



iPiD

VERIFICATION OF PAYEE: THE RACE TO COMPLIANCE

APRIL 2024



EXECUTIVE SUMMARY

As European Regulators are pushing for an acceleration in the adoption of instant payments in Europe, they have also set a new benchmark in payment security with the introduction of the Verification of Payee (VoP) mandate, which could have a global ripple effect, much like the GDPR did for data privacy.

This paper aims to guide Payment Service Providers (PSPs) to comply with the VoP mandate by October 2025. This obligation, detailed in Article 5c, demands that PSPs implement services to cross-verify payee names against banking records, offering a safeguard against misdirected payments. In the case of "defectively executed payments", the Regulation also introduces a liability shift from the payer to its PSP for those PSPs failing to offer a VoP service. This shift is in line with a worldwide trend where the liability framework for credit transfers is evolving to resemble practices already widespread in the card industry.

PSPs have 18 months to implement significant changes:

- 1. Build capability to query payee data stored in core banking systems;*
- 2. Implement a name-matching algorithm;*
- 3. Expose a secure API endpoint to allow other European PSPs to query them;*
- 4. Identify an aggregator to connect to all the other PSPs in Europe;*
- 5. Expose VoP in all channels (e-banking, mobile banking...);*
- 6. Besides the compliance aspects, successful PSPs will leverage VoP to design premium payment security solutions for their corporate customers who require additional functionalities.*

This paper delves into two key aspects of interest within the industry: the inter-PSP communication, and the challenge introduced by the liability shift.

Firstly, from the start of the VoP discussions at the European level, our perspective has been that the main challenge for the industry is in ensuring the reachability of PSPs rather than finding the "right" infrastructure to appoint as the European VoP switch. The task of identifying a single entity that would be both legitimate and capable of operating a unified open-loop VoP switch proves elusive, especially considering that VoP is mandated for thousands of PSPs, including non-banks, and is expected to extend beyond euro credit transfers. Therefore, interoperability can only be realised at the European level if VoP is conceived as an "open" data service.

The UK Confirmation of Payee model has demonstrated that interoperability can be effectively achieved by the combination of common rules and standards, ideally supplemented by a common directory and service providers acting as aggregators.

The European Payments Council (EPC) is following a similar path with its efforts to define a Scheme Rulebook, API Specifications, and a Directory service. We are encouraged to see that the EPC is guided by the same principle of ensuring the reachability of all PSPs.

We expect the European landscape to feature a patchwork of country-specific VoP hubs operated by local payment systems, integrated into a wider network of individual European PSP VoP endpoints.

Many international banks and payment fintechs will fall outside of local VoP hubs, while European regional banks will have to weigh the pros and cons of following a unified European approach, or integrating in each local hub where they have branches.

Secondly, we are confident that the combination of the EU Regulation and the EPC Scheme Rulebook provides sufficient clarity to navigate the liability challenge. PSPs will not breach their Article 5c obligation if they are not able to reach the counterparty PSP for a VoP check, provided that they inform the payer with the right warning message. Likewise, the strict definition of a match, equating only to a perfect match, removes the risk of a false match.

Given the publication of the Regulation on March 19th, 2024, and the ongoing work of the EPC, PSPs have no alternative but to commence immediate preparations to build their VoP capabilities.



CONTENTS

1. Safer Instant Payments: New European Regulation Mandates Verification of Payee (VoP)	4
- 1.1 What Is Required by The New Regulation in Europe?	4
- 1.2 The European Direction Fits a Global Trend of Account Validation and Liability Shift	6
2. Interoperability of VoP Solutions Is Essential	9
- 2.1 Local VoP Infrastructures Remain Important	9
- 2.2 Local Schemes Without VoP Infrastructure May Augment Scheme Rules to Their Requirements	9
- 2.3 Standalone PSPs Will Adopt Request and Respond Capabilities to Meet Regulatory Mandate	10
- 2.4 European Payments Council (EPC) Scheme Enables Efficient Processing Across Markets	10
3. Liability Shift: A Pragmatic Approach to PSP Liabilities	13
- 3.1 Addressing the Availability Challenge	13
- 3.2 Addressing the Risk of Incorrect Matches	14
- 3.3 Opportunity to Help Corporates in Managing Fraud Risks	15
4. Meeting the Regulatory Compliance Challenge: What Is Needed?	17
- 4.1 Building Blocks for A Successful VoP Solution	17
- 4.2 The Way Forward – What You Should Do in The Next 6 Months	22
About The Author	23
Your Regional Contacts in Europe	23
Get Started Now! - Contact Us	24
References	24

01

SAFER INSTANT PAYMENTS: NEW EUROPEAN REGULATION MANDATES VERIFICATION OF PAYEE (VOP)

1.1 What is required by the new regulation in Europe?

*In a prior whitepaper issued in 2023*¹, we presented our insights on the European Commission's (EC) proposal, introduced in October 2022, to update the Instant Payment Regulation, aiming to enhance the Security, Speed, and Affordability of Euro payments. Our focus centered on the requirement for Payment Service Providers (PSPs) to implement bank account validation intended to bolster the security of payments within Europe.

The proposal was officially published on the 19th of March 2024, mandating PSPs in countries whose currency is the euro to comply with the IBAN validation requirements by October 9th, 2025, and PSPs in countries whose currency is not the euro by July 9th, 2027. **Article 5c of the regulation introduces a novel obligation of "Verification of Payee" for credit transfers within Europe**². Notably, the introduction of the term "Verification of Payee" (VoP) instead of adopting existing terms like "Confirmation of Payee" (CoP) from the UK or IBAN name-check from the Netherlands underscores the commitment to establish a new standard in payment security, distinct from existing frameworks.

Given the pervasive influence of the "Brussels Effect", it is foreseeable that the term VoP may evolve into a global benchmark for account validation, akin to GDPR's significance in data privacy regulations. In light of this, it is pertinent to outline the principal changes introduced by Article 5c:

- 1 Payer PSPs are mandated to alert payers in case of discrepancies between the payee's provided name and the name recorded in the payee's PSP banking records.
- 2 Payee PSPs must provide a VoP service accessible to Payer PSPs.
- 3 In the instance of "close match," PSPs are required to propose the correct payee's name to the payer.

¹iPID (2023):The Future of Confirmation of Payee in Europe, retrieved 20 March 2024
²Regulation (EU) 2024/886 of The European Parliament and of the Council, retrieved 25 March 2024

4

PSPs failing to fulfill their obligations and resulting in defectively executed payment transactions bear liability for refunding the payer.

5

Verification of Payee service must be free of charge for the payer

In addition to the updated Instant Payment Regulation, two additional European initiatives warrant attention. Firstly, the European Payments Council (EPC) is working on a VoP Scheme Rulebook, intended to offer guidance to PSPs regarding VoP implementation, as discussed in a later section of this paper. Secondly, the European Commission has proposed a PSD3 and PSR legislative package in June 2023 that includes an extension of the VoP obligation beyond credit transfers denominated in euro.

1.2 The European direction fits a global trend of account validation and liability shift

The new European obligations follow a global trend of countries implementing account validation solutions to protect customers from Authorised Push Payment (APP) fraud. The past 10 years have seen many emerging markets implementing VoP at the same time as their new generation of Instant Payment Systems. We are now seeing a new wave of projects on the back of the rapid growth of payment scams. In the past few months, we saw Australia, New Zealand, and India announcing new Account Validation projects. The UK has also notably extended their Confirmation of Payee (CoP) program to all PSPs.

Australia's recent Scam-Safe Accord (established in November 2023)³ requires banks to implement additional measures like name-matching for APP. The industry has committed AUD 100 million to develop a nationwide CoP system. This is complemented by significant investments in new account-opening verification processes, scam intelligence sharing, and other initiatives. The multifaceted approach underscores that no single tool can effectively combat scams.

Another interesting development is the trend towards shifting the liability away from payers towards PSPs. The paradigm shift in liability regimes for credit transfers (authorised push payments) resembles the mature practices in the card industry where issuers protect customers from unauthorised payments.

Ministers Treasury (2023): Government welcomes Scam Safe Accord, retrieved 20 March 2024

What are the regulatory changes in liability for APP fraud?

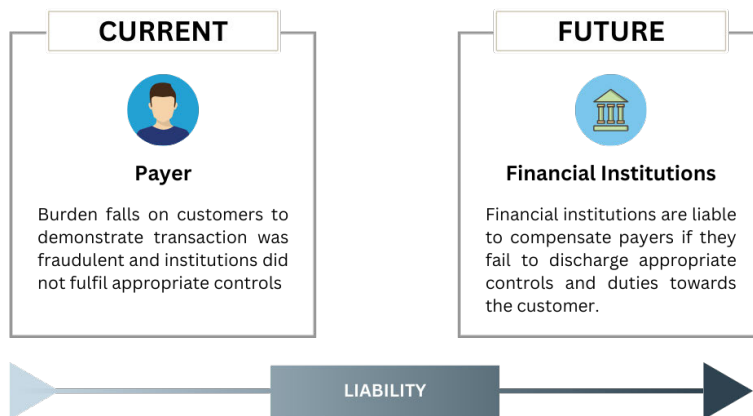


Exhibit 1: The changes in liability from payers to financial institutions.

This shift acknowledges that customers (payers) alone should not bear the full burden of scam fraud losses. Contingent liability and reimbursement models define the circumstances under which financial institutions may be held liable for reimbursement. In the UK, a Contingent Reimbursement Model (CRM) was introduced in 2019. Although initially voluntary, it has led to the reimbursement of hundreds of millions of pounds to UK consumers. The UK has since moved to introduce regulations mandating reimbursement in most cases. To fulfill their responsibilities to customers, financial institutions are adopting increasingly sophisticated methods to protect their clients and themselves from growing liability risks. The UK's CoP service, for example, helps customers verify if the beneficiary of their payment is the intended recipient through name and account matching, often supplemented with other fraud detection measures.

The emergence of these accords, frameworks, codes, and regulations worldwide indicates a significant shift towards a more accountable and collaborative fraud management framework. This transition will certainly increase the responsibilities of financial institutions. Regardless of where the liability line between consumer and institution falls, it is clearly in the institution's interest to stay ahead of this line for better brand, reputation, and customer outcomes.

Reducing APP Fraud in the UK: The Confirmation of Payee Service's Journey and Future Enhancements.

CoP, initiated in 2017 and launched in 2020, has proven to be an effective tool against APP Fraud in the UK. CoP is a name-checking service used by PSPs to verify the recipient's name and account before executing a payment, helping to avoid accidental or deliberate misdirection of funds. After the peak of APP Fraud losses in 2021, CoP contributed to a 17% reduction in 2022, despite a total of over 100,000 cases amounting to £482 million.

CoP users are regulated PSPs, governed by the PSR Directive. The system's operation, including the rulebook, commercial and legal terms, directory management, and PSP onboarding, is jointly managed by Pay.UK and the Open Banking Implementation Entity (OBIE). Starting with the six largest banks under the Competition and Markets Authority (CMA), the service now extends to more than 100 PSPs, encompassing over 92% of CHAPS and Faster Payment transactions. To further enhance coverage, the PSR's Specific Direction 17 of October 2022 mandates an additional 300+ PSPs to implement CoP by October 2024, increasing the coverage to 99%.

CoP operates through API calls made by the payer's PSP to the payee's PSP, with responses indicating Match, No Match, or Close Match. Each PSP must provide a response based on the account holder's record at the time. Despite the directory management by OBIE and new participants onboarding through Dynamic Client Registration, each participant is required to maintain their own matching engine without a centralized matching or account database. While the decentralized model allows autonomy in managing account data and matching, it poses challenges such as increased overheads for each institution due to the need for an independent matching engine.

2024 will herald significant change for CoP as Pay.UK introduces a new directory service provider, to replace OBIE, and a new participation model (Aggregator Model) to support the scaling of the service to more than 400 PSPs overall. These changes will intensify already busy roadmaps and must be delivered before the October 2024 deadline from the Payment System Regulator (PSR). However, they pave the way for simpler administration and operations for Pay.UK and PSPs as Vendors pick up more responsibilities on their behalf.

A successful transition will reinforce CoP as a gold standard for other domestic schemes worldwide to follow. As the EC's Verification of Payee (VoP) mandate for instant credit transfers seeks to emulate CoP's success, Bottomline propositions will be significantly enriched by the expertise we've developed over the last four years. And as the ubiquity of account name verification grows across the global payment landscape it offers a promising future in pre-validating payment transactions to prevent fraud.

Written by,
Vitus Rotzer
Chief Revenue Officer, Banks & FIs
Bottomline Technologies





INTEROPERABILITY OF VOP SOLUTIONS IS ESSENTIAL

The European Central Bank (ECB) reports that there are over six thousand institutions in Europe providing payment services or eligible to do so. While the decision by EU legislators to separate VoP rails from payment rails was well-advised, it prompts the question of the ideal inter-PSP communication platform. It's clear that a singular VoP network will not exist. Consequently, we anticipate the European landscape will evolve into a patchwork of Verification of Payee (VoP) solutions composed of local VoP infrastructures, local/regional schemes, and standalone PSPs.

2.1 Local VoP infrastructures remain important.

In the realm of European payments where the majority of transactions are domestic, we believe that local VoP infrastructures are crucial. Local needs are typically better met by local infrastructures, and we anticipate that many local banking associations and payment systems will take steps in implementing VoP solutions tailored to their member banks.

We expect to see local VoP infrastructures following a "Central Orchestration Platform" model.


A Central Orchestration Platform is not synonymous with a centralised database. Instead, it involves centralising specific functions, which brings efficiency to the local ecosystem of PSPs. These functions may include routing VoP requests, centralised matching, data enrichment, and facilitating international interoperability.

2.2 Local Schemes without VoP infrastructure may augment scheme rules to their requirements.


Establishing a local VoP infrastructure necessitates a robust collaboration framework among local PSPs and the appointment of a VoP infrastructure operator by the community. In cases where these elements are lacking, countries may opt to augment the EPC scheme Rulebook with additional local scheme rules to align more closely with domestic or regional preferences. For example, the Nordic Payment Council (NPC) has introduced the Confirmation of Payee (CoP) Scheme, which outlines roles, practices, and standards for participating entities. Notably, the NPC Scheme predates the adoption of the EU Regulation and the EPC Scheme, and it will be informative to observe how they may coexist. The Nordic countries face the additional complexity that they are part of SEPA but only Finland uses the euro as its domestic currency. Hence, the EU Regulation (and timeline) will not uniformly apply to all credit transfers.

2.3 Standalone PSPs will adopt request and respond capabilities to meet regulatory mandate.

By default, or by choice, some PSPs will fall outside of the two categories mentioned above. Those PSPs will expose their responding capability in alignment with the EPC scheme and will source their own aggregator to connect to all other Payee PSPs. Such institutions include:

 **European Regional Banks:** Large international banks with a presence in multiple countries may prefer a unified approach by exposing a VoP endpoint that is consistent across their group instead of implementing localised responding capabilities in each country. While this approach aligns with the EU regulatory framework, regional PSPs should review the business case of opting out of local VoP infrastructures.

 **European entities of international Banks:** Some international banks with entities in Europe may be connected to European payment rails (e.g. EBA Clearing) but not to a local payment system. The ECB or EBA Clearing may play a role as an aggregator to access Payee PSPs VoP services, but it remains uncertain whether they could serve as full-fledged VoP infrastructure providers, especially considering that many of their participants may delegate their responding capability to local VoP infrastructures. Consequently, European entities of international banks are likely to expose their own VoP endpoint.

 **The long tail of PSPs:** The past decade has witnessed a surge in the number of neobanks and fintechs offering IBANs to retail or business customers. These institutions, though typically not part of local infrastructures, must comply with EU regulations. Addressing the long tail of PSPs presents a challenge both for these PSPs, who need to procure their own VoP solutions, and for Payer PSPs, who require a solution to access these long-tail Payee PSPs. For instance, in the UK alone, the long tail of PSPs (also identified as Group 2 in the CoP initiative) amounts to around 400 institutions, and considering the European Union's 27 countries, this figure will be significantly higher.

2.4 European Payments Council (EPC) scheme enables efficient processing across markets.

In this complex patchwork of VoP solutions, we are thrilled to see that the industry has begun collaborating, with the EPC taking the lead in defining a VoP European scheme, expected to be finalised by the end of 2024. Following the subsidiarity principle, we believe it's realistic for the EPC scheme to establish key guidelines for VoP to enable interoperability without being overly prescriptive. Local schemes and infrastructures may then build upon the EPC scheme with additional requirements reflecting local sensitivities and realities. For instance, matching principles could incorporate specificities related to language and data privacy preferences.

Standard for Verification of Payee Interoperability

The obligation to offer Verification of Payee (VoP) as part of new EU regulation on SEPA payments will soon become effective. VoP obligates a PSP to inform a payer of the correctness of the name of the payee, as registered by the PSP of the beneficiary before the payment is authorised. With that PSPs in SEPA are confronted with an additional interoperability and reachability challenge, with very little time available to realise this with full SEPA reach. The EPC, having already set the de facto market standards for SEPA payments and direct debits has therefore taken the initiative to set up a new, additional VoP Rulebook with a set of rules, practices, and standards to:

- Achieve interoperability for the provision and operation of verifying payment account numbers and payment account holder names;
- Between participants of the scheme
- Prior to initiating an account-based payment within SEPA.

To achieve true SEPA interoperability and given the short timeline, this first VoP Rulebook aims to set the core basis for interoperability between PSPs in SEPA. The VoP Rulebook will be separate from the already-in-place EPC Rulebooks on payments. PSPs will need to adhere separately to VoP, with the aim that the large majority of PSPs choose this VoP Rulebook as their basis for SEPA VOP reachability. In line with the infrastructure for payments, PSPs can make use of service providers, provided they offer VoP services in line with the EU regulation, including (routing to) full reachability.

A directory service and API specifications are foreseen. After the public consultation period ending 9 June 2024, the first version of the VoP Rulebook will be finalised.

An inventory by the EPC teaches us that there is a variety of setup, operating rules, and additional services. Additional services are left to the service providers under the condition that they do not hinder the basic functionality of the VoP standard i.e. the requirements of the EU regulation. Additional (optional) requirements can in the future become part of the EPC VoP Rulebook when a majority of its users decides that it is beneficiary for all. The Focus for now is to achieve basic interoperability and reachability.

Written by,
Frans C. van Beers
Senior Policy Consultant Payments, Dutch
Payments Association;
Chair CoP (VOP) Task Force European Payments
Council (EPC)



We are encouraged to see the initial version of the VoP Scheme Rulebook, for the following reasons:



-  **Open interoperability:** The scheme ensures that Payee PSPs do not restrict VoP endpoint accessibility to closed-loop environments, thereby ensuring equitable access for all Payer PSPs.
-  **Standardised data elements:** The EPC's definition of standardised data elements and technical Inter-PSP requirements based on ISO 20022 will enhance interoperability.
-  **Recognition of third parties:** The rulebook introduces the role of Routing and Verification Mechanisms (RVMs), and outlines their role in routing VoP requests, and possibly responding on behalf of PSPs. Local infrastructures and providers like iPiD fall under the category of RVMs. Importantly, the Scheme emphasises that the PSPs remain responsible for their obligations.
-  **Acknowledgment of Additional Optional Services (AOS):** The rulebook demonstrates pragmatism by recognising the likely existence of complementary services enriching the VoP service. These AOSs are likely to exist at the national, sub-regional, or RVM levels. Importantly, the drafted Scheme stipulates that AOSs must not compromise European-level interoperability, thereby preventing organisations from utilising AOSs to construct de facto closed-loop environments.
-  **Guidelines for matching principles:** While the rulebook does not include technical specifications for matching, the EPC is separately defining recommendations for the matching process, which will prove helpful. Regulatory frameworks and EPC drafts suggest that a positive "match" response will denote an exact match. Identifying an exact match between name strings does not necessitate sophisticated matching capabilities. However, since PSPs will be obligated to return the payee's name in case of a "close match," the quality of the matching algorithm will play a crucial role in distinguishing a "close match" from a "no match" in a manner that safeguards data privacy.

We believe the EPC has successfully balanced pragmatism with ambition. A notable example of this balance is the EPC's intention to participate in the establishment of a common directory encompassing all PSPs, along with their reachability details, including the locations of their VoP endpoints. This directory, combined with the Scheme Rulebook, lays a solid foundation for achieving practical interoperability of VoP across Europe.



LIABILITY SHIFT: A PRAGMATIC APPROACH TO PSP LIABILITIES

The Instant Payment Regulation shifts liability for fraudulent transactions from the payer to their PSP in two instances:

-  If a payment is defectively executed and the payer was incapable of performing a VoP, or the namecheck was wrongly returning a match.
-  If a payment is defectively executed and the Payee PSP is unable to respond to a VoP request or returns incorrect results.

We advocate for a pragmatic interpretation of the liability shift provision. The EU legislator's underlying intention is to move the payment industry away from situations where payee names are not verified, allowing payers to be deceived into sending money to the wrong account. To achieve this, the legislator imposes operational obligations on PSPs to provide VoP services to payers and on Payee PSPs to invest appropriately in maintaining quality payee data and exposing a VoP capability.

Two primary liability concerns for PSPs will be (i) the unavailability of the VoP service and (ii) incorrect matches. We believe that the crucial factor for PSPs in managing their liability implications lies in how effectively they communicate with payers regarding VoP outcomes.

3.1 Addressing the availability challenge

We expect that VoP schemes will coalesce around four potential outcomes:

1. Match
2. No Match
3. Close Match (with name suggestion)
4. VoP not possible

In instances of outcomes 2, 3, and 4, the Payer's PSP will be obligated to alert its account holder that executing the transaction may result in a payment to an incorrect payee. By providing a warning, Payer PSPs fulfil their regulatory obligations and absolve themselves of liability if the payment is defectively executed.

Occurrences of Outcome 4 should be minimized, but they may be unavoidable in scenarios such as when the Payee PSP's VoP endpoint is inaccessible, the service provider is unavailable, or the PSP is not yet reachable.

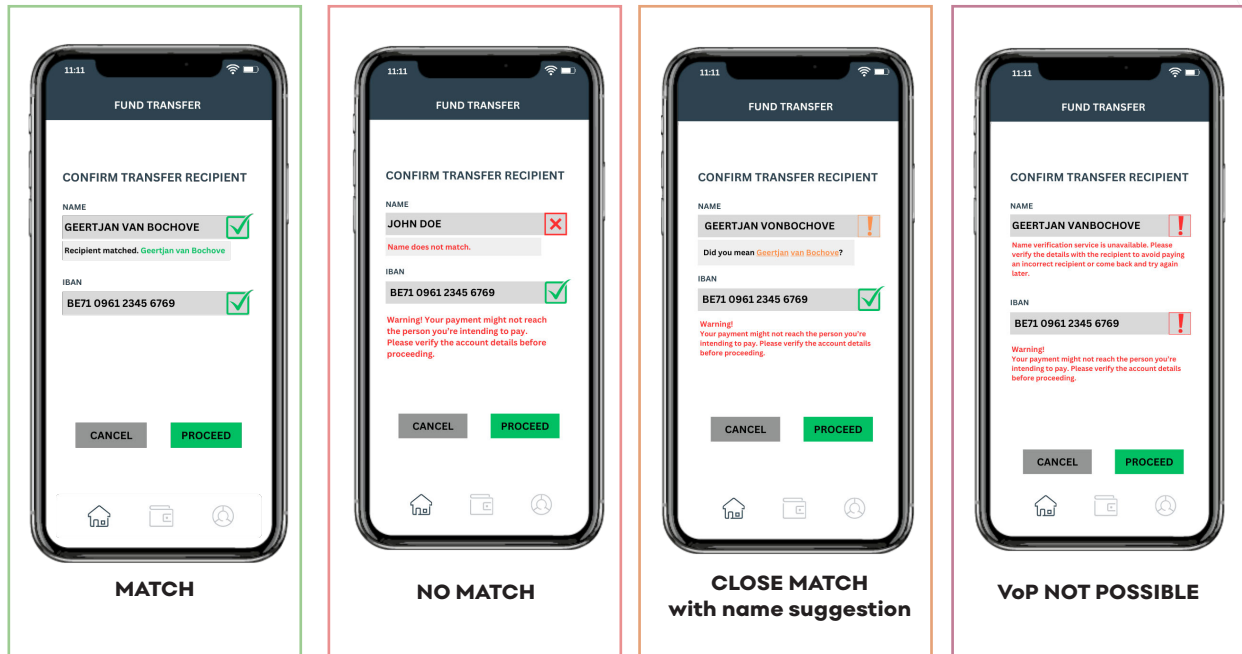


Exhibit 2: Examples of VoP outcomes

To optimise their communication with customers, Payer PSPs can display customised messages to guide payers on the appropriate course of action. For example, during temporary downtime, PSPs could advise payers to retry later or suggest queuing the instruction until the name verification can be completed.

The remarks mentioned above should not be interpreted as a way to bypass regulatory obligations. PSPs and service providers will have to treat VoP as a high-availability service and leverage available technology solutions to ensure a high resiliency.

3.2 Addressing the risk of incorrect Matches

Our understanding of the Regulation and EPC Scheme regarding matching outcomes indicates that "match" will predominantly entail perfect matches, with minimal tolerance for fuzzy logic. Consequently, the risk of a "false match" is virtually inexistent as matching algorithms can easily identify perfect matches between two name strings. This interpretation diverges from current practices in the UK or the Netherlands, potentially resulting in a lower percentage of "match" outcomes in the European VoP context. However, we believe this variation will not significantly impede the successful deployment of VoP in Europe. Taking the example of two names that would only differ by one character, instead of a "match", VoP will return an "almost match" with a name suggestion, which remains practical and effective, especially within mobile and e-banking platforms.

Adopting a strict definition of the match as a perfect match significantly mitigates the risk of "false matches". As an additional safeguard, we propose that Payee PSPs also provide the payee's name in instances of a "match" as illustrated in Exhibit 3.

3.3 Opportunity to help corporates in managing fraud risks

The main advantage of the liability shift introduced in Article 5c is that it constitutes a strong incentive for PSPs to comply with the Regulation and introduce VoP within the timeline. Retail customers and SMEs are expected to derive immediate benefits from VoP being exposed in mobile and e-banking channels.

Larger corporates will also benefit from this new security layer, but they will require more sophisticated solutions integrated into their vendor onboarding portals, ERP, or Treasury Management System. It's important to note that the Regulation includes an opt-out provision for bulk payments. Corporations might be tempted to utilise this option to avoid the operational challenges associated with having their payment files subjected to a line-by-line VoP review for each payee.

APP fraud remains a genuine threat for CFOs and Treasurers, underscoring the importance of adopting dedicated technology solutions tailored to their operational needs. We anticipate that corporates will increasingly turn to these solutions to bolster their defenses against fraudulent activities. Additionally, PSPs stand to capitalise on this trend by offering white-labeled corporate payment security solutions to their clients.

Verification of Payee for large companies: a perfect match?

In 2023, only 15% of B2B transfers were carried out instantaneously. While the obligation to make instant transfers available is becoming clearer by 2024, there are many questions to be answered, as few bank service providers are yet equipped to carry out this type of transfer. And what about the risk of fraud? With instant transfers, one can send a payment to the recipient in less than ten seconds. If the bank details are fraudulent, money is gone, with no chance of recovery. This risk is too important to be taken lightly.

Thanks to the new European regulations, most of the irritants aim to be resolved. As far as fraud and compliance are concerned, banks will be responsible for alerting if the match between an account number and bank details entered is invalid and for reconciling beneficiaries with international sanction lists to comply with LCB-FT obligations. Although CoP schemes such as CopUK, provide this type of information in Europe, there is a lack of uniformity in the level of response depending on the implementation methods used in each country, rendering it insufficient for corporates to make the right decision. And finally, validation is too late in the payment chain. In order to carry out in-house remediation, knowing the reason for an invalidation is a non-negotiable asset for companies.

In response to this need, tools such as Sis ID integrate the validation process as early as possible in the payment chain and provide a detailed analysis of the suitability of bank details for the addressee, which goes beyond mere legal status (payment holding company, mule company, factoring).

Thanks to a unified and shared approach to fraud detection within the real-time user community, the solution supplements the available bank and institutional databases with shared databases, enabling companies to check whether a bank identifier corresponds to the bank details entered. When this is not the case, the tool provides the reason for the invalidation (closed establishment, manual input error, identity theft...). This enables companies to simplify their remediation actions upstream of the payment chain, rather than at the point of instantaneous dispatch of funds.

The advantage of Sis ID is to achieve the perfect match. If a customer gets a red flag because the company entered is closed, Sis ID will pass on the information. In parallel, the solution also offers a bank details certification service. If companies check bank details/identifier couple well upstream of the payment chain, they will obtain the perfect match they're looking for."

Written by,
Laurent Sarrat
CEO and Co-Founder
Sis ID



04

MEETING THE REGULATORY COMPLIANCE CHALLENGE: WHAT IS NEEDED?

4.1 Building blocks for a successful VoP Solution

PSPs will need the support of service providers to meet their regulatory requirements. The market demands several categories of solutions:

- Channel and payment workflow integration:** All Payer PSPs must integrate VoP in their channels (mobile banking, e-banking, branches...).
- Aggregation of access to Payee PSPs:** Payer PSPs and Domestic VoP infrastructures need a single access point to all other Payee PSPs, including the long tail PSPs.
- VoP PSP module:** PSPs not delegating their responding obligations to local infrastructure will need a module encompassing a matching capability, a VoP endpoint for Payer PSPs, and connectivity to an aggregator to access Payee PSPs.
- Core banking integration and data management:** All Payee PSPs must maintain high-quality payee data and develop the capability to query this data promptly.

Most PSPs are on a journey of modernizing their core infrastructures towards more flexibility and "composability". Traditional monolithic systems are replaced by smaller, independent components or "microservices." VoP will be an additional project next to several others, and we expect PSPs to look for a similar "composable approach".

Modernising Banking Technology and Enhancing Compliance

To stay competitive and comply with evolving regulations, PSPs are modernizing their technology infrastructures and enhancing compliance. We delved into these crucial changes in a discussion with **Damien Dugauquier**, CEO of iPiD, **Christian Sarafidis**, Chief Executive EMEA Financial Services at Microsoft, and **Jeroen Holscher**, Global Head of Payment Services at Capgemini.

Dugauquier: What is your perspective on how banks are modernising their technology stacks?

Sarafidis: The Financial Services industry continues to witness transformative trends that are reshaping how banks engage with their clients. With clients at the center of their digital strategy, enhancing client experience is paramount. To achieve this, banks must adapt their business models, streamline end-to-end processes, and modernise their core platforms. As part of their digital transformation journey, banks are increasingly adopting Microsoft Cloud, specifically Azure, to migrate their critical applications

D: Based on your long experience working with banks, what are the key considerations that banks should have in mind as they plan the integration of VoP with their channels on the payer side?

Holscher: From the payer's perspective, VoP integration must be frictionless and seamlessly integrated into the customer payments initiation journey. We are anticipating banks to adopt a more adaptable "as-a-service" approach rather than hardcoding VoP into channels. However, some banks will face the challenge that a lot of channels do not have real-time and always-on capabilities. They will have to review channel capabilities to meet their regulatory obligations. Even host-to-host channels for bulk files will require meticulous design to meet non-functional requirements.

D: And what about from the payee's perspective?

H: As a payee PSP, data quality and the always-on requirement are paramount. Ensuring accessibility to data 24/7/365 presents its own set of challenges, especially with data updates and synchronisation. Core banking systems are not meant to be used as real-time data pools. On the side of new opportunities, we see a potential value-add in leveraging VoP requests to aid in fraud prevention. Leveraging early fraud signals at the VoP pre-transaction stage can be helpful, especially in the context of instant payments.

D: Could you provide some insights into how banks are adapting their business models and leveraging technologies like Microsoft Azure in this context of being real-time and always-on?

S: We see a growing number of banks leveraging Azure to pave their journey towards resilient, modern, and adaptable architectural designs. Azure offers best-in-class cloud capabilities, unparalleled scalability, high performance, and robust security indeed. This globally distributed cloud infrastructure is designed with sustainability in mind, allowing applications to be deployed closer to users. It provides comprehensive compliance and resiliency options for customers. Moreover, Azure leads the way in innovation with its robust data platforms, powerful AI capabilities, and its rich partner ecosystem, enabling the transition to composable banking, where banking applications securely interact as microservices.

D: How do you see solutions like iPiD fitting into this landscape?

H: iPiD offers a flexible and innovative solution to address the Verification of Payee requirements, supporting banks in their journey to compliance with easy integration and multiple service options. With the evolving landscape of composable banking and the need for seamless VoP integration, solutions like iPiD play a crucial role in accelerating banks' compliance efforts while enhancing the overall customer experience.



Ideally, VoP would seamlessly integrate as a native component within all key applications, including Core Banking, Payment Engines, Channel applications, Payment networks, Payment systems, Hosting providers, payment data providers, and managed services offered by system integrators. Additionally, some PSPs may seize the opportunity to extend VoP capabilities as a service to other PSPs.

At iPiD, our core mission revolves around aggregating connectivity to all eligible Payee PSPs and powering the ecosystem with the simplicity of a single API. The industry would incur substantial costs if every PSP and service provider had to independently establish connections to all Payee PSPs. At iPiD, we are committed to undertaking the arduous task of aggregating these endpoints and offering them as an open infrastructure layer that can be utilised by all stakeholders in the ecosystem.

Empowering Global Financial Institutions with End-to-End Payment Solutions and Fraud Prevention.

Finastra has been delivering mission-critical payment solutions for over 30 years with a global customer base of over 300 financial institutions of all sizes; more specifically we have been delivering instant payment solutions since 2008 with UK Faster Payments, and following with Singapore FAST, Australia NPP, America TCH and now FedNow, Europe RT1 and TIPS and many more. Our multi-rail payment hub solutions (Global PAYplus, and our PaaS offering, Payments To Go) are pre-integrated with our innovation and collaboration marketplace, FusionFabric.cloud (FFDC) which hosts specialist fintech services that complement our products and help us provide end-to-end solutions. We are focused on digital initiation, AML & compliance filtering (OFAC), fraud detection, and alternate methods of payment. With the new EU regulations on instant payments mandating a VoP service, we recognized this as a functionality we would need to deliver through our partner ecosystem.

Using iPiD's services we are able to offer a single window for global VoP (access to live VoP services across the world covering 2.5+ billion accounts e.g. UK, India, and South Korea) and an adaptor for local VoPs (with pre-built integration for new standalone VoP services). In addition, with iPiD, Finastra can support an unattended use case where decisions are automated; this is particularly relevant to instant payment processing where target turnaround times are of the order of one second.

For Finastra, the partnership with iPiD gives the company access to iPiD's global bank account validation API. This will allow Finastra to offer its customers a wider range of financial services and solutions that are specially built to combat the rising level of fraud and scams in the context of instant payments **(for example, in H1 2023 in the UK, over 80% of all APP fraud occurred on instant payments)**⁴.

Written by,
Eran Vitkon
Head of Open Banking solutions
Finastra

FINASTRA

⁴UK Finance (2023): Half Year Fraud Update, retrieved 20 March 2024

Enhancing Global Payment Security: The Impact of Verification of Payee Proposals on Fraud Prevention and Efficiency.

Authorised Push Payment fraud is a growing concern worldwide, so it is with great anticipation that we welcome the recently published Verification of Payee proposals by the EPC. The powerful combination of IBAN-based account verification with ISO 20022 is guaranteed to standardise push payments while ensuring the speedy and effortless payment experience we have all grown to expect.

Having witnessed the implementation of Confirmation of Payee in the UK, it is clear that standard industry-wide orchestration with common APIs will regulate how bank participants share account information with their trust networks. What's more, as network participants adopt the regulation, VoP promises to be extremely scalable.

The success of VoP for banks, corporates, and PSPs will vary, depending on how account verification is implemented. Those seeking maximum impact must embrace the following:

- Think big! While the scope of VoP is restricted to Europe, large banks and corporates will benefit from solutions and suppliers that extend beyond Europe, empowering them to realise cross-border payment benefits on a global scale.
- PSPs and corporates should view the benefits of VoP through a holistic lens, with consideration for end-to-end payment efficiencies and straight-through processing in relation to SEPA payments.
- Holistic fraud management is extremely important. Organisations should adopt VoP in the context of wider fraud challenges, such as robust onboarding of new customers and avoiding impersonation attacks on existing customers. This will drive end-to-end efficiencies and foster significant value across the organisation.

Supercharging STP rates while propelling fast and cost-effective payments is made possible by a successful partnership with the right strategic supplier – they will make the process smoother and reduce long-term costs. Whether you are looking for solutions that enable common APIs for VoP, CoP, or cross-border account verifications, LexisNexis® Bankers Almanac® Validate™ delivers safe, seamless, and one-stop account-level confirmation on a global scale.

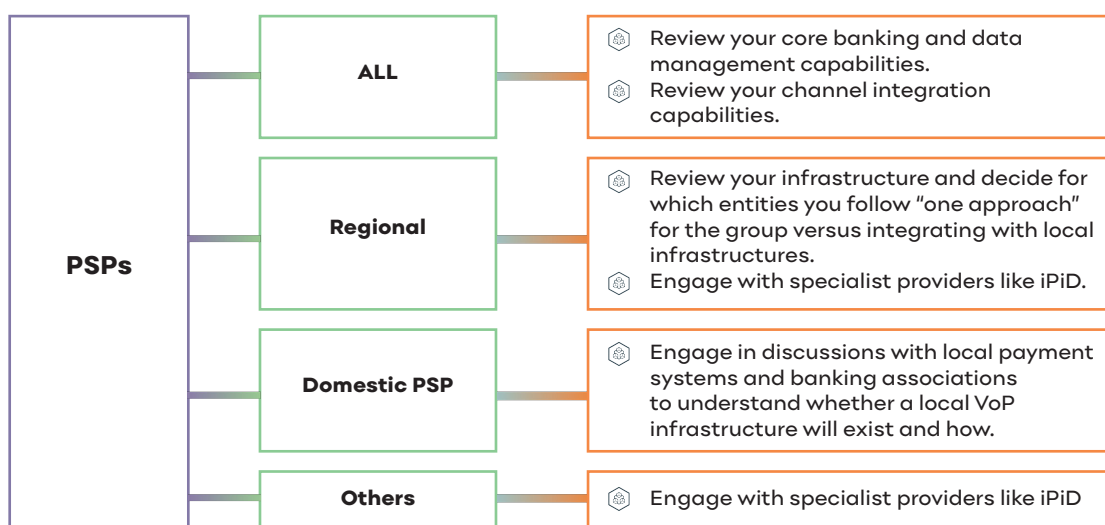
LexisNexis® Risk Solutions is thrilled to be partnering with iPiD to deliver Bankers Almanac® Validate™ Safe Payment Verification, enabling organisations to verify that account details are routed to the true intended end recipient and reduce the risk of fraudulent or inaccurate transactions.

Written by,
Ed Metzger
VP Payments Efficiency
LexisNexis® Risk Solutions



4.2 The Way Forward – What you should do in the next 6 months

Whether the industry likes it or not, the race to compliance has started! These are the next steps PSPs shouldn't miss in the next 6 months.



At iPiD, our commitment is to shield PSPs from the complexity of the VoP Regulation. We provide a one-stop-shop solution that integrates with PSPs' core-banking systems, manages bulk file validation, leverages a matching algorithm aligned with VoP requirements, ensures compliance with the EPC Scheme Rulebook through an exposed API endpoint, and provides a single API to reach all other PSPs in Europe.



ABOUT THE AUTHOR

Damien Dugauquier, Co-founder and CEO at iPiD. As former Head of Data and Analytics at SWIFT, Damien brings a wealth of payment knowledge and experience, having worked with financial institutions and corporates across Asia and Europe.

YOUR REGIONAL CONTACTS IN EUROPE

Geertjan van Bochove, Co-founder, COO, and CFO at iPiD based in the Netherlands. Geertjan is a serial entrepreneur, and has amassed considerable experience in the payment industry, working closely with European banks and European payment systems.

Alain Raes, founding partner and CCO at iPiD based in Belgium. With his 15-year tenure in the executive committee of Swift, Alain has built a reputation of formulating effective business growth strategies. Alain has worked with banks and market infrastructures alike, and was there at the inception of instant payments and overlay systems across the globe.

Greg Huguet, Regional Director for Europe at iPiD. With over nine years of experience in Swift, Greg has played a pivotal role in various capacities, notably as the Payments Market Director for the UK & Ireland, driving forward the evolution of cross-border payment infrastructures in these regions.

ABOUT iPiD

iPiD is a fast-growing, venture-backed fintech start-up that was founded in late 2021 by a global team who have held senior roles at major payments and technology companies, including SWIFT and Thomson Reuters. In addition to our HQ in Singapore, our global team has representatives in India, Belgium, Malaysia, UAE, the Americas, Australia, Netherlands, South Africa, Spain, and Vietnam.

iPiD's vision is to make cross-border payments easy, secure, and seamless by facilitating trust in the global financial ecosystem, and we achieve this by partnering with financial services providers such as banks, payment systems, payment fintech, and wallets. We offer two core solutions, Validate and Fetch, both of which are designed to provide an enhanced payment journey that reduces cost, mitigates fraud, and improves the overall customer experience. iPiD is built for all – we do not replace banks, payment fintech, wallets, or remittance companies; nor do we replace existing payment rails.

Our Advisory Board includes senior figures from across the industry: Christian Sarafidis, Microsoft Chief Executive EMEA Financial Services and Chief Business Development Officer, WWFSI; Kosta Peric, Deputy Director, Financial Services for the Poor, the Bill & Melinda Gates Foundation; and Nick Lewins, former banking Chief Technology Officer and now an advisor in data and AI, cloud technology and digital transformation.

GET STARTED NOW!

iPiD provides infrastructure solutions for bank account validation and proxy addressing, as well as a global bank account validation API that interconnects local schemes.



Get in touch for a free trial of iPiD's Validate API

Contact us now at sales@ipid.tech

REFERENCES

1. iPiD (2023): The Future of Confirmation of Payee in Europe, <https://ipid.tech/the-future-of-confirmation-of-payee-cop-in-europe>.
2. Regulation (EU) 2024/886 of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202400886.
3. Ministers Treasury (2023): Government welcomes Scam Safe Accord, <https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/government-welcomes-scam-safe-accord>.
4. UK Finance 2023 Half Year Fraud Update, <https://www.ukfinance.org.uk/system/files/2023-10/Half%20year%20fraud%20update%202023.pdf>.