OneSpan
Be bold. Be secure.

ENABLING PSD2-COMPLIANT FRAUD MONITORING WITH ONESPAN RISK ANALYTICS

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

On 27 November 2017, the European Commission adopted the Regulatory Technical Standards (RTS) for Strong Customer Authentication (SCA) and Common and Secure Open Standards of Communication, supplementing the Revised Payment Services Directive (PSD2). They were published in the Official Journal of the European Union on 13 March 2018 and will be enforced starting 14 September 2019. The RTS document introduces general requirements for fraud monitoring along with SCA to detect and prevent fraudulent payments. Fraud monitoring becomes mandatory for all the cases explained in this paper.

Our white paper provides Payment Service Providers (PSPs) with an analysis of the impact these requirements have on the digital retail channel. We review the main aspects of the RTS and recommend how PSPs should establish their fraud prevention and risk analysis strategy. Finally, we highlight the solutions best suited to achieve compliance and beyond.

The Regulatory Technical Standards also details a range of exemptions from SCA. These exemptions are included to compensate for the expected negative impact on the rate of successfully processed transactions. As we describe in this paper, so long as PSPs meet certain criteria and perform transaction risk analysis per the required scope, they will be eligible for these exemptions to facilitate the customer journey and reduce friction.

Part 1: General PSD2/RTS Authentication Requirements for Transaction Monitoring

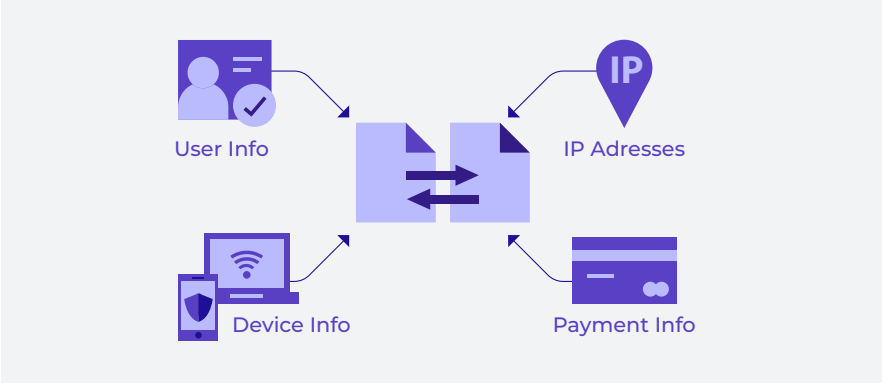
In Article 2(1) of the RTS, the Commission specifies the requirement for detecting unauthorised or fraudulent payment transactions and through the term "transaction monitoring mechanisms", introduces the methods that will enable detection. These transaction monitoring mechanisms should be based on the analysis of payment transactions, taking into account elements typical for the particular payment service user.

Payment service providers have to ensure that transaction monitoring mechanisms at a minimum take into account a number of risk-based factors, as per Article 2(2) of the RTS. Below is an outline of each requirement and an explanation of how OneSpan Risk Analytics can help achieve compliance.

Requirement: List of Compromised Data

"A list of compromised or stolen authentication elements" Article 2(2)

Hotlists are a fundamental tool in fraud prevention. They store assorted data elements, and an update on a regular basis with newly detected fraud-related data is required. This data is used as a reference for rules and workflows, which in turn screen the database for linked cases.



When monitoring transactions, the RTS requires payment service providers to collect and screen lists with stolen and compromised data elements such as IP, device, email, credit card number, or other.

Solution

OneSpan Risk Analytics provides customizable dynamic hotlists (white, gray, and black) specific for each channel, without limiting the type of data. Process automation is a key element for a new generation of fraud monitoring solutions that includes OneSpan Risk Analytics. In keeping with that trend, screening and updating hotlists is an automated workflow of OneSpan Risk Analytics. Additional entries can be added manually, an external file can be uploaded, or a data feed connection can be created with a third-party source.

In the predefined PSD2 package, we have created hotlists configured to collect suspicious elements detected during fraud monitoring and to populate them in gray lists. After an analyst reviews the gray list, the confirmed, compromised, and stolen data elements are then moved to a blacklist.

After reviewing client's data, OneSpan applies the best-suited machine learning algorithms, considering the business needs and risk appetite.

Requirement: Known Fraud Scenarios

"Known fraud scenarios in the provision of payment services" Article 2(2)

Transaction monitoring needs to take into account several known fraud scenarios and must take appropriate measures to detect them.

Solution

OneSpan Risk Analytics supports this requirement with pre-built, configurable rules that cover attacks related to:

- Customer communications
- Login and authentication
- Payment initiation
- Payment execution

The rules are assembled based on our industry expertise and experience with known fraud scenarios, such as:

- Account takeover fraud (malware, phishing, trojans, man-in-the-middle, etc.)
- New registration fraud
- Mule accounts
- Card-not-present fraud
- Batch transactions fraud
- Invoice redirection fraud
- CEO fraud
- And more

With the help of machine learning, OneSpan Risk Analytics is also able to address more complicated fraud scenarios and exceptions that expert rules alone cannot cover. Machine learning is an artificial intelligence that analyses users' typical behaviour and scans for deviations. When deploying OneSpan Risk Analytics, the OneSpan team will review the client's data and apply the best-suited algorithm. In our analysis, we consider the nature of the provided services as well as the PSP's tolerance for risk. If a single algorithm is not sufficient, OneSpan data scientists are able to apply a combination of multiple algorithms to achieve best results.

Requirement: Malware Infection Detection

> *"Signs of malware infection in any session of the authentication procedure"*
> *Article 2(2)*

This requires the ability to identify malware in the authentication session during both the initiation and/or the authentication procedures, as well as during post-session activity. To do so, the fraud solution must stay up-to-date with all user events, both monetary and non-monetary.

Solution

OneSpan Risk Analytics does not simply monitor single events. It continuously analyses all provided user events in a session. This includes events with both sensitive and non-sensitive operations, such as transactions, logins, registrations, changes of address, and more. It creates a detailed profile of the authentication process, including events during and after the authentication takes place.

For example, malware is not confined within the transaction itself. The session could have been compromised before the transaction even begins. A malicious actor could change credentials or revoke or increase permissions as part of the attack. Leveraging such information, our solution can anticipate a malicious payment.

Another key aspect of OneSpan's session monitoring is its ability to unify the sessions of the initiating and authenticating devices in order to identify potential risks. For example, if a user initiates a payment from France and authenticates from Germany, the bank can force proximity authentication with the authenticating device used to initiate the session.

Our comprehensive monitoring approach enables malware identification from multiple layers:

- Device
- Application
- Behavioural analysis
- Historical data
- Multi-channel
- Server-side analytics
- Machine learning

Through an analysis of each layer, the collected data indicates the level of risk present and dictates how to proceed with the authentication request.

Requirement: Transaction Amount

"Amount of each payment transaction" Article 2(2)

In all cases, the payment amount must be taken into account.

Solution

Predefined expert rules and machine learning in OneSpan Risk Analytics cross-reference the transaction amount against the average transaction amount for the same user, group of users, or corporation. Should there be a deviation from the typical amount for the service, channel, or merchant, this may be an indication of fraud.

The payment amount is not the only feature analysed by our solution. All collected and acquired data elements are aggregated using multiple functions, such as volume, velocity, distinct count, exact match, and comparison. In each channel, we define more than 200 aggregated data elements that can be used in rule building.

Requirement: Device/Software Access

"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" Article 2(2)

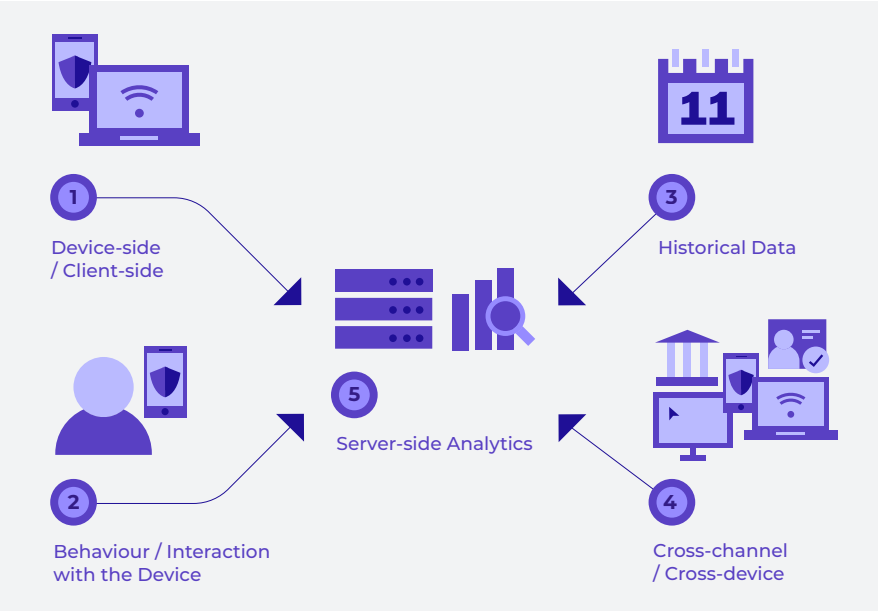
This requirement focuses on scenarios in which the access device and application are provided by the PSP. In such a scenario, this requires fraud monitoring of the device and application. Because the security status of a user's device changes dynamically, the solution must provide continuous, real-time monitoring of the client-side device. Further, this keeps track of the history and analyses the behaviour of the user and their access device.

Solution

OneSpan Risk Analytics and OneSpan Mobile Security Suite monitor the client side continuously and work through an understanding of user behaviour and knowledge of a user's devices, patterns of life, and account activity. The solution analyses the user's devices together with all user actions in order to evaluate the level of risk in real time.

The combined solution provides multi-layered online security (see image below). Together they not only cover the requirements of the regulation; their capabilities also extend beyond compliance.

- **Characteristics of the Initiating and Authenticating Devices (Client Side):** Device data collectors compile information, such as device type, version, screen size, location data, and security components, from the device's browser or mobile application.
- **Behaviour on the Initiating and Authentication Devices (Client Side):** Navigation within the application, speed of browsing, area of touch, accuracy, and swipe move are only part of the behaviour data elements collected to enrich user and device profiles.
- **Historical Data (User Account):** To identify anomalous behaviour, we link all user actions to data collected during their previous activities. We continuously update the profiles of users and accounts, as well as peer groups, in order to compare events and identify suspicious ones. These events include adding new beneficiaries, transfers, logins, and others performed with the same or different devices.
- **Cross Channel/Device:** We back a holistic approach to fraud monitoring, because fraudsters attack all available channels and devices simultaneously when trying to make the most of the stolen data they possess.
- **Server-side Analytics (Machine Learning/Big Data/Entity-link):** Our advanced machine learning evaluates the behaviour of the user, group of users, device, actions within a particular session/or timeframe, and all links between the collected data elements on a historical basis. Machine learning compares each user's behaviour against all users within a certain group, corporation, and the whole bank's user database.



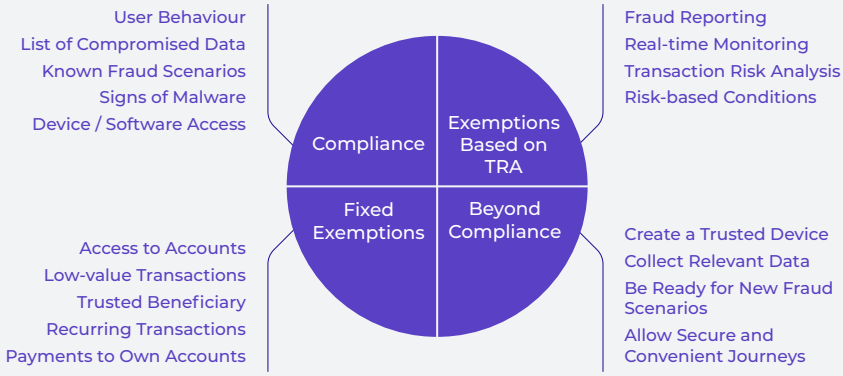
Part 2: Exemptions from Strong Customer Authentication (SCA)

The Regulatory Technical Standards foresee several exemptions from SCA that Account Servicing Payment Service Providers (ASPSPs) and Third Party Account Information/Payment Initiation Service Providers (AISP/PISPs) can benefit from. These exemptions fall into two categories: fixed and risk-based.

In general, an exemption from SCA is allowed when certain criteria have been met. These criteria include, but are not limited to, cases with a low risk of fraud, low-value transactions, or transactions processed by PSPs with low fraud rate. While transaction monitoring is required for all of them, eligibility for certain exemption cases is subject to applying increased fraud monitoring and reporting.

The ASPSPs decide for themselves and for AISP/PISPs if they allow any of the SCA exemptions, regardless of whether or not they qualify.

OneSpan Risk Analytics equips fraud analysts with a reliable fraud monitoring solution for all transactions, both exempted and not. It also provides a comprehensive reporting tool that identifies both an increased risk level and when changes in the exemption policy need to be applied. The predefined PSD2 package includes expert rules, workflows, and reports created to support a smooth and easy application of the SCA exemptions.



SCA Exemptions Based on Fixed Requirements

Both ASPSPs and AISP/PISPs can benefit from SCA exemptions in a fixed range of cases that are independent from calculated fraud rates. To qualify, they have to comply with the general authentication requirements specified in Article 2 as well as some additional conditions depending on the exemption case.

OneSpan's focus is to provide ASPSPs with reliable data to facilitate the decision of whether an exemption can be applied. We accomplish this by assuring collection of all necessary data, aggregating it with the user history, and processing it through special workflows. The transaction will be released in cases where there are no other suspicions. This real-time process does not delay the execution of the transaction and facilitates an optimal user journey.

OneSpan Risk Analytics brings much more trust related to the beneficiary than required by the Regulation.

The list of fixed exemption cases is as follows:

SCA Exemption: Payment Account Information

Article 10 excludes from SCA viewing:

- Balance of one or more designated payment accounts
- Transactions processed 90 days since the last SCA

With the following exceptions:

- First-time view requires SCA
- If SCA has passed 90 days, the user will need to authenticate again

Solution

OneSpan Risk Analytics meets this requirement with predefined expert rules, which include time period checks following specific actions such as the last successful SCA. Expert rules guide the user via a particular workflow if checking their balance for the first time.

SCA Exemption: Low-value Transactions

Article 16 allows SCA exclusion for low-value transactions less than €30. However, it is still required when the accumulated transaction value exceeds €100 or the number of transactions exceeds five.

Solution

OneSpan Risk Analytics uses velocity and cumulative amount checks, which can trigger certain workflows and facilitate the appropriate user journey. Such rules are pre-defined in the proposed PSD2 package.

SCA Exemption: "Trusted" Beneficiary

Article 13 allows an exemption for payments to a previously created beneficiary. However, creating or changing the beneficiary does require SCA.

Solution

OneSpan Risk Analytics brings much more trust to the beneficiary than is required by the Regulation. Not only do we link the beneficiary trust level with the SCA associated with it; we go beyond that. The machine learning evaluates the risk level of each transaction, even for known beneficiaries. The PSP will be notified in real time by the system if the level of risk associated with a transaction to a certain beneficiary changes.

SCA Exemption: Recurring Transactions

Article 14 excludes series of recurring transactions with the same amount and payee. However, initial creation or a change does require SCA. The same exemption is valid for the initiation of all subsequent payment transactions included in the series of recurring transactions.

Solution

OneSpan Risk Analytics defines subsequent transactions with a special sub-event type. This allows the solution to receive information that a transaction corresponds to a subsequent transaction that was previously initiated.

Although these type of transactions are considered safe and the regulation exempts them from SCA, OneSpan Risk Analytics will continuously monitor the level of risk associated with all users and their actions, interactions, and devices. The solution will always analyse the potential for account number alteration or other risks that can occur.

SCA Exemption: Payments to Own Accounts

Article 15 also excludes credit transfers in circumstances where the payer and payee are the same person or legal entity, and both payment accounts are held by the same ASPSP.

Solution

OneSpan Risk Analytics is aware of relationships between accounts and users within a group or organisation. Payments to oneself can be isolated by pre-built rules and processed without further friction for the customer. Meanwhile, all user events will be monitored silently in the background for abnormal behaviour.

SCA Exemption Based on Transaction Risk Analysis (TRA)

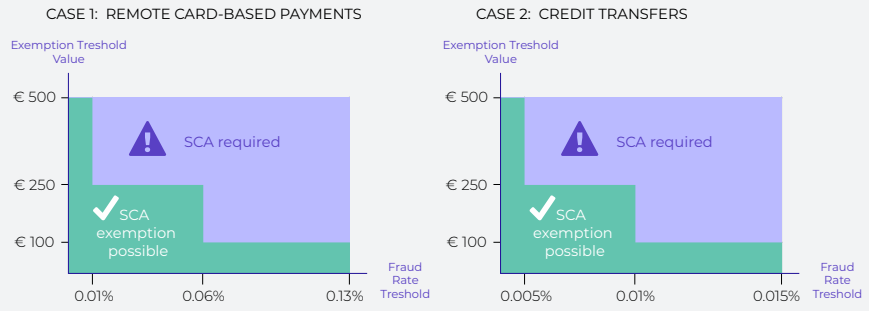
Article 18(1) explains that payments can be exempted from SCA if the transaction analysis indicates that the risk level of the payment is low, according to the transaction monitoring mechanisms referred to in Article 2 and Article 18(2c).

The regulation specifies which transactions can be exempted based on their low risk level, bearing in mind the following conditions:

- Fraud rate is equivalent or below the reference fraud rate
- The amount cannot exceed the Exemption Threshold Value
- The Transaction Risk Analysis standards are met

Condition 1: The Fraud Rate Is Equivalent or Below the Reference Fraud Rate

The payment service provider should ensure that overall fraud rates for each type of transaction authenticated through SCA and exempted per Articles 13 to 18 should be equivalent to, or lower than, the fraud rate for the same type of transaction indicated in the graphs below:



Condition 2: The Allowed Amount Cannot Exceed ETV

The amount of the transaction cannot exceed the Exemption Threshold Value (ETV) specified in the graph above and up to a maximum value of €500.

The ETV defines the payment value at which the reference fraud rates must be adhered to, in order to secure a payment using TRA.

The overall fraud rate for each type of transaction has to be calculated using a specific equation:

The total value of unauthorized or fraudulent remote transactions (regardless of whether the funds have been recovered or not) is divided by the total value of all remote transactions for the same type of transactions.

This equation takes into account all payments, either authenticated with the application of SCA or executed under any relevant exemption in accordance with Articles 13 to 18 on a rolling quarterly basis (90 days).

The calculation of the fraud rates and resulting figures should be assessed by the audit review referred to in Article 3(2), which shall ensure that they are complete and accurate.

Documentation regarding the fraud calculation approach has to be available to the relevant competent authority upon request.

If fraud levels at a PSP rise above the €100 or 0.13% hurdle rate for two consecutive quarters, this provider cannot use the exemption any longer and must alert the competent authority.

Solution

OneSpan Risk Analytics has the ability to label events as fraudulent or genuine. The solution uses these labels in its pre-built report to help calculate the fraud rates separated per transaction type, for all successful remote transactions with and without SCA.

For example, if the fraud rate is up to 0.1% for card transactions, the PSP qualifies for an SCA exemption for card transactions up to €100. A set of rules that exempts performing SCA will be enabled and will allow SCA exemption for transactions below that ETV. In addition, OneSpan Risk Analytics will continue real-time monitoring of exempted transactions. The PSP will be alerted if exempted transactions are suspicious, and the solution will trigger step-up authentication.

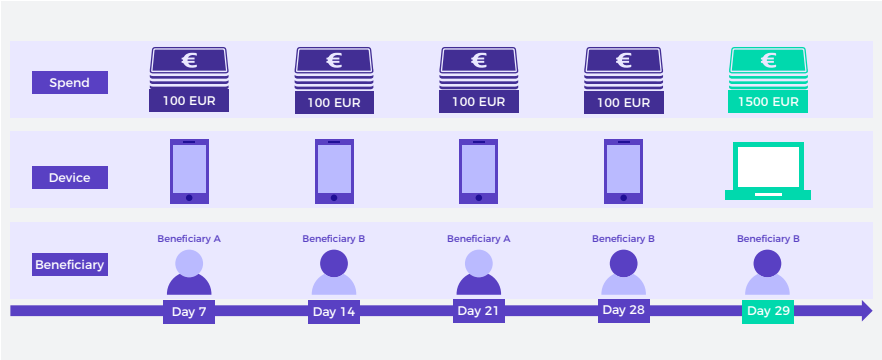
Condition 3: Transaction Risk Analysis Standards Are Met

Independent from the specific provisions of the general authentication requirements, PSP's real-time TRA should identify the following factors specified in paragraph 2(c) of Article 18:

- Abnormal spending or behaviour
- Device and software access
- Malware or known fraud scenarios
- Abnormal location of the payer
- Payee's location level of risk

Factor 1: Abnormal Spending or Behaviour

"Abnormal spending or behavioural pattern of the payer" Article 18(2c)



OneSpan provides sophisticated and precise analysis based on more than 200 different factors in multiple dimensions.

Solution

OneSpan Risk Analytics defines patterns for each user by aggregating data elements. Aggregation takes into consideration the user's history, specifically: transaction amounts, number of transactions, average transactions, beneficiaries, merchants, navigation within the bank application, logins, and more. Knowing each user's typical habits, machine learning analyses all collected data elements in real time and decides how relevant they are for each particular situation. When there is a suspicious combination of otherwise normal actions, the system identifies abnormal behaviour patterns. For example, if the user sends an abnormal amount of money to a known beneficiary using an unknown or new device, the system would flag this as a high-risk transaction. Criminals could be in control the payer and payee's accounts. Such atypical behaviour can be identified by machine learning, which evaluates each collected data element.

Factor 2: Device and Software Access

> *"Unusual information about the payer's device/software access" Article 18(2c)*

See the section: "Requirement: Device/Software Access" to learn how OneSpan Risk Analytics complies with this requirement.

Factor 3: Malware or Known Fraud Scenarios

> *"Malware infection in any session of the authentication procedure" and "Known fraud scenarios in the provision of payment services" Article 18(2c)*

See the sections: "Requirement: Malware Infection Detection" and "Requirement: Known Fraud Scenarios" to learn how OneSpan Risk Analytics complies with this requirement.

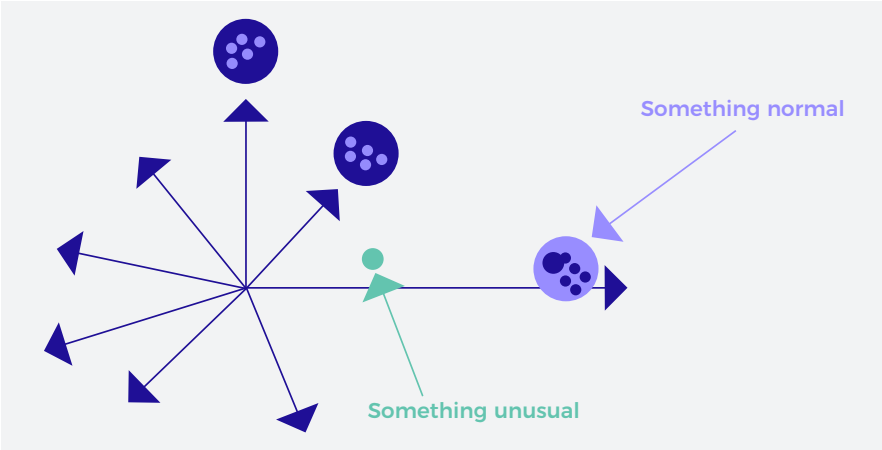
Factor 4: Abnormal Location of the Payer

> *"Abnormal location of the payer" Article 18(2c)*

Solution

OneSpan Risk Analytics analyses the location profile of the user and identifies abnormal locations. This includes knowledge and understanding of the data attributes that identify the common location of the user, such as history of IP addresses, geolocation, and all information derived from them. The solution aggregates location data combined with the user's activity and checks it against previous actions and locations. A particular user's behaviour in the new location is compared to their behaviour in the typical location and other locations in their history. To assess the probability of fraudulent activity, machine learning performs real-time analysis of the location in combination with more than 200 other factors.

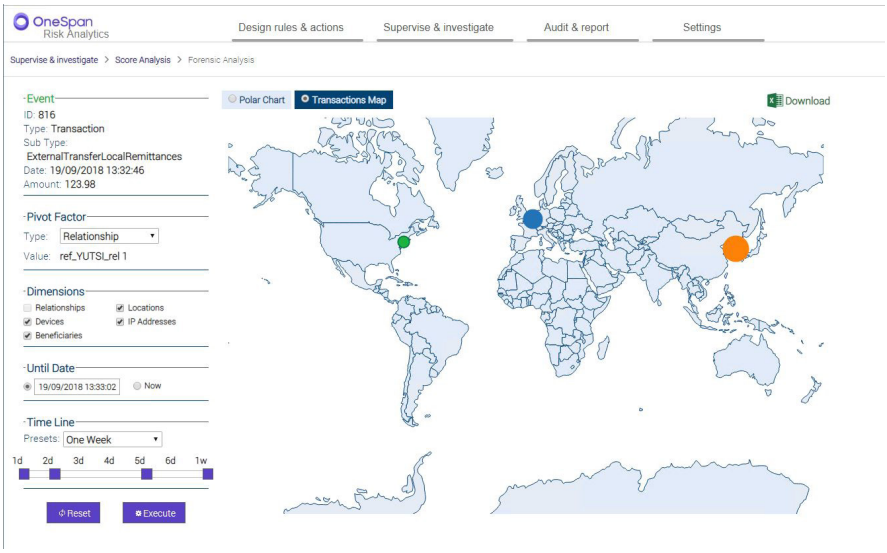
Looking into the current location and the history of typical locations is a two-dimensional comparison. This can be done easily with a regular fraud management tool; however, adding all the remaining data elements and creating multi-dimensional links yields a much more sophisticated and precise analysis.



Machine learning profiles the user and their habits (e.g. traveling to certain locations, transacting in different locations or countries, etc.) to determine what a normal location profile looks like.

OneSpan's Component Score Analysis Map provides an analysis of the score generated as a result of fraud detection rules and machine learning. The feature includes an overview of the user activity that includes the proximity of the payer within a certain period and where abnormal locations can easily be identified. Other dimensions such as IP address, device, beneficiary, etc., are also available.

For example, in the graphic below, the payer's typical locations are in South Korea and Belgium, while abnormal locations are in the U.S.



Factor 5: Payee's Location Level of Risk

"high risk location of the payee" Article 18(2c)

Solution

OneSpan Risk Analytics stores risky locations specified in hotlists like blacklisted IPs, risk countries, addresses with bad reputation, known bad proxies, known TOR exit nodes, sanction lists, and so on. Moreover, the solution can automatically add locations generated as a result of fraud monitoring to black, grey, and white hotlists. They can also include external known fraud information, such as known fraud IPs.

In addition, OneSpan Risk Analytics can address known fraud patterns. For example, if during the last week, several fraudulent transactions were discovered with the same euro amount transferred from country A to country B, OneSpan Risk Analytics can request additional review or authentication for the transactions sent out to country B, as long as the pattern continues.

Location data is easy to manipulate. Trusted server-side analysis becomes essential for fraud identification.

Risk-based Factors for Low-risk Transactions

PSPs that intend to use the exemptions on the grounds of low risk should take into account at a minimum the risk-based factors listed in Article 18(3) concerning:

- User's spending patterns and transaction history
- Location of the payer and the payee

Factor 1: User's Spending Patterns and Transaction History

> *"The previous spending patterns of the individual payment service user" Article 18(3a)*

> *"Payment transaction history of each of the payment service provider's payment service users" Article 18(3b)*

> *"The identification of abnormal payment patterns of the payment service user in relation to the user's payment transaction history" Article 18(3d)*

Solution

OneSpan Risk Analytics stores a user's payment transaction and behaviour history in the database to support the analysis and detection processes. Using score analysis dashboards, analysts can link events of current and previous cases.

A rule test on real historical data can be used to check the hit rate of newly created rules. This exercise allows the analysts to fine-tune their rules before activation.

Factor 2: Location of the Payer and the Payee

> *"Location of the payer and of the payee account at the time of the payment transaction providing the access device or the software is provided by the payment service provider" Article 18(3c)*

Solution

OneSpan Risk Analytics acquires the location data collected from all of the PSP's channels and sources, such as the user's device. The solution uses a browser data collector to gather information from the user's PC or laptop and a mobile application data collector for the application on the mobile phone or tablet.

Components, such as IP geolocation and proxy analysis, are also included in the quality enhancement process of the collected data.

Location data can be manipulated easily. For that reason, it is important to have trusted analysis on the server-side to identify fraud, even if the data has been altered.

From a mobile device, more location-related data (Wi-Fi, roaming, GPS location, and others) can be extracted with a device data collector. However, this data can be spoofed if the following protection elements are not in place:

1. Reliable mobile application security
2. A secure communication channel between the user's device and the back-end server
3. Server-side analytics to link the collected data to a device profile

Due to the interaction between OneSpan Risk Analytics and OneSpan Mobile Security Suite, the solution is able to provide these three elements.

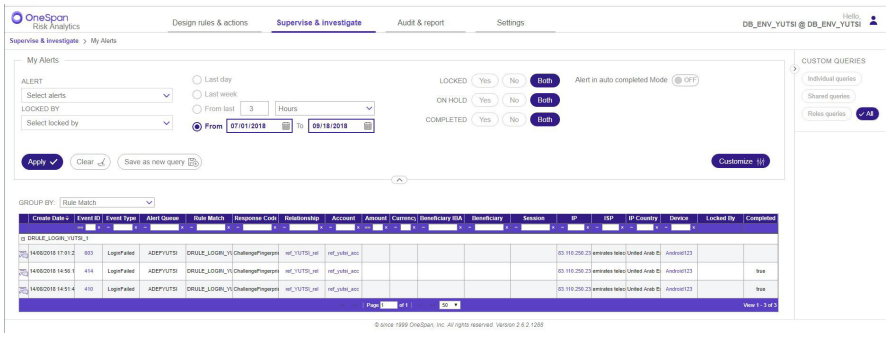
OneSpan Mobile Security Suite is a client-side solution using a mobile software development kit (SDK) and integrated into the payment institution's mobile application.

Scoring Using Risk-based Factors

A transaction monitoring solution needs to perform risk analysis based on factors mentioned in Article 18(3). It also needs to be able to combine these requirements in a detailed scoring system to determine the risk level of a transaction.

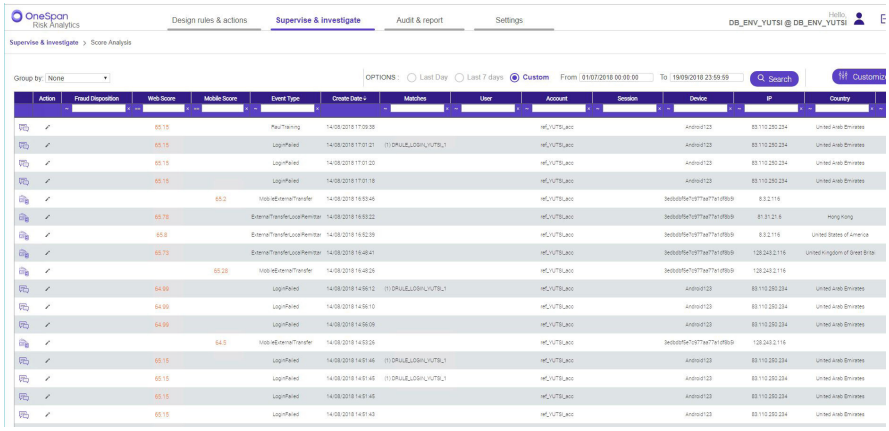
The machine learning found in OneSpan Risk Analytics scores each user action and evaluates the level of risk in real time. A score can be sent back as a response, which can trigger certain actions or be implemented as a condition in a rule.

To facilitate the investigation of suspicious transactions, OneSpan Risk Analytics provides analysts with a real time "My Alerts" screen, where events with alerts are displayed for manual review.

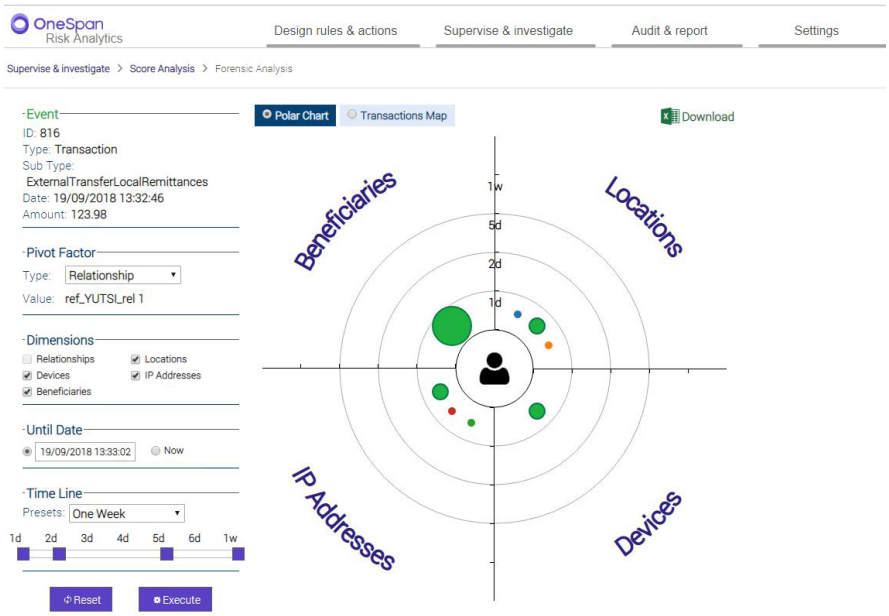


The analyst can dig deeper into a particular case and explore more of the user's history as well as all other relevant data. A score analysis tool can provide additional understanding and insight into the case and score.

The Score Analysis tab displays all events and their scores, which helps analysts investigate high-rated events, either by grouping all events from the same session or all transactions to the same beneficiary.



The other tool supporting the score analysis is the Visualization Dashboard. The Visualization Dashboard offers a graphical representation of the context associated with a selected event, like locations, devices, IP addresses, and beneficiaries linked to the user. This helps analysts understand the decisions based on the assigned score. The link is established in the form of Pivot Factors, with the attributes used as filters to construct the visualization graph.



Monitoring of Fraud Rates and Reporting

According to Article 21(1), payment service providers need to record and monitor the following data for each type of payment transaction, with a breakdown for both remote and non-remote payment transactions on a quarterly basis if they want to make use of the exemptions set out in Articles 10 to 18:

- The total value of unauthorised or fraudulent payment transactions in accordance with Article 64(2) of Directive (EU) 2015/2366. According to the article, a transaction or series of transactions shall be considered unauthorised without consent to execute the payment
- The total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions
- The average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions
- The number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions

OneSpan's comprehensive reporting tool provides this information via pre-built reports. The reports allow extracting all data to calculate a fraud rate that will be used to decide if the SCA exemption can be applied. For the needs of the fraud rate calculation, the reporting considers successfully processed transactions. Further, additional data showing the levels of stopped/blocked fraud and fraudulent attempts are available in the system to facilitate the management reporting.

Major Disruptions to the Payment Market

The payment market is undergoing a major disruption with new challenges, business models, and players. PSD2, with its Regulatory Technical Standards, will transform the banking and payment industry, though not as quickly or drastically as it may seem. Its impact is already being felt, in that it indicates the general direction of the market, of technology innovation, and even of the next generation of regulations.

We are now seeing the importance of fraud monitoring being elevated, as it becomes mandatory for all types of payments in Europe. Further, we expect that Strong Customer Authentication exemptions will facilitate user convenience in the transaction flow. A thorough and reliable analysis has long been one of the important building blocks of successful fraud prevention. Now, the result is not only reduced fraud rates, but a better experience for all parties involved in a transaction.

An experienced partner, OneSpan has the expertise to guide you through this new reality and provide intelligent solutions supporting compliance and best-in-class security. OneSpan Risk Analytics ensures full compliance with new legal requirements and standards through features such as the pre-defined PSD2 package. And in combination with the OneSpan Mobile Security Suite, OneSpan Risk Analytics creates an experience that ensures both user convenience and a highly secure environment.

Our mission at OneSpan is to help PSPs find their way through compliance to success in the post-PSD2 era. OneSpan Risk Analytics not only helps banks and fintechs meet the compliance requirements, it is also capable of providing solutions beyond compliance.

For more information on PSD2 compliance,

visit www.OneSpan.com/psd2

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US

For more information:
info@OneSpan.com
www.OneSpan.com