms due to poor experience. [1] So the question is, how do you balance security with customer experience? To gain competitive advantage in the new PSD2 landscape, payment processors and merchants will need to collaborate closely to maximize SCA exemptions and reduce friction for those transactions subject to SCA requirements.

The Regulatory Technical Standards (RTS) have instilled the increased importance of fraud prevention. To retain control over the buyer's journey merchants will need to work cooperatively with payment processors to reach the highest exemption thresholds. Successful collaboration can provide a major competitive advantage on a number of fronts:

- **One click shopping:** Being able to expedite payment processing for a higher volume of transactions, e.g. all transactions below €500 vs. only transactions below €30 (the default amount).
- **Cost savings:** Reduce the overall number of transactions subject to higher cost SCA checks.
- **Reduced friction:** Only step-up transactions above the exemption threshold or with risk signals to SCA.

This white paper presents how iovation's solutions can help maximize SCA exemptions, and decrease friction for those transactions that are subject to SCA—allowing you to strike the balance between security and a positive customer experience.

PSD2 in a Nutshell

PSD2 is an update to the Payment Services Directive (PSD) that was adopted in 2007 by the European Commission (EC). PSD created the legal foundation for a Single Euro Payments Area (SEPA); essentially establishing a single market for payments (e.g. credit transfers, direct debits, cards) in the European Union. There has been tremendous innovation in the online economy in the last decade meaning that many new services have been added to the economy that were not covered by the original scope of the PSD, making an overhaul essential.

Similar to the GDPR, the geographical reach of PSD2 will be broader. It now takes a 'one leg in' approach meaning that all transactions with at least one party located within the EU will be in scope versus the previous requirement of 'two legs in' where both parties were required to be located in the EU.

The stated objectives of PSD2 are to:

- Make cross-border payments as easy, efficient and secure as national payments within a Member State.
- Reduce the cost of transactions.
- Make payments more secure.
- Increase protection for the consumer.
- Foster innovation and competition in payment services.
- Create a level playing field for all players, including new ones.

For the purposes of this paper we will focus primarily on the objectives to make payments more secure and increase protection for the consumer.

Strong Customer Authentication (SCA) Requirements

One of the biggest changes introduced with PSD2 is the addition of the Strong Customer Authentication (SCA) requirements laid out in the RTS, which require the use of two or more of the following independent factors of authentication:

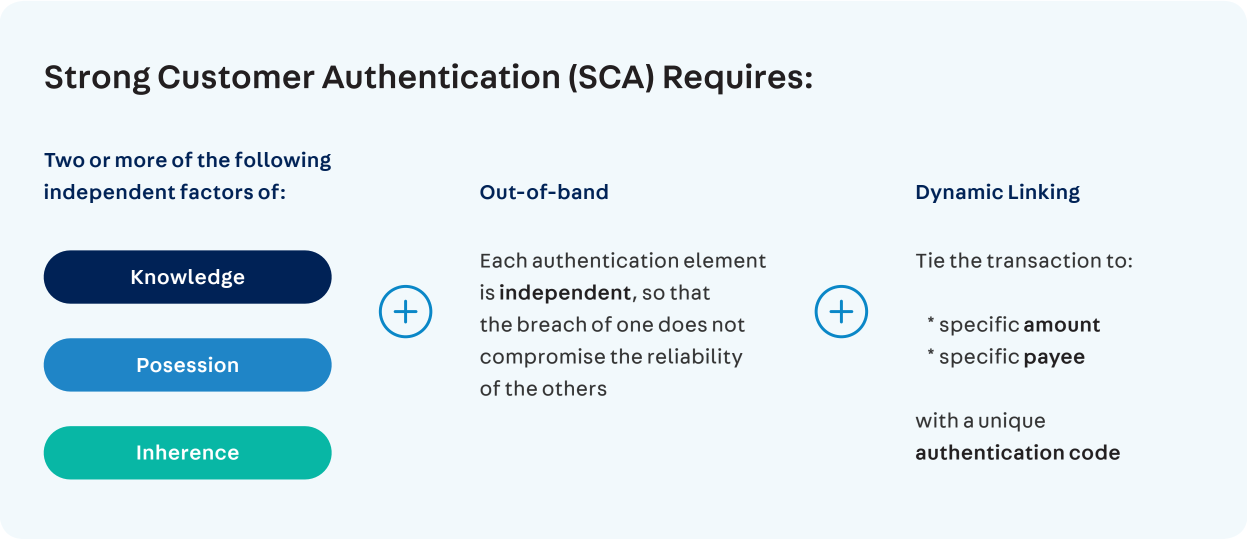
Knowledge – something only the user knows (password, PIN)

Possession – something only the user possesses (key material, token)

Inherence – something uniquely identifying to user (fingerprint, biometrics)

The SCA requirements also call out that the factors must be independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device ...such as a mobile phone. In other words, SCA requires out-of-band authentication, which is the use of separate, secure channels for each authentication factor.

Lastly, an SCA solution is required to provide dynamic linking for remote transactions, essentially tying the transaction both to a specific amount and to a payee with a unique authentication code.



Strong Customer Authentication (SCA) Requires:

Two or more of the following independent factors of:

- Knowledge
- Posession
- Inherence

+

Out-of-band

Each authentication element is **independent**, so that the breach of one does not compromise the reliability of the others

+

Dynamic Linking

Tie the transaction to:

* specific **amount**
* specific **payee**

with a unique **authentication code**

Maximize SCA Exemptions with Risk-Based Transaction Analysis

The good news is that the European Banking Authority (EBA) has made some concessions for Payment Service Providers (PSPs) to seek to exempt more transactions from SCA including: transactions below a certain threshold, recurring payments, and through transaction risk analysis. In Paragraph 21 of the EBA's Response to Industry Concerns they conceded that some exceptions should be allowed for risk-based SCA. The relevant section details:

> *21. [...] the EBA agrees with the view expressed by these respondents that a risk-based approach, including the ability to conduct detailed transaction-risk analysis and fraud monitoring, is essential to achieve the objective under PSD2 of reducing overall fraud. Consequently the EBA arrived at the view that, in accordance with Article 98(2)(a) PSD2, an exemption based on such an analysis should be added in a new Article 16 RTS. The RTS also reiterate the importance of risk and fraud monitoring in general as a necessary complement to the principle of SCA laid out in PSD2 as stated in a new Article 2 RTS.*

Essentially, the EBA comments are consistent with the idea that payment service providers (PSPs) should be able to request exemptions to SCA if they can attain target fraud rates.

Requirements of Risk-Based Transaction Analysis

In order to obtain the exemption based on transaction risk analysis, the solution must operate in real-time and must verify a transaction against anomalies in user behavior. Checkpoints shall include the following:

- Previous spending patterns of the payer
- Payment transaction history of the payer
- Location of the payer and the payee at the time of the payment
- Previous use of the access device or the software provided to the payment service user for SCA

Exemptions thresholds for remote, card-based transactions, are as follows:

Exemption Threshold Value	Reference Fraud Rate % Remote Card-based Payments
€500	<0.01
€250	0.01 - 0.06
€100	0.06 - 0.13
€30	Default rate

The reference fraud rate percentage calculation is:

$$\text{Reference Fraud Rate \%} = \frac{\text{Total value of successful fraudulent transactions}}{\text{Total value of all successful transactions (including SCA and exempted)}}$$

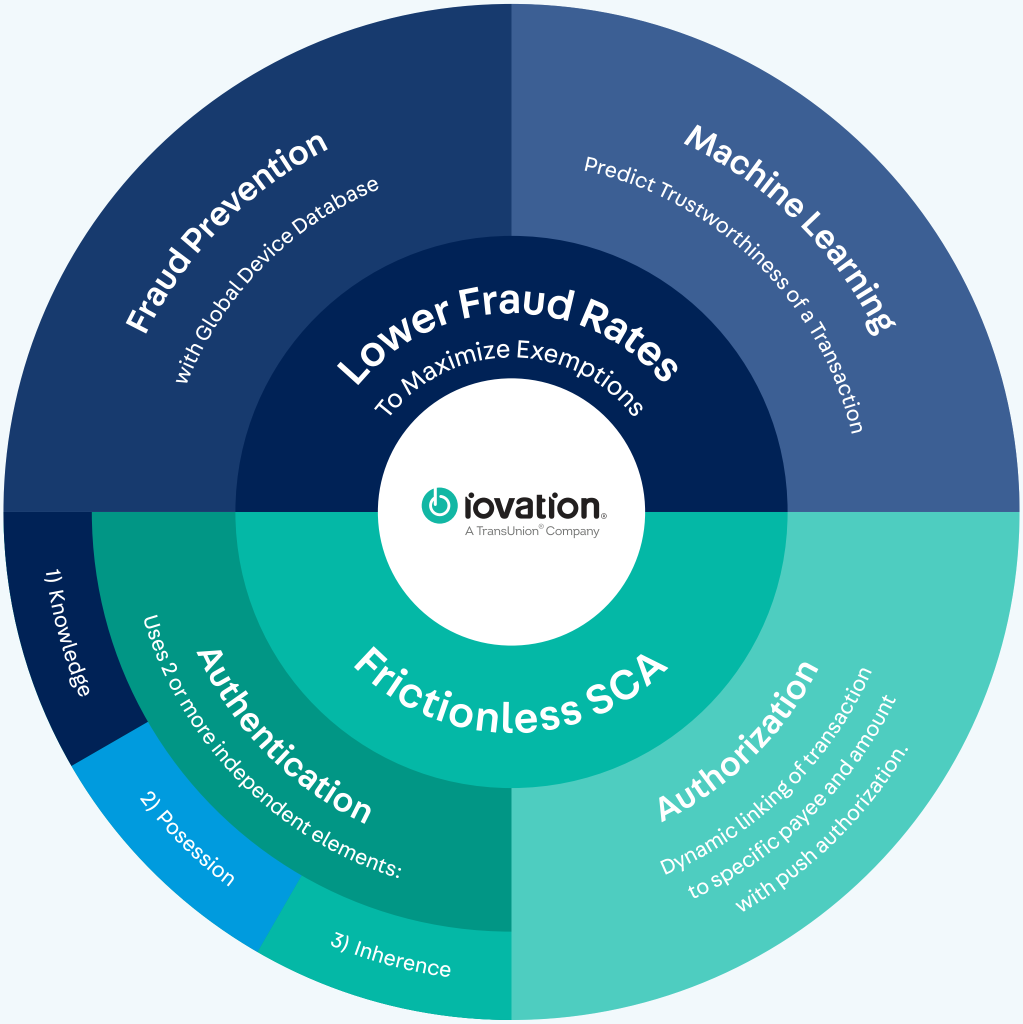
iovation's Response to Risk-Based Transaction Analysis

iovation's deep device intelligence allows us to provide real-time data on the location of the payer at time of payment, and to determine previous use of the access device. This intelligence coupled with your data on previous spending patterns of the payer will allow your business to more confidently decide whether to allow, deny or review each transaction.

iovation's comprehensive fraud solution can help detect and prevent fraud at any high risk touchpoint in the customer journey. Combined with our machine learning technology that predicts the likelihood that a transaction will be fraudulent, you can better prioritize your review queue and catch more fraud. This will ultimately enable you to reduce your fraud rate, maximize your SCA exemptions, and minimize customer friction.

Meet SCA Requirements of PSD2

Maximize Exemptions. Minimize Friction.


Fraud Prevention
with Global Device Database
Machine Learning
Predict Trustworthiness of a Transaction
Lower Fraud Rates
To Maximize Exemptions
iovation
A TransUnion® Company
Frictionless SCA
Authentication
Uses 2 or more independent elements:
1) Knowledge
2) Posession
3) Inherence
Authorization
Dynamic linking of transaction to specific payee and amount with push authorization.

Solving for SCA (MFA without the Friction)

For those transactions still subject to SCA, it will be imperative to reduce friction and provide a seamless authentication flow that won't drive away customers.

In a well-designed system you can incorporate risk signals to tailor the level of authentication to the riskiness of the transaction. So for instance if a customer is logging in from a known device and just wants to view their balance, that's a low risk transaction. But if the same customer logs in from a new, unknown device and wants to make a €2,000 purchase; that's a much riskier transaction. This is why risk insight is so important. Not only will it allow you to apply the right level of authentication it will also help you meet SCA requirements and preserve the customer experience.

iovation's device-based authentication solution, ClearKey, can help lower friction by providing a transparent authentication factor. ClearKey uses the customer's device as a possession factor to satisfy one of required authentication elements for SCA. Customers simply pair their devices with their account. On subsequent visits, they'll be allowed to transparently authenticate if the device matches and there are no risk signals such as the use of a Tor network, geolocation mismatch or detection evasion.

For transactions that need to be stepped up or if a full solution is needed to meet SCA requirements, employ iovation's mobile multifactor authentication (MFA) solution, LaunchKey. LaunchKey provides users with all three types of authentication factors: knowledge, possession, and inherence.

Available methods include: facial scan, fingerprint scan, PIN, circle code, device factor and wearable factor.

All credentials are stored locally on the user's device, eliminating the need to store and protect either biometric data or credentials in a central location.

Additionally, the lightweight SDK can be deployed through your own application so that you don't have to take customers out of your brand experience. All authentication processes across both online and offline platforms (web, mobile web, application, call center, kiosk, ATM, IoT devices) can be managed right through the users mobile device. All while maintaining your own brand identity.

The RTS also set a much higher bar for securing users' credentials. LaunchKey was built from day one with the high security standards, including:

- **Decentralized, anonymous architecture:** user credentials are stored locally on the user's device, eliminating a central credential store that is a common attack target for password-based, and even many two-factor authentication solutions.
- **Out of band authentication:** both independent authentication elements are delivered in one service, the user's mobile device. Each element uses its own secure channel so that the compromise of one element does not compromise the other.
- **Advanced public-key cryptography:** iovation doesn't possess the private keys necessary to decrypt requests and responses that cross iovation's network meaning that our authentication is well protected from a centralized attack on the service provider.
- **Dynamic Linking:** a unique authentication code is generated for each transaction that ties the transaction to a specific amount and payee.

LaunchKey has the ability to include contextual information within the authentication request packet. This information can be anything from the transaction amount to a few paragraphs of informative text. This allows you to dynamically link the transaction to a specific amount and payee with a unique authentication code, which is one of the requirements laid out in Article 5 of the RTS.

Authentication Built with the Customer in Mind

It's easy to lose sight of the customer experience when you're adding security to the customer journey. With LaunchKey, the entire authentication experience was built around customers from the start. Firstly, the modes of authentication are user-selectable allowing customers to choose the way they are most comfortable authenticating. This creates buy-in as customers are being asked to participate in securing their account. This is also helpful for managing generational and early adopter differences. Since LaunchKey uses the built-in features of mobile devices, additional authentication factors can be added as they become available. So for instance you might find that millennials are more comfortable with using newer technology such as facial scans. For boomers you might find that they are more comfortable with PINs or thumbprints. This flexibility allows you to add new modes of authentication as they are gaining market acceptance without having to impact all customers.

Security doesn't have to come at the cost of degrading the customer experience. To achieve market differentiation in the age of PSD2, PSPs and merchants will need to closely collaborate to optimize their fraud prevention strategies while also elegantly solving for SCA requirements. Learn how iovation's solutions can help your business.

How iovation Can Help Meet the Regulatory Technical Standards

Requirement	iovation's Solutions
Article 2 General authentication requirements **RTS 2.1** - Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions for the purpose of the implementation of the security measures referred to in points a and b of Article 1. Those mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalized security credentials.	● iovation can protect the entire customer journey, from user authentication to transaction monitoring to detecting unauthorised or fraudulent payments. ● Our unparalleled ability to track and understand the reputation of a device over time, across different accounts and geographies, allows you to detect and prevent payment fraud. ● Our advanced machine learning predicts the likelihood that a transaction will be fraudulent, allowing you to better prioritize your review queue and catch more fraud.

RTS 2.2
Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

a. Lists of compromised or stolen authentication elements;

b. The amount of each payment transaction;

c. Known fraud scenarios in the provision of payment services;

d. Signs of malware infection in any sessions of the authentication procedure;

e. In case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

- Failed authentication methods are included in the authentication response. Deregistration is provided for devices that have been lost or stolen.
- Amount of payment transaction can be recorded as part of payment transaction monitoring.
- We log known fraud reports in our unique device reputation database. With over 66M incidents reported, this comprehensive database stops fraudsters as they move across businesses, industries and countries. iovation's solutions are meant to provide a high level of flexibility to cover both known and emerging attack vectors.
- iovation does not detect malware on a device, but we provide a number of device integrity checks. Specifically, we check for jailbroken and rooted devices, which is a common vector for malware.
- iovation maintains transaction history along with giving insight into abnormal use of devices including if a device has been rooted or jailbroken, cloaking attempts, bot detection, velocity detection, geolocation spoofing, and geolocation mismatch.

Article 4 Authentication code

RTS 4.1 - Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.

The authentication code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

- iovation's device-based authentication solution provides the possession element for SCA.
- iovation's mobile multifactor authentication provides all three elements of:
  - **Knowledge** (PINs, circle codes)
  - **Possession** (device, wearable factor)
  - **Inherence** (fingerprint, facial scan)
- Every authorization request is unique, can only be responded to once, and any successive authorization attempts require a new authorization request.

RTS 4.2 - For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:

a. No information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;

b. It is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;

c. The authentication code cannot be forged.

- iovation's mobile MFA solution leverages a decentralized architecture in which all authentication data (e.g. passcodes, location data, biometric signatures, etc.) is distributed and stored on each end user's mobile device where it is inaccessible to both iovation and our subscribers.
- Our authentication request and response packages are encrypted in such a way that any change to the data within the package would invalidate its signature, revealing the fact that an authentication code was forged. This significantly limits the ability to tamper.

RTS 4.3 - Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

a. Where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;

b. The number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 97(1) of Directive (EU) 2015/2366 shall be temporarily or permanently blocked, shall not exceed five within a given period of time;

c. The communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter V;

d. The maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed 5 minutes.

- Our MFA solution employs public key cryptography in such a way that the request and response packages that traverse the authenticator are end-to-end encrypted and cryptographically signed and verified for authenticity. As such, only the end user's device possesses the private key necessary to decrypt requests, and only your services possess the private key necessary to decrypt responses.
- iovation's MFA solution can be configured to lock after a prescribed number of failed authentication attempts, including five failed attempts.

Article 5 Dynamic linking

RTS 5.1 - Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:

a. The payer is made aware of the amount of the payment transaction and of the payee;

b. The authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

c. The authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;

d. Any change to the amount or the payee results in the invalidation of the authentication code generated.

- iovation's MFA solution provides custom text that can be supplied within an authorization request in multiple forms: as part of the request details, as part of the request title, or as part of the request push notification, to ensure the payer is aware of the amount of a transaction and of the payee.
- With mobile MFA all information within an authentication request is cryptographically tied to the request response itself, including the amount of the payment transaction.
- Request and response packages are encrypted in such a way that any change to the data within the package would invalidate its signature thereby revealing the fact that something in the package was altered. This significantly limits the ability to tamper.

RTS 5.2 - For the purpose of paragraph 1, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:

a. The amount of the transaction and the payee throughout all of the phases of the authentication

b. The information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.

- iovation's MFA solution encrypts request and response packages in such a way that any change to the data within the package would invalidate its signature thereby revealing the fact that something in the package was altered. This ensures the confidentiality, authenticity and integrity of each transaction throughout all phases of the authentication.

RTS 5.3 - For the purpose of paragraph 1(b) and where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 the following requirements for the authentication code shall apply:

a. In relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 75(1) of that Directive, the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction;

b. In relation to payment transactions for which the payer has given consent to execute a batch of remote electronic payment transactions to one or several payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees.

- iovation’s MFA solution ties the authentication code to the total amount of the batch of payment transactions and to the specified payees by including contextual information in the encrypted authentication package which generates a unique authentication code.

Article 6 Requirements of the elements categorised as knowledge

RTS 6.1 - Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.

RTS 6.2 - The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.

Article 7 Requirements of the elements categorised as possession

RTS 7.1 - Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.

RTS 7.2 - The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.

Article 8 Requirements of devices and software linked to elements categorised as inherence

RTS 8.1 - Payment service providers shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the payment service providers shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.

RTS 8.2 - The use by the payer of those elements shall be subject to measures ensuring that those devices and the software guarantee resistance against unauthorised use of the elements through access to the devices and the software.

iovation's mobile MFA solution was built from day one with high security standards, including:

- **Decentralized, anonymous architecture:** User credentials are stored locally on the user's device, eliminating a central credential store that is a common attack target for password-based authentication.
- **Out of band authentication:** Both independent authentication elements are delivered in one service, the user's mobile device. Each element uses its own secure channel so that the compromise of one element does not compromise the other.
- **Advanced public-key cryptography:** iovation doesn't possess the private keys necessary to decrypt requests and responses that cross iovation's network meaning that our authentication is well protected from breaches.

This provides a high level of assurance that all three authentication elements: knowledge, possession and inherence are secured from being uncovered by, disclosed to, or replicated by unauthorised parties.

Article 9 Independence of the elements

RTS 9.1 - Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.

- All authentication methods in iovation's mobile MFA solution are independent and segregated ensuring that the compromise of one element does not jeopardize another.

RTS 9.2 - Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.	● A number of features are included in iovation's MFA solution to mitigate compromising scenarios such as a lost or stolen device. For instance, the authenticators can be remotely unlinked and rendered inoperable in the case of a stolen device.
RTS 9.3 - For the purposes of paragraph 2, the mitigating measures shall include each of the following: a. The use of separated secure execution environments through the software installed inside the multi-purpose device; b. Mechanisms to ensure that the software or device has not been altered by the payer or by a third party; c. Where alterations have taken place, mechanisms to mitigate the consequences thereof.	● We leverage secure execution environments for authentication methods. ● iovation's authentication request and response packages are encrypted in such a way that any change to the data within the package would invalidate its signature, revealing the fact that an authentication code was forged. This significantly limits the ability to tamper.

Article 18 Transaction risk analysis

RTS 18.1 - Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.

RTS 18.2 - An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

a. The fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for 'remote electronic card-based payments' and 'remote electronic credit transfers' respectively;

b. The amount of the transaction does not exceed the relevant exemption threshold value ('ETV') specified in the table set out in the Annex;

c. Payment service providers as a result of performing a real time risk analysis have not identified any of the following:

    i. Abnormal spending or behavioural pattern of the payer;

    ii. Unusual information about the payer's device/ software access;

    iii. Malware infection in any session of the authentication procedure;

    iv. Known fraud scenario in the provision of payment services;

    v. Abnormal location of the payer;

    vi. High-risk location of the payee.

iovation's fraud prevention solution can:

- Give insight on monetary value per account or device.

- Detect abnormal behavior such as if a device has been rooted or jailbroken, device spoofing, bot detection, velocity detection, geolocation spoofing, and geolocation mismatch.

- Detect indicators of malware vulnerability using device integrity checks which look for jailbroken and rooted devices.

- Track known fraud reports in our unique device reputation database. With over 66M incidents reported, this comprehensive database stops fraudsters as they move across businesses, industries and countries. iovation's solutions are meant to provide a high level of flexibility to cover both known and emerging attack vectors.

- Detect location and use rules to blacklist high risk locations

RTS 18.3 - Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

a. The previous spending patterns of the individual payment service user;

b. The payment transaction history of each of the payment service provider's payment service users;

c. The location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;

d. The identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history.

- Our fraud prevention solution tracks monetary amounts by account and by device. Rules can be set to trigger when the amount transacted by an account or device meets or exceeds a set threshold within a specific period of time.
- Our service provides geolocation and IP data for the payer.
- Our solution provides insights to assist PSPs in making an assessment on whether a transaction should be allowed, denied or reviewed. By combining risk-based factors into a risk score for each individual transaction the PSP can determine whether a specific payment should be allowed without strong customer authentication based on risk insights.

Article 22 General requirements

RTS 22.1 - Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.

- iovation's MFA solution encrypts request and response packages in such a way that any change to the data within the package would invalidate its signature thereby revealing the fact that something in the package was altered. This ensures the confidentiality, authenticity and integrity of each transaction throughout all phases of the authentication.

RTS 22.2 - For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

a. Personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;

b. Personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text;

c. Secret cryptographic material is protected from unauthorised disclosure.

iovation's MFA solution ensures:

- Security credentials are masked when displayed
- Security credentials are fully encrypted. Additionally our solution uses a decentralized, anonymous architecture meaning that user credentials are stored locally on the user's device, eliminating a central credential store that is a common attack target for password-based authentication.

RTS 22.3 - Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.

- iovation fully documents our cryptographic and data security practices.

RTS 22.4 - Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards.

- Our MFA solution uses advanced public-key cryptography, which means iovation doesn’t possess the private keys necessary to decrypt requests and responses that cross iovation’s network making our authentication well protected from breaches.
- LaunchKey takes advantage of multiple things to secure the environment through which the authentication flow takes place including leveraging public key cryptography and digital signatures to secure the authentication data both at rest and in transit, as well as the employment of secure and trusted storage environments (e.g. Keychain, Secure Enclave) on the mobile devices themselves. There are also further software protections in place to limit the ways in which the mobile devices and other apps on the device can interact with the authenticator, and this includes the detection and prevention of jailbroken/rooted devices that could otherwise allow the installation of malicious apps capable of syphoning sensitive data.

Article 23 Creation and transmission of credentials

Payment service providers shall ensure that the creation of personalised security credentials is performed in a secure environment.

They shall mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.

- iovation’s authenticators are both securely provisioned, and can be easily deprovisioned if lost or stolen by virtue of our remote unlinking capability. With regards to the copying of authenticators, we have protections against that as well.

Article 25 Delivery of credentials, authentication devices and software

RTS 25.1 - Payment service providers shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.

RTS 25.2 - For the purpose of paragraph 1, payment service providers shall at least apply each of the following measures:

a. Effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment service user;

b. Mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the internet;

c. Arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service provider or through a remote channel:

    i. No unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel;

    ii. The delivered personalised security credentials, authentication devices or software require activation before usage;

d. Arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software have to be activated before their first use, the activation shall take place in a secure environment in accordance with the association procedures referred to in Article 24.

- A number of features are included in our MFA solution to mitigate compromising scenarios such as a loss, theft or copying of a device. For instance the authenticators can be remotely unlinked and rendered inoperable in the case of a stolen device.

- iovation’s MFA solution encrypts request and response packages in such a way that any change to the data within the package would invalidate its signature thereby revealing the fact that something in the package was altered. This ensures the confidentiality, authenticity and integrity of each transaction throughout all phases of the authentication.

Article 28 Requirements for identification

RTS 28.1 - Payment service providers shall ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.

RTS 28.2 - Payment service providers shall ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

- All requests to our mobile MFA solution are encrypted and signed in such a fashion that only the recipient's device can decrypt and respond thereby making it highly unlikely a request for an out-of-band process to be rerouted.

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the web a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multifactor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation
A TransUnion® Company

Global Headquarters

iovation Inc
555 SW Oak Street,
Suite #300
Portland, OR 97204 USA

PH	+1 (503) 224 - 6010
FX	+1 (503) 224 - 1581
EMAIL	info@iovation.com

iovation.com