New approaches to security and fraud prevention in instant payment

Collaboration to improve security in instant payment through Verification-of-Payee (VoP)

-

Specialized article

Faster and safer
SEPA credit transfers through the verification of the payee (VoP)

The Instant Payments Regulation sets a new standard in European payment transactions. It aims to speed up payment transactions within the SEPA (Single Euro Payments Area) and make them more secure. A central component of this regulation is the introduction of the Verification of Payee (VoP) procedure. This procedure enables customers of payment service providers (PSPs) to verify the identity of the payee before initiating a SEPA Instant Credit Transfer (SCT Inst). The introduction of the Verification of Payee process pursues the following main objectives in particular:

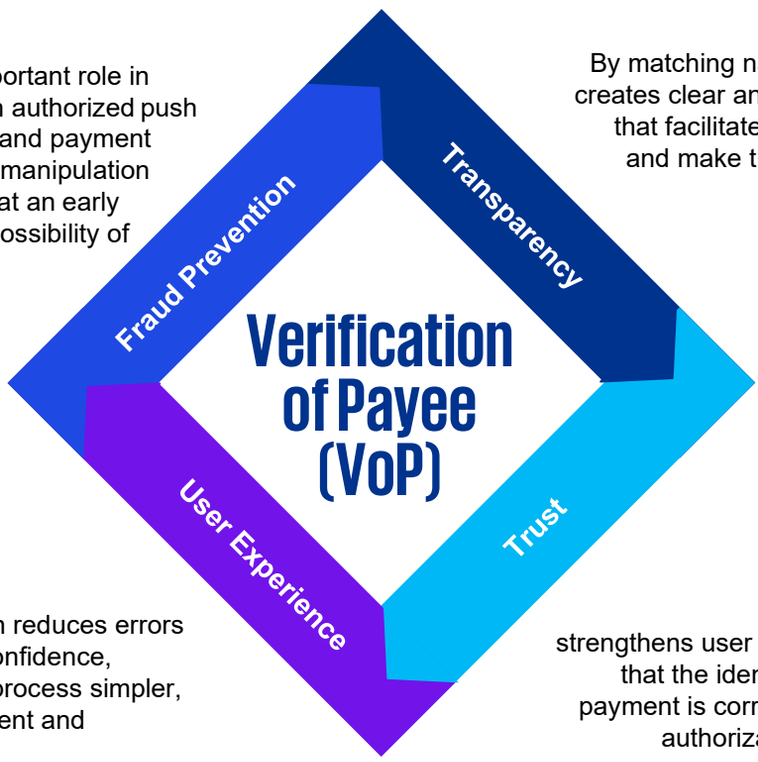
Fig. 1: The main objectives of the Verification of Payee (VoP) process

Fraud prevention:

The VoP plays an important role in combating fraud, such authorized push payment (APP) fraud and payment detour, by preventing manipulation and false information at an early stage and offers the possibility of detecting suspicious transactions to block.

Transparency:

By matching names and IBANs, VoP creates clear and traceable processes that facilitate payment transactions and make them more transparent.



User experience:

Automated verification reduces errors and enhances user confidence, making the payment process simpler, more secure, convenient and efficient.

Trust:

The VoP strengthens user confidence by ensuring that the identity of the recipient of a payment is correctly verified before the authorization of the transaction.

Source: KPMG in Germany, 2025

The VoP process will be as follows in the future:

Step 1: Data acquisition

The payer's payment service provider (requesting PSP) collects the necessary information from the payer: IBAN and name of the counterparty. If the data is transmitted by a payment initiation service provider (PISP), it is up to the PISP to ensure that it is correct. If the counterparty is a legal entity, unique identification codes such as tax number or LEI can also be used instead of the name, provided the receiving PSP's systems support them.

Step 2: Forwarding the request

As soon as the information is available, the requesting PSP sends a VoP request to the payment service provider where the counterparty's payment account is held (responding PSP). The request is transmitted via a standardized routing system, supported by the EPC directory service (EDS). This checks whether the responding PSP participates in the VoP procedure and provides the necessary connection data. If the account is held at the requesting PSP's bank, this bank also performs the check.

Step 3: The review

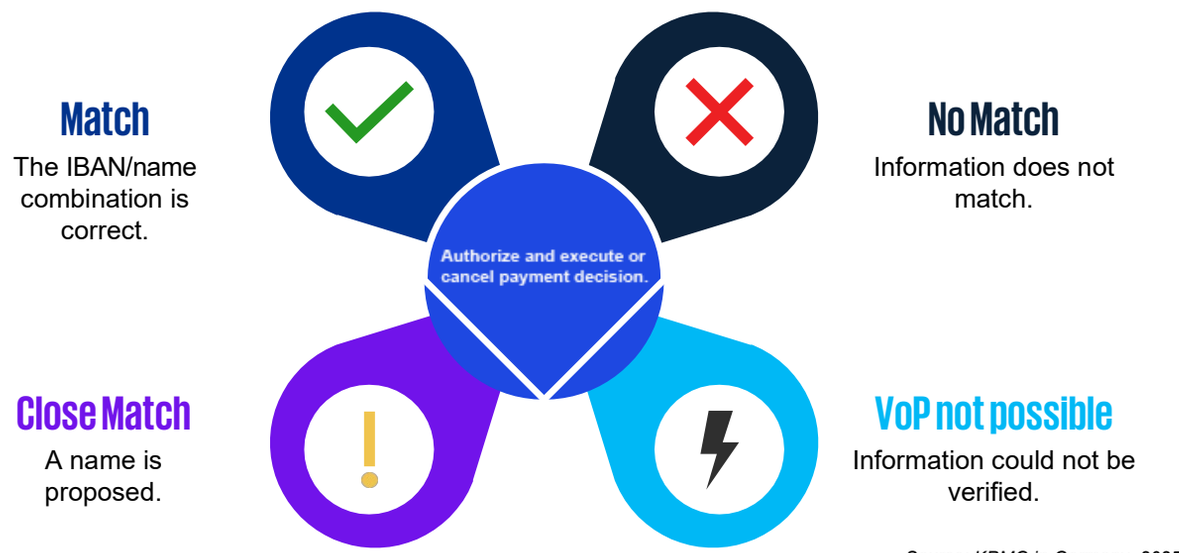
The responding PSP checks the request immediately. It compares the transmitted data (e.g. name and IBAN) with the information it has stored. In the case of a "close match
If the "consent" function is activated, it reports the stored name of the counterparty to the requesting PSP.

Step 4: The feedback

The VoP response is immediately sent back to the requesting PSP. This contains the name linked to the counterparty's payment account or informs of a mismatch.

The following feedback is possible:

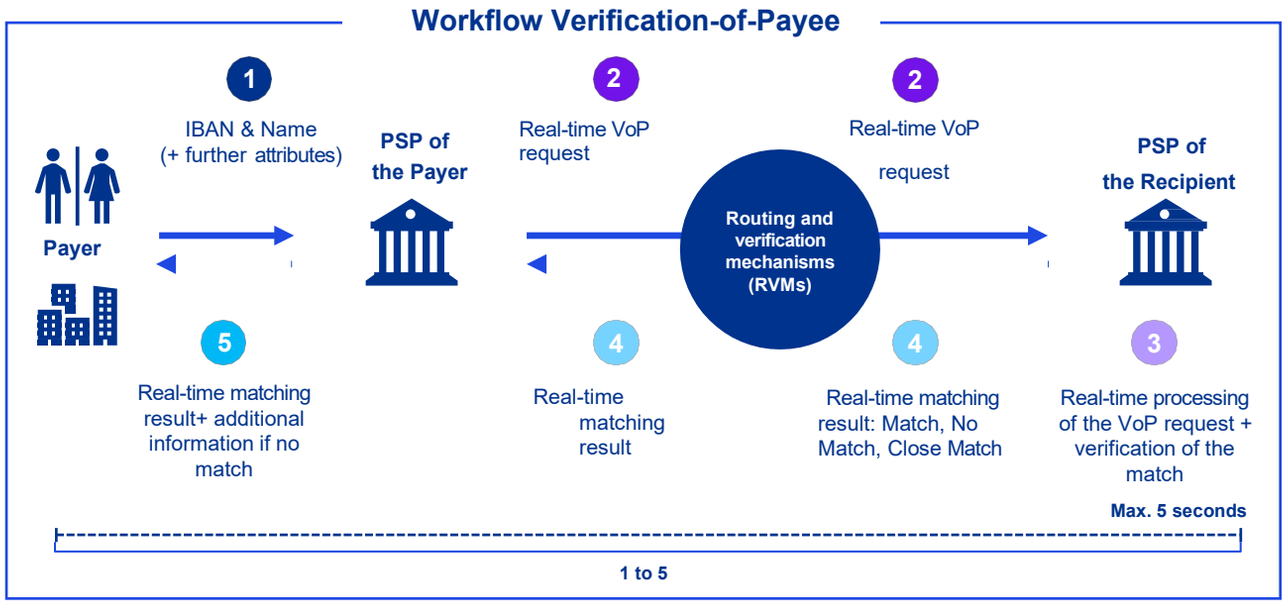
Fig. 2: IBAN name check possible results.



Source: KPMG in Germany, 2025

	Description	Consequence
Close agreement (match):	The IBAN and the name of the recipient match or correspond to a minimal, non-critical deviation that is considered acceptable.	The full name of the payee is reported back. This confirmation makes it possible to authorize and execute the payment immediately.
Partial match (close match):	There is a partial match between the information transmitted and the data stored at the recipient bank, for example a slight difference in the name (such as a typing error or different spelling).	A suggested name is returned, which requires the payment sender to check and confirm the data to subsequently authorize and execute or cancel the payment. The suggested name should only be specified in the event of minor deviations.
No agreement (No Match):	The name and IBAN do not match, or there is a significant discrepancy in the verification of the payee.	It is reported back that the data provided does not match the data stored with the recipient's PSP. The recipient is informed/notified of the discrepancy and asked to check the recipient data to ensure that no incorrect information has been provided in order to authorize and execute or cancel the payment.
Verification check not possible (VoP not Possible):	The verification could not be carried out for technical reasons, for example if the responding PSP does not participate in the VoP procedure (e.g. outside the SEPA scope for IPV) or if there is a technical problem.	The payer is informed that the verification could not be carried out due to system or network problems. The requesting payment service provider immediately informs the payer that the release of the payment may result in funds being transferred to an account that does not belong to the specified payment partner.

Fig. 3: Process flow of the IBAN name check (VoP)



Source: KPMG in Germany, 2025

In addition, VoP has a significant impact on the processing of bulk payments, which are often carried out by companies or public institutions. These usually involve several, sometimes thousands of transactions that are directed to different recipients and are triggered at the same time. Various challenges therefore arise in the context of IPV and VoP:

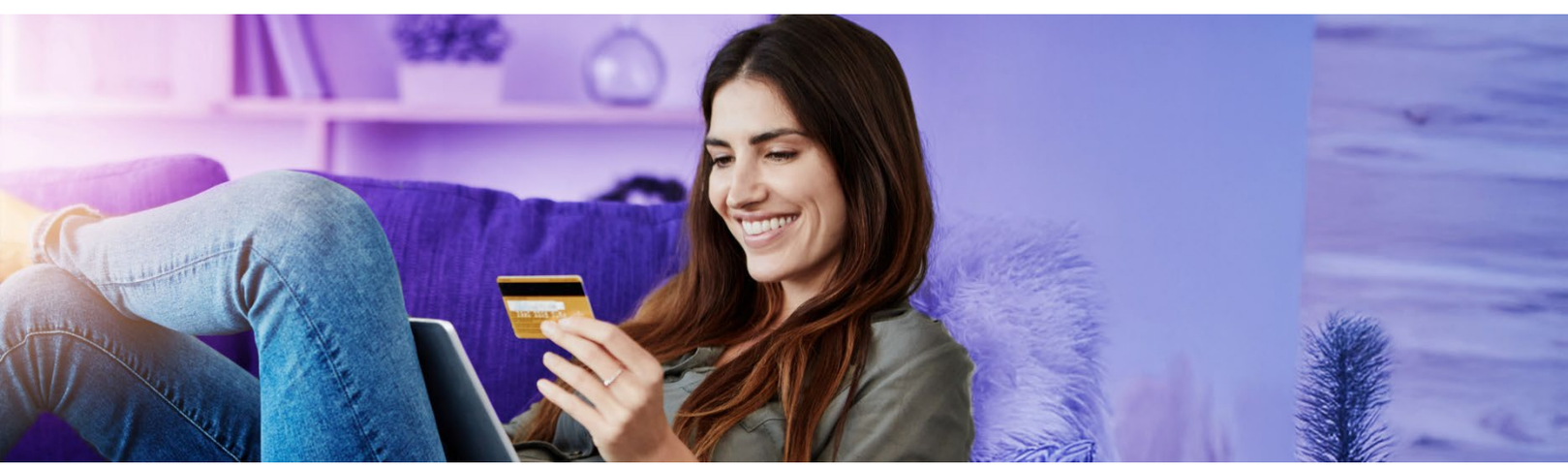
Automated verification: Each individual transaction must undergo a VoP check to ensure that the specified recipient name matches the IBAN within the prescribed maximum execution time of 5 seconds.

Scalability and system capacity: Mass payments often require the processing of thousands of transactions simultaneously.
The integration of the VoP check into the payment settlement process increases the demands on the processing performance and scalability of the PSP's systems. These must meet the time requirements in order to enable the real-time verification of a large number of transactions.

Error handling and manual verification: In the event of close matches or no matches, the affected payments must be verified, which could lead to increased manual effort. The payment initiation service provider (PISP) or the payer's PSP must therefore take measures to process the responses promptly and return them to the payer. In the case of bulk payments, this can lead to considerable delays.

Exceptions for bulk payments: The regulation allows for exceptions when carrying out the VoP for bulk payments, as the VoP check for each individual payment is difficult to implement.

For example, it will be possible to apply a blanket confirmation of the payee. The PSP can carry out a blanket confirmation of payment recipients based on existing verified data (e.g. through whitelists). In the case of regular payments to the same recipient (e.g. salary payments), the VoP can thus access already verified data without having to check each payment transaction again.



Effects on liability and responsibilities

The introduction of the VoP as part of the IPV has a direct impact on the distribution of liability between the various players in payment transactions. The changes affect both the responsibilities of PSPs and potential liability issues in the event of incorrect or fraudulent payments. According to Article 5c of the Regulation, PSPs are obliged to ensure that the payee's details (IBAN and name) have been correctly verified prior to payment authorization.
If a PSP fails to carry out the prescribed VoP check or carries it incorrectly, it shall be liable for any losses that the payer or a third party may incur as a result.

The regulation obliges PSPs to inform the payer of any discrepancies between the name and IBAN:

Close Match: The responsibility for releasing the payment lies with the payer, provided that the PSP has made the deviation transparent.

No Match: If a payer authorizes the payment despite a VoP warning, they are generally responsible for the resulting loss. Banks or payment service providers may be excluded from liability in this case as long as they have correctly informed the payer.
If a payment service provider does not carry out the VoP check properly or issues an incorrect warning, it can be held liable if this leads to financial loss.

Future-proof: challenges and solutions in the verification-of-payee process of the Instant Payment Regulation

Verification-of-Payee (VoP) helps with fraud prevention and detection by ensuring that the payee's name matches the IBAN provided. This prevents payments from being routed to false or fraudulent accounts, as is often the case with phishing or invoice fraud.

Fig. 4: Summary of the main benefits of fraud prevention

Advantages	Description
Improved detection of anomalies	Detection of discrepancies between the payee's name and the IBAN, possible fraudulent activity.
Prevention of APP (Authorized Push Payment) Fraud	Can help protect customers from scams that trick them into transferring money to fraudulent accounts.
Reduction of human error	Minimization of errors by typing errors or incorrect information when initiating payments.
Mitigation of payment evasion fraud	Prevents funds from being diverted to fraudulent accounts due to manipulated account data.
Additional protection against synthetic identity fraud	Ensures that payment details match verified names to reduce exploitation by fake identities.
Prevention of BEC fraud	Checks whether the payment details match the intended recipients and thus prevents fraud with business emails.
Improved auditability for investigations	Provides a clear trail of verified payee data, which helps to resolve fraud cases more quickly.

Source: KPMG in Germany, 2025

Advantages through real-time processing:

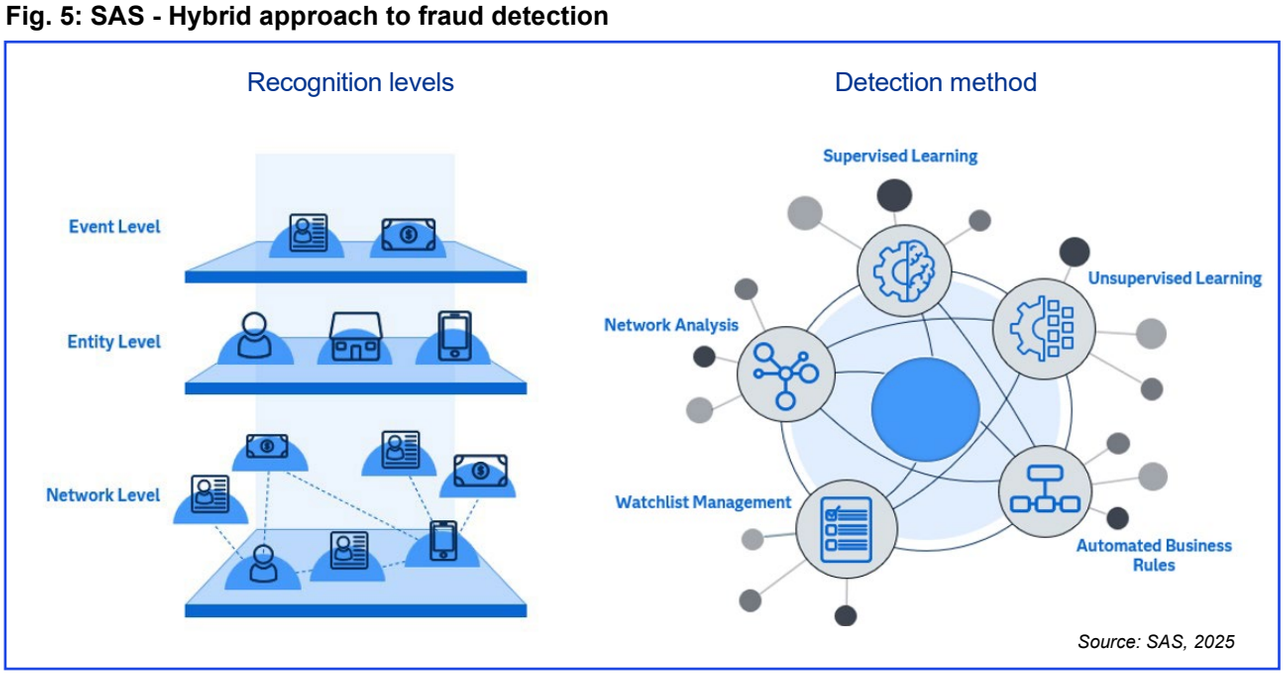
- **Proactive fraud detection:** VoP works seamlessly with real-time fraud detection systems and identifies anomalies within seconds.
- **Improved trust:** Ensures funds are transferred securely to the intended recipient, boosting user confidence in instant payments.

Real-time verification and the integration of other real-time fraud detection systems increases the security of instant payments by detecting potential fraud within seconds before money is transferred.

SAS integrates the results of **VoP** into a hybrid fraud detection system. By using **behavioral analytics** for risk assessment - including transaction history and detailed device data - a dynamic picture of payment activity is generated. In addition, SAS implements continuous **feedback loops** that allow fraud detection models to be constantly refined and optimized. This integrative approach, which combines a wide range of strategies and technologies, creates a **holistic fraud detection** system that goes beyond the capabilities of VoP checks alone.

"SAS solutions integrate the VoP process via API connectors and also fulfill several critical technical requirements that ensure seamless integration, scalability and regulatory compliance of the solution with PSPs' existing infrastructures." - SAS

Fig. 5: SAS - Hybrid approach to fraud detection



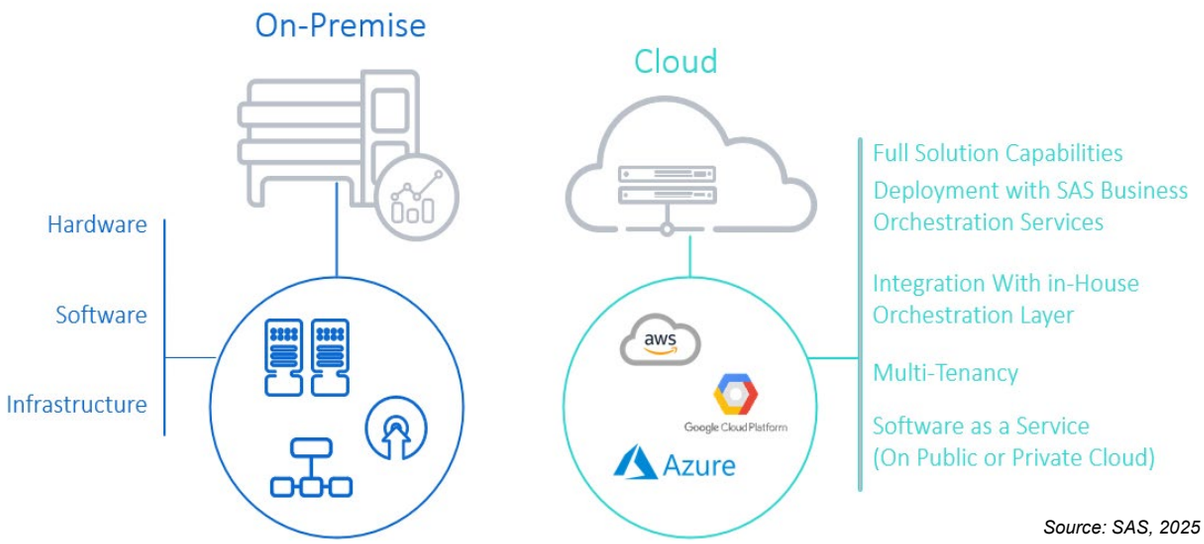
SAS also offers various implementation options, whether on-premises or via a cloud connection (public or private cloud) and with a multi-tenancy option.

In addition, data quality and interoperability are crucial for the successful implementation of the VoP and a more efficient design of the fraud detection system.

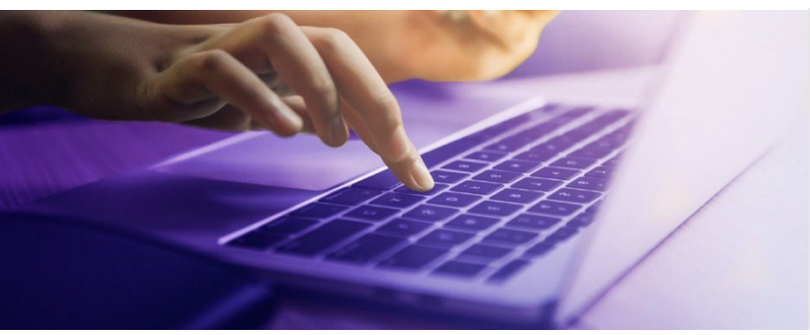
A precise and up-to-date match of IBAN and recipient name requires an error-free and complete database. Inaccurate or outdated data increases the risk of errors and fraud and can lead to liability problems for PSPs.

The interoperability between different payment systems and banks is essential to ensure smooth and fast verification of recipient data across country and bank borders. Only through the combination of high-quality data and seamless system integration can the VoP develop its full effectiveness and guarantee the security of payments.

Fig. 6: Possible applications of SAS fraud management



Source: SAS, 2025



"KPMG is a reliable integration partner and regulatory expert for PSPs in the implementation of the Verification of Payee (VoP) and its integration.
to improve the fraud detection system."

Technical requirements and support from KPMG

The integration of Verification-of-Payee (VoP) into existing IT infrastructures of payment service providers (PSPs) requires the fulfillment of several technical requirements. KPMG acts as an expert technical partner and offers comprehensive support in the implementation of VoP solutions - whether through a new technical solution or as an integration into existing solutions - which also take into account the implications for real-time fraud detection. There are various ways to implement VoP. Companies can either develop their own solutions or rely on specialized RegTech providers.

KPMG assists in the selection and integration of the appropriate solution to ensure that the specific requirements and regulatory specifications are met.

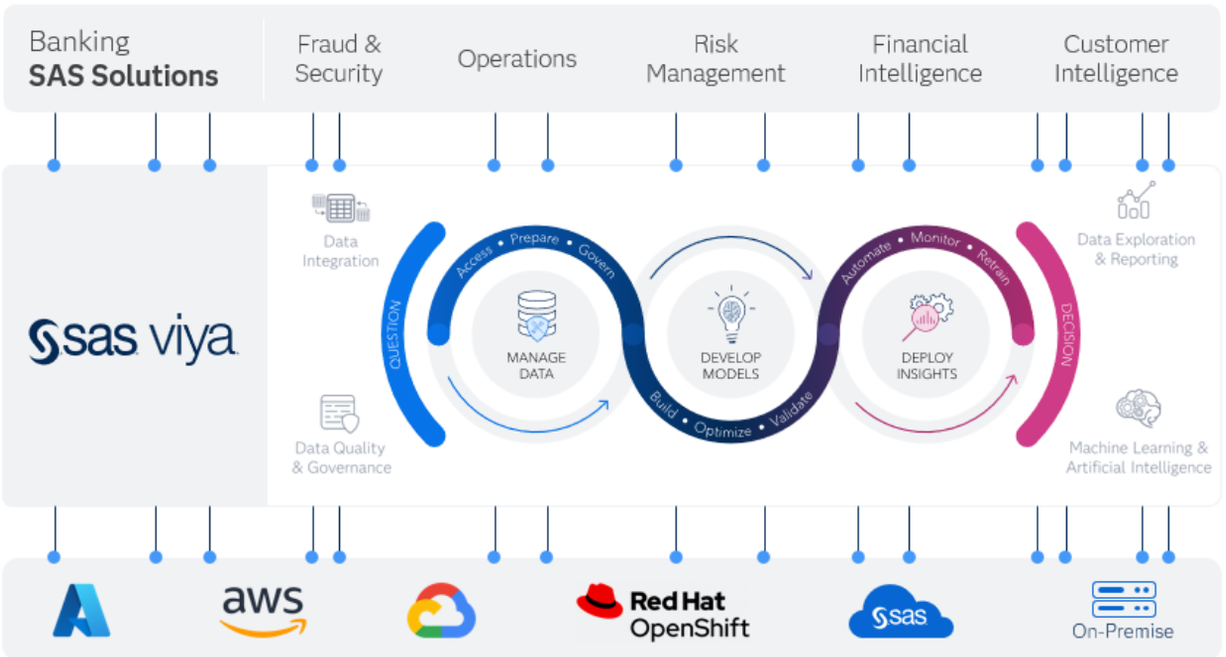
SAS solutions for fraud detection and prevention

SAS offers a solution set of fraud detection and prevention tools hosted in the SAS Viya platform, a robust platform for advanced analytics, artificial intelligence, and machine learning. The true strength of VoP lies in being part of a broader, integrated strategy that incorporates behavioral analytics, transaction monitoring and multi-layered authentication. Integrating VoP with SAS Solutions can enhance fraud detection capabilities by embedding account auditing into a real-time monitoring, anomaly detection, fraud, compliance, and risk management framework to help organizations achieve a proactive and scalable fraud prevention framework that adapts evolving threats.

Advantages of the SAS platform

SAS solutions provide a robust platform for VoP integration that includes seamless API (Application Programming Interface) connectors, scalable architectures, and advanced data matching capabilities. These techniques enable accurate verification of payee names despite variations, typos, and abbreviations. In addition, SAS offers rule-based and risk-adaptive logic with configurable rules and dynamic thresholds based on transaction risk profiles.

Fig. 7: SAS fraud detection platform



Source: SAS, 2025

Performance of SAS in real-time fraud detection

SAS technology provides a robust basis for real-time fraud detection in payment transactions. During performance tests, a throughput of 20,000 transactions per second (TPS) was achieved, a response time in the 99th percentile of less than 75 milliseconds. This performance was maintained consistently over a period of one hour.

The high efficiency was achieved using Azure Cache for Redis Enterprise (ACRE) with Redis compression enabled, which was identified as a central component of the infrastructure. For use cases with less stringent service level requirements, future tests could demonstrate the suitability of the ACRE flash tier. In addition, the use of Azure Managed Redis is being evaluated to assess its potential for high throughput requirements.

They create a resilient basis for the implementation of instant payments and compliance with regulatory requirements.

Together into the future: KPMG and SAS - your key to value-added security in the Verification of Payee process of the Instant Payment Regulation

The introduction of VoP opens far-reaching opportunities for technological innovations in payment transactions. The use of artificial intelligence (AI) and machine learning can significantly increase the precision and efficiency of identity verification. Cloud technology provides a secure and transparent method of storing transaction data, which increases the integrity and traceability of payments.

Together with SAS, KPMG enables seamless integration of the VoP process into existing payment and compliance systems.

The partnership approach between KPMG and SAS in implementing the requirements of the Instant Payments Regulation contains several success-critical factors increase the security and efficiency of instant payments while meeting the regulatory requirements of today and the future. The steps outlined illustrate a structured approach to implementing the requirements of the Instant Payments Regulation, utilizing the strengths of both partners - KPMG in the areas of consulting, compliance and implementation support and SAS with the appropriate technological solutions.

To KPMG	To SAS
Comprehensive expertise: KPMG has in-depth expertise in the area of regulatory & compliance. We know the specific requirements of IPV and can offer tailor-made solutions.	**Experience and expertise:** SAS has a long history in data analytics and risk management. SAS solutions are designed to process complex data sets and gain insights that are critical for regulatory compliance.
Industry experience: With extensive experience in working with financial institutions and payment service providers, KPMG has developed proven methods that make the implementation process efficient.	**Real-time analytics**: The Instant Payment Regulation requires fast transactions and immediate reviews. SAS offers powerful real-time analytics tools that enable payment service providers to review transactions instantly and quickly identify potential risks.
Integration of best practices: KPMG can bring in best practices from different projects and industries to ensure that the implementation not only complies with regulatory requirements, but also promotes operational efficiency and safety.	**Verification-of-Payee (VoP):** The VoP process is crucial to ensure that payments go to the right recipient. SAS solutions can help to perform identity checks and ensure that the account information matches the payee's details. This significantly reduces the risk of fraud.
Verification of Payee (VoP): The Verification of Payee process is crucial for the security of instant payments. KPMG offers specialized advice to ensure that payment service providers effectively implement the necessary measures to verify payees.	**Fraud detection:** SAS offers fraud detection algorithms that use machine learning and AI. These technologies can recognize patterns and identify anomalies that could indicate fraudulent activity. This enables payment service providers to take proactive action against fraud.
Risk management and compliance: KPMG supports payment service providers in identifying and managing risks, associated with the implementation of the regulation. This also includes adherence to compliance requirements.	**Regulatory compliance:** Compliance is of paramount importance for payment service providers. SAS solutions are designed to meet current regulatory requirements and help minimize compliance risks.
Technology support: KPMG has partnerships with advanced technology partners who can support the implementation process and increase efficiency.	**Flexibility and scalability**: SAS solutions are flexible and scalable so that they can be adapted to the specific needs of a payment service provider. This is particularly important in a rapidly changing regulatory environment.
Individual advice: Every company is unique. KPMG offers individual consulting approaches that are tailored to the specific needs and challenges of each payment service provider.	**Integration with existing systems:** SAS technologies integrate well with existing systems, enabling seamless implementation while increasing efficiency.

For a detailed look at the specific requirements and solutions, please refer to other **specialist articles on this topic:**

- Fast payments, strong partnerships: The future of the Instant-Payment-Regulation with KPMG and SAS
- Reporting obligations in the context of the Instant-Payment-Regulation
- Sanctions

We will be happy to continue to inform you about the Instant Payment Regulation on our website: Instant Payment Regulation - KPMG Germany

Contact us

KPMG AG Wirtschaftsprüfungsgesellschaft

Danic Seiwert
Senior Manager,
Financial Services
M +49 151 46259053
dseiwert@kpmg.com

The following person contributed to this article: Tom Schmelzer, Financial Services

SAS

Katarina Garai
Fraud & FinCrime Partnerships & Strategic Initiatives Lead, Western, Central and Southern Europe
T +43 664 106 2543
katarina.garai@sas.com

Anna Lykourina
Head of Fraud & Security Intelligence Customer advisory, South-East Europe
T +30 6947 377 960
anna.lykourina@sas.com

Some or all of the services described herein may not be permitted for KPMG audit clients and their affiliates.

www.kpmg.de

www.kpmg.de/socialmedia