

Digital payments: Navigating the landscape, addressing fraud, and charting the future with Confirmation of Payee solutions

Received (in revised form): 3rd November, 2023

Damien Dugauquier*

Co-founder and Chief Executive Officer, iPiD, Singapore

Geertjan van Bochove**

Co-founder and Chief Financial Officer/Chief Operations Officer, iPiD, The Netherlands

Alain Raes†

Founding partner & Chief Commercial Officer, iPiD, Belgium

Jean-Julien Ilunga††

Regional Director, Europe, iPiD, Belgium

Damien Dugauquier is the co-founder and Chief Executive Officer at iPiD based in Singapore. As former Head of Data and Analytics at SWIFT, Damien brings a wealth of payments knowledge and experience, having worked with financial institutions and corporates across Asia and Europe.

Geertjan van Bochove is the co-founder, Chief Operations Officer and Chief Financial Officer 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 is a founding partner and Chief Operations Officer 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.

Jean-Julien Ilunga is Regional Director for Europe at iPiD, based in Belgium. Jean-Julien spearheads the development of iPiD's sales strategies and initiatives in Europe and has an investment banking background.

ABSTRACT

This paper explores the evolving landscape of digital payments, with a specific focus on the confirmation of payee (CoP) mechanism, which has been designed to enhance the accuracy and security of payee identification. Traditional payee identification methods, reliant solely on account numbers, face increasing limitations amid the growing sophistication of both domestic and cross-border payments. The rise of instant payments and their associated fraud risks underscore the urgent need for more reliable payee identification systems. Drawing insights from domestic markets where CoP has been implemented, this paper presents the challenges, regulatory responses and the potential of a CoP scheme for Europe and globally. We argue that while a singular European solution is unlikely, interoperability will be the key to success. The paper concludes by envisioning the future of payee identification, exploring the global potential of CoP, and urging the industry to perceive CoP solutions as public goods of benefit to all stakeholders in the payments sector.

Keywords: digital payments, confirmation of payee (CoP), payee identification, instant payments, cross-border payments, fraud risks, interoperability



Damien Dugauquier



Geertjan van Bochove



Alain Raes

*iPiD,
80 Robinson Rd,
#18-03,
Singapore 068898

E-mail: dd@ipid.tech

**iPiD, The Netherlands

E-mail: gvb@ipid.tech

†iPiD, Belgium

E-mail: alain.raes@ipid.tech

††iPiD, Belgium

E-mail: jean-julien.ilunga@ipid.tech

Journal of Payments Strategy & Systems
Vol. 17, No. 4 2023, pp. 359–371
Henry Stewart Publications,
1750-1806



Jean-Julien Ilunga

INTRODUCTION

In the ever-evolving landscape of financial technology, the importance of secure, efficient, and user-friendly methods of payment cannot be overstated. As digital push payments continue to grow in popularity and sophistication, both domestically and across borders, the demand for reliable payee identification also grows exponentially. The traditional approach, where payment processing relies solely on account numbers for identification, no longer suffices in today's digitised and globalised world, prompting us to re-examine how payees are identified.

Confirmation of payee (CoP) — an emergent solution designed to improve the reliability of payee identification — is increasingly shaping conversations around payment security.¹ This system, which matches the payee name with account details, has shown promise in reducing fraudulent transactions and accidental misdirected payments, enhancing consumer confidence in digital payment methods.

The European Commission's recent proposals to mandate IBAN name-checks (in other words, CoP) is only intensifying the interest on the topic. This paper explores the challenges and potential of CoP, focusing on its implementation within both domestic and cross-border payment contexts. We delve into the rise of digital payments, the existing limitations within payee identification, and associated fraud risks. We continue with the learnings from domestic markets where CoP has already been implemented and suggest key principles to ensure the success of CoP in Europe and globally.

THE EVOLUTION OF DIGITAL PAYMENTS

The last two decades have borne witness to an unprecedented evolution in the world of payments. This shift, from traditional modes of transactions to digital payments, is spurred by various technological innovations and

changing consumer behaviour. To better comprehend the dynamics of today's digital payment landscape, it is crucial to understand this evolution.

Digital payments first emerged as a fringe idea, primarily limited to tech-savvy consumers and forward-thinking businesses. However, their convenience, efficiency, and ability to transcend geographical boundaries quickly became apparent.

In the world of card transactions, the introduction of contactless payments using near-field communication (NFC) and radio frequency identification (RFID) technologies has simplified in-person transactions immensely, allowing customers to execute payments by simply tapping their card, phone or watch on point-of-sale terminals. Card transactions are also known as pull payments as they are initiated by the merchant (payee) and approved by the customer (payer).

Push payments — referring to payments initiated by the payer, from their account to the payee's account — have seen even greater digital transformation. Internet banking, for instance, replaced the need for physical cheques and visits to the bank by facilitating instant money transfers, bill payments and remote access to account information. The advent of smartphones further expedited this digital revolution, introducing mobile wallets and apps, allowing individuals to make payments directly from their mobile devices.

Businesses were quick to embrace digital pull and push payments, recognising the value they offered in terms of increased efficiency, cost reduction and improved customer experience. Simultaneously, FinTech startups and the new generation of instant payment systems have disrupted peer-to-peer (P2P) payments, offering quick, easy, and often free money transfers between individuals.

However, despite these advancements, the rise of digital payments has not been without its challenges. Push payments offer great

benefits in terms of costs, but they face an inherent deficiency. As push payments are initiated by the payer, they rely on the payer to identify the payee correctly. Unfortunately, identifying payees by their banking details is not a straightforward process. Furthermore, payment systems are not designed to validate those banking details as part of the payment clearing process. The issue of payee identification has persisted as a significant concern in domestic payments, becoming more acute with the increased speed and volume of transactions.

THE PROBLEM WITH PAYEE IDENTIFICATION IN DOMESTIC AND CROSS-BORDER PAYMENTS

An essential but often overlooked aspect of digital payments, whether domestic or cross-border, is the accurate identification of payees. The need for this is evident when considering the volume of transactions processed daily and the substantial risk of fraud within such an ecosystem.

In the current payment model, the responsibility of inputting correct payee details rests largely on the payer. This is especially true for bank transfers, where a customer has to provide the name and account number (and in some jurisdictions, the sort code or bank identifier) of the payee. In most countries, for domestic transactions, neither the payment system nor the beneficiary banks perform name checks on payment instructions. Human error, such as mistyping a single digit, can result in funds being sent to the wrong recipient.

Worse, fraudsters exploit these weaknesses to commit ‘authorised push payment’ (APP) fraud, where they trick individuals into sending them money. The victim believes they are making a legitimate payment, such as buying goods online or paying an invoice, when they are actually sending money directly to the fraudster. The immediacy of digital payments, especially instant transfers,

makes it almost impossible to reverse the transaction once it has been initiated.

According to a recent report from ACI Worldwide, APP scams were the most common fraud tactic in 2022.² Financial crime and fraud are perennial problems for banks and financial institutions, with the global cost of fraud predicted to be US\$40.62bn by 2027.

In another report produced by ACI Worldwide, losses to APP fraud are expected to double across the UK, India and the US in the next four years, hitting US\$5.25bn (£4.44bn), with a compound annual growth rate of 21 per cent across the period.³ Last year, losses to APP fraud amounted to US\$2.7bn, accounting for 0.047 per cent of the total value of real-time payments across the three markets studied.

In the UK, over £1.2bn was stolen through fraud in 2022, with APP scams accounting for over one-third of these losses, at £485.2m.⁴ Within this, 57 per cent of all reported cases related to purchase fraud, with case volumes breaking 100,000 for the first time. Investment fraud continued to be one of the largest proportions of APP losses (24 per cent).

In Australia, meanwhile, more than AU\$3bn has been lost to APP scams in 2022.

Payee identification problems also affect businesses. Without a reliable payee validation method, the burden of preventing fraud and managing and rectifying errors can be substantial. Fraudulent activities, such as identity theft, fake invoices and payment scams, can cost business a significant amount of money. Accurate payee identification helps in preventing such fraudulent transactions and contributes to building trust and credibility with customers and suppliers. When businesses can confidently verify the identities of their payees, it demonstrates a commitment to information security practices and enhances the overall relationship with stakeholders.

Furthermore, a large part of the technology handling cross-border payment

systems is based on legacy technology built when paper payment processes were initially being migrated to electronic systems. These legacy technologies have fundamental limitations, including the need to process in batches, a lack of real-time monitoring and low data processing capacity. This requirement to interface with legacy technology can be an obstacle to the emergence of new business models and new-generation technologies.

PAYEE IDENTIFICATION AND VALIDATION SOLUTIONS

Proxy payments have been implemented in several countries to simplify the payment process. These enable users to use easily identifiable information, like e-mail addresses or phone numbers, instead of bank details.

Most proxy payment systems also include a payee validation as they return the payee’s name partially masked and display it to the payer to confirm the payee before sending the payment. Proxy payments, however, are no panacea. Proxy services require both payer and payee to be registered to the service before the benefits can be reaped. Users must provide information about both their account details and the proxy they will use. While this closed system reduces privacy concerns, it also serves as an inhibitor to adoption. Additionally, certain demographics are less likely to link their mobile phone number to an account, and most proxy services have so far not been very successful in enrolling business customers (see Figure 1).

We must acknowledge that proxy payments are only well suited for a limited list of use cases and will not solve the overall

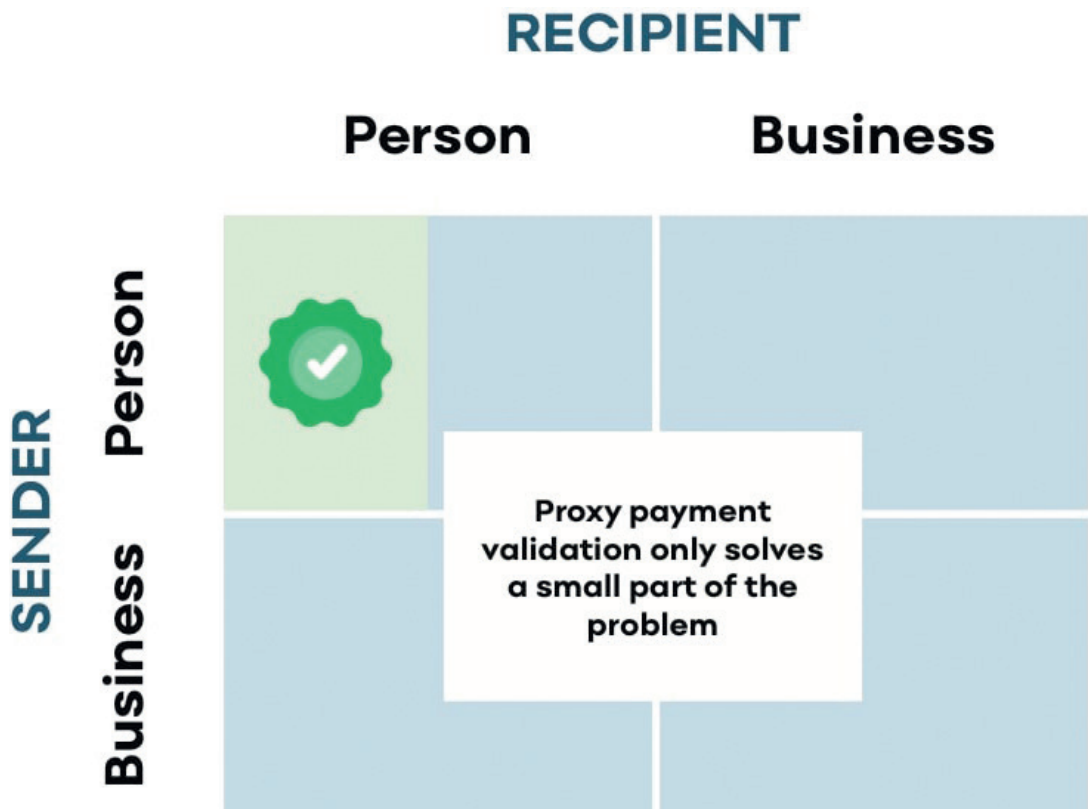


Figure 1: Proxy addressing is largely restricted to P2P payments

payee validation problem associated with credit transfers.

Many countries have therefore implemented an additional feature to pre-validate the account name prior to initiating a transaction.

The pre-validation can be as simple as returning the name of the recipient account as per the beneficiary's bank records. The name-check is done by the customer at the point of initiation within the banking channel. Most countries in Asia follow this validation method, and countries in the Middle East and Africa are also implementing similar approaches.

Because of data privacy concerns, many western countries fell short of implementing account validation as part of the payment process. Rising fraud cases led the UK and the Netherlands to innovate and introduce the concept of 'confirmation of payee'. Instead of simply returning the recipient's name, CoP involves a 'match score' between the recipient name volunteered by the payer, and the actual recipient name as per the banking records. Depending on the match score, customers will be warned that there is a mismatch in the names. Such systems do not provide binary yes/no answers, as they also include a scenario of close match, where the actual recipient's name will be suggested to the payer.

Other countries have opted to return a partially masked name in order to inform the sender of the identity of the recipient, while not displaying the full name for data-privacy reasons. The payee validation issue is compounded in cross-border transactions due to varying banking practices, different languages and regulatory norms in different countries. Given these complexities, making international payments can be a daunting task for many consumers. The lack of standardised verification methods across border exacerbates this user experience issue.

As digital transactions continue to grow and become more globally intertwined, the

need for efficient and secure payee validation mechanisms cannot be overstated. Robust payee validation not only improves customer trust but is also crucial for minimising fraud, enhancing operational efficiency and improving the overall payment experience.

THE REVISED RULES IN THE EU PAYMENTS FRAMEWORK TO IMPROVE CUSTOMER PROTECTION

A superior payment experience is characterised by four key attributes: simplicity, security, speed and affordability (Figure 2). In October 2022, the European Commission proposed an update to the Instant Payment Regulation to enhance three of these attributes by improving security, speed and affordability of euro payments.

The Commission's key objective of the proposal is to remove the barriers that prevent instant payments and their benefits from becoming more widespread. The idea is to achieve this by making instant payments in Europe available at no extra costs, secure and processed without hindrance across the EU.

The payment service provider (PSP) of the payee will be required, at the request of the PSP of the payer, to verify whether the IBAN and the name of the payee as provided by the payer match.⁵ The PSP of the payer will be obliged to notify the payer of any discrepancy before the payer finalises the payment order. Once notified of any discrepancy, the payer is then free to decide whether or not to authorise the credit transfer.

FOUR CONSIDERATIONS FOR ENSURING THE SUCCESS OF COP IN EUROPE

The challenge of consumer protection has been acknowledged. Now, with regulators on board, Europe is poised to take action. For many European countries, this entails






Superior payment experience	Update to instant payment regulation	Focus of this paper
 Simplicity		
 Security	Iban-name check	 Iban-name check
 Speed	Instant payments must be offered if regular transfers are	
 Affordability	instant payments should not be more expensive than regular transfers	

Figure 2: Superior payment experience, regulation update and focus of this paper

the establishment of a new infrastructure for IBAN–name verification, given the absence of existing CoP solutions.

Before exploring the optimal CoP approach for Europe, we provide four guiding principles for those aiming to develop a CoP system or strategy.

Conviction 1: CoP alone will not eradicate APP fraud

While CoP effectively curtails misdirected payments stemming from invoice–fraud schemes; its efficacy diminishes in scenarios where fraudsters can convincingly present accurate names or rationalise name discrepancies.

For a holistic approach to APP fraud mitigation, the integration of supplementary fraud prevention measures is imperative. Financial institutions are advancing their protective mechanisms by incorporating tools like behavioural analytics, risk assessment and machine learning (ML):

- *Behavioural analytics*: Tracking user behaviour can help identify instances where customers have been coerced by fraudsters during the creation of a new payee, for example, unusual time spent during the process or being on the phone with a fraudster are indicative factors;
- *Risk scoring*: Evaluating the risk associated

with a customer and transaction based on various factors, including the customer’s history with the bank and the type of account used, can enhance fraud detection;

- *ML*: Utilising machine-learning algorithms allows for the identification of suspicious activity patterns in both inbound and outbound payments.

Implications 1: Consider CoP as a first step in a larger trend of payment risk context

Banks have significantly advanced their use of behavioural analytics, risk assessment and artificial intelligence. However, there remains an information gap concerning the details available from the counterparty bank during transactions. It is helpful to perceive a CoP scheme as an information-sharing platform, underscoring the importance of contemplating the inclusion of enriched fraud indicators in the data exchange. In the process of payee validation, banks could share both customer and transaction risk evaluations.

Payment market infrastructures are the logical operators of CoP solutions, and they are in a unique position to leverage the transactional data to build real-time risk scores per IBAN. The account risk score can be based at first on simple metrics such

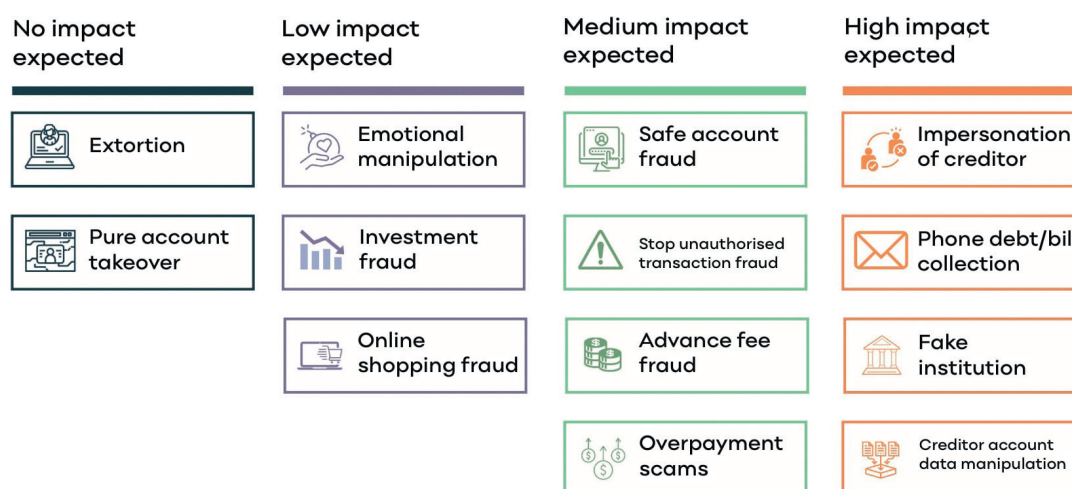


Figure 3: Potential impact of CoP based on relevant EBA fraud taxonomy

Source: Oesterreichische Nationalbank, Deutsche Bundesbank, the Euro Banking Association and PwC strategy& (2023) 'IBAN-name check: current developments and concepts', white paper, available at: https://www.oenb.at/dam/jcr:d627429d-a38a-4308-979b-f33cca34bcee/202306_Whitepaper-IBAN-name-check.pdf (accessed 8th November, 2023)

as transaction velocity, transaction amounts and first/last transaction date. Eventually, AI can come into play with a feedback loop from banks on actual accounts involved in fraud cases.

Further, collaborations with third parties, such as databases flagging suspicious entities and telecommunications providers, could provide insights into whether customers are engaged in simultaneous phone calls during transactions, offering an augmented security layer.

By embracing a holistic strategy that integrates broader information channels, CoP schemes can be fortified to counter emerging fraud methodologies, bolstering the overall security framework.

Conviction 2: Name verification enhances client confidence

Ever experienced unease when setting up a new payee, questioning if your funds will indeed land in the intended account? While payment missteps are frustrating, transferring funds to an incorrect account amplifies that concern. Although banks have the capability

to detect typographical errors through IBAN checksum protocols, the real value-add in the client experience comes from highlighting recipient name inconsistencies or showcasing a verification checkmark next to the legitimate account holder's name. Imagine the assurance provided when confronted with slight name deviations, the system prompts, 'Did you intend to select?' while displaying the account holder's name for validation (Figure 4).

European CoP implementations have showcased that it is feasible to address these privacy hurdles. Three features worth noting are: (1) displaying the name if the recipient account pertains to a business entity (this is typically permissible as numerous jurisdictions consider this to be public data); (2) for accounts owned by individuals, limiting the display of the name to cases where the payer's input closely aligns or exactly matches the legitimate account owner's details, on the basis that such a degree of matching servers as a testament to the payer's awareness of the beneficiary's identity; and (3) displaying a partially masked name

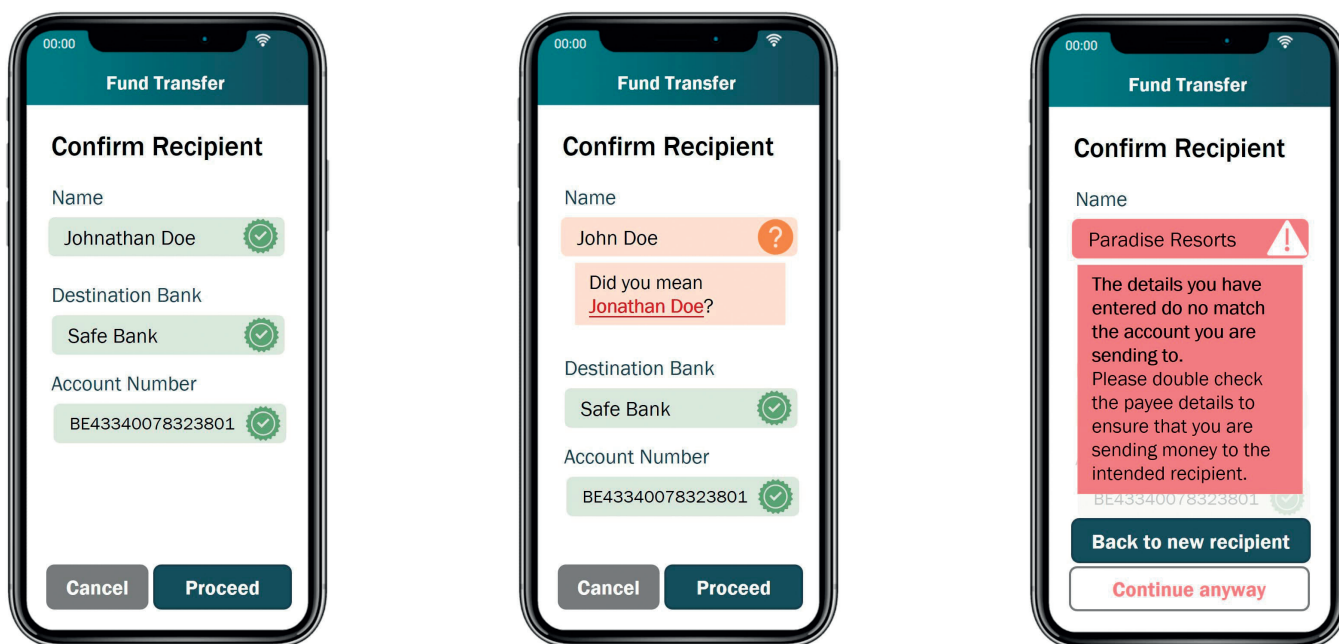


Figure 4: Examples of CoP user experience

In summary, with careful adherence to the outlined guidelines, General Data Protection Regulation constraints and name recommendations can coexist harmoniously. Certain nations might express apprehensions towards CoP owing to their banking confidentiality laws. However, the European Commission's draft regulation encompasses a compelling assertion, paving the way for clarity.

Conviction 3: CoP is about the bank account endpoint, not about the payment rails

There is an array of methods for executing euro credit transfers, each leveraging distinct payment infrastructures. These range from bulk to instant, low to high value, and national to international transactions. Even within the realm of instantaneous European transactions, various infrastructures come into play. Pan-European banks may also undertake intra-group transfers as ledger transactions within their proprietary networks. While it is rational for every payment infrastructure provider to envisage a bespoke

CoP solution to enhance client engagement and align with regulations, this could lead to a segmented user experience due to disparate CoP structures. Furthermore, banks could face increased expenses by integrating with a plethora of CoP systems.

Implications 3: Envisioning CoP beyond the confines of your payment infrastructure

We believe that payment systems are well suited to operate CoP solutions due to their expertise in managing other overlay services. In this regard, we encourage payment systems that choose to develop a CoP solution to treat it as a distinct and standalone service, separate from their existing payment rails. This entails establishing a clear distinction between the technical integration of the CoP solution and the integration with the payment infrastructure itself.

Moreover, we emphasise the importance of oneness and re-usability. For instance, when a bank is connected to a CoP solution operated by a local automated clearinghouse,

this solution should be permitted for use in verifying inbound payments from other countries, regardless of the clearing system involved, such as TIPS, RT1, T2 or any other applicable system.

Conviction 4: A single CoP solution is probably unrealistic

Although an all-encompassing European CoP system that transcends individual payment infrastructures stands as the ideal framework, its realisation appears challenging. Europe’s diverse perspectives on data privacy and nuanced regional payment experiences highlight the intricacies involved.

Aligning with the principle of subsidiarity well known to European institutions, local and regional payment market infrastructures should be empowered to design CoP solutions that align with their preferences.

Implications 4: Create an interoperable CoP framework

In light of the elusive unified European CoP, fostering cross-border interoperability

becomes paramount. In this vein, we welcome the European Payments Council (EPC) initiative to define a European CoP scheme.

THE IDEAL BLUEPRINT FOR COP SOLUTIONS IN EUROPE

Upon comprehensively examining Europe’s CoP terrain, we identify three scenarios of how the future of CoP may play out in Europe (Figure 6).

Assuming that there will be multiple CoP designs in Europe, and a need for interoperability, we share five recommendations.

Leverage central hubs to enhance operational streamlining and uniformity

Reflecting upon the UK’s approach, a wholly decentralised design proves detrimental both in terms of cost-effectiveness and consistent user experiences.

In the UK, the CoP framework integrates closely with open banking directives, with

	One Single CoP solution	Many designs but some common principles	Many designs and no common principles
Will it happen?	Unlikely	Likely & preferred	Possible
Risk	Follows lowest denominator principle	Need for interconnectivity solution	Inability to connect to some CoP schemes
Opportunity	One integration for all payments	Aligns with local preferences & allows interoperability	/

Figure 6: Potential scenarios of CoP in Europe

banks offering open banking APIs. While PayUK establishes the guidelines, the system lacks a centralised connectivity hub and a unified matching mechanism.

With respect to cost and consistency challenges, without a centralised nexus, banks resort to establishing multiple individual connections. Even as third-party service providers propose aggregation solutions, these escalate complexity and financial burdens; issues which a central switch could bypass.

The unique requirement of a matching algorithm demarcates CoP from open banking. Despite PayUK's directive, inconsistencies emerge as individual providers utilise distinct algorithms. As a result, customer experiences differ based on their bank or service provider.

We propose a hub-and-spoke model (Figure 7) where hubs consist of microservices, including:

- *Routing/switching service*: Channelising participant requests and feedback;
- *Matching service*: Determining matching scores; and
- *Interoperability service*: Facilitating connectivity in alignment with EU directives.

Additionally, hubs can augment services by synergising with external data sources like payment system transactional data, telecom firms, fraud records and business registries.

Decouple scheme rules from the payment rails for enhanced adaptability and interoperability

Within the hub-and-spoke paradigm, every regional CoP solution has its own design and scheme rules. Interoperability will be essential to meet the Regulation requirement. To that effect, the scheme rules should be payment rail agnostic with participants/

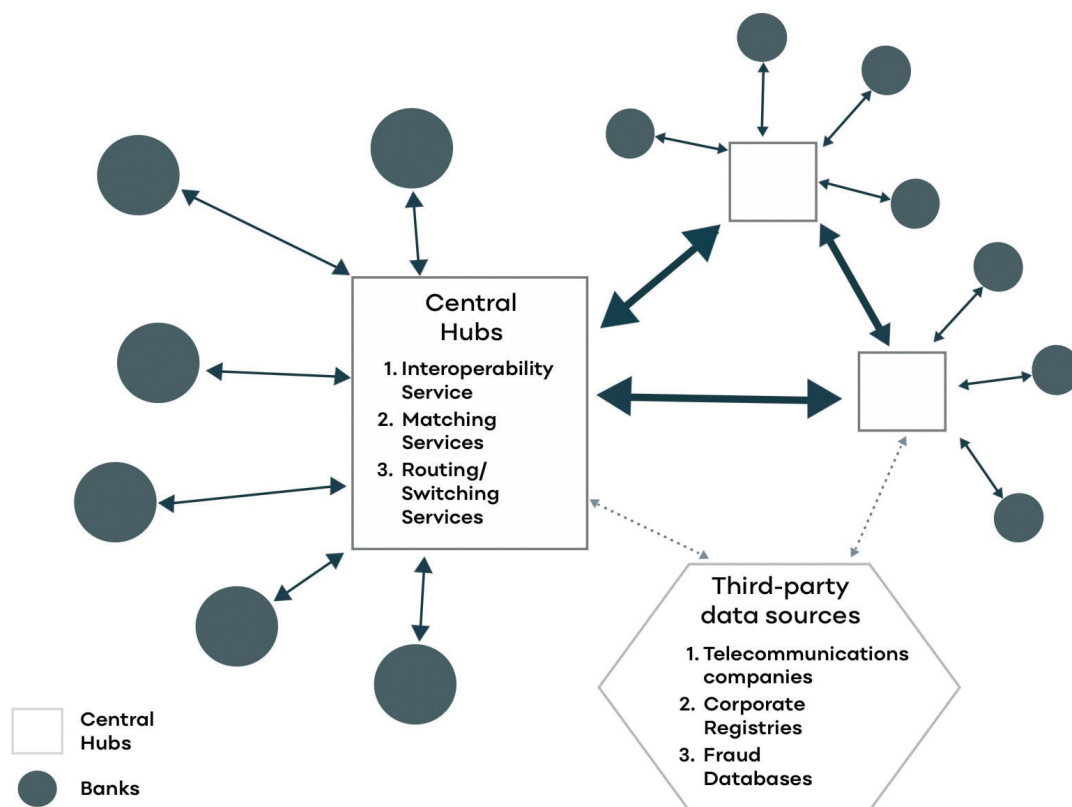


Figure 7: Hub-and-spoke model

hubs to expose the service domestically and internationally to third parties with the appropriate safeguards against data phishing.

Further, to make cross-border integrations easier, we commend the EPC's initiative in delineating a European CoP standard as a foundation for diverse solutions, ensuring pan-European compatibility (Figure 8). This should highlight the fundamental datasets required to meet the EU directive requirements and enable interoperability. Beyond fundamental data, these standards could specify matching algorithm criteria, beyond character set comparisons. The EPC could also provide a scheme template that local payment system operators can reuse and adapt.

Prioritise bank's implementation ease

CoP should transcend its image as a mere regulatory compliance checkbox. Banks ought to recognise its potential in fortifying customer protection and amplifying user experiences, even as a potential revenue stream for business clients.

The design's financial implications will determine banks' stance on CoP. Through judicious design principles:

- *For data requestor*: Assimilation can be streamlined to a unified API model;
- *For data responder*: Banks can direct account responses to the central hub, which acts as

a security buffer, centralising connection and matching efforts. Pre-configured nodes provided by CoP infrastructure entities can further smoothen bank integrations.

For optimal efficiency, the central hubs should champion interoperability, negating the need for banks to forge individual connections with other European banks and CoP models.

Clearly articulate the advantages and goals of CoP

It is pivotal to underscore CoP's specific function in bridging the gap in credit transfer processes rather than portraying it as a panacea for APP fraud. A prevailing misconception among consumers is the belief that banks consistently verify recipient names prior to processing payments. This leads to queries about the rationale behind inputting beneficiary names if they are not subjected to verification. Contrarily, most beneficiary banks do not routinely cross-check names on inbound payments.

Mandating beneficiary banks to confirm recipient names post-initiation of a transaction would be both financially and operationally burdensome. CoP instead entrusts the payer with the duty of verifying the payee's name before commencing the transaction, optimising the process. Feedback

Baseline of mandatory elements	Non-exhaustive list of optional data objects	EPC recommended
<ul style="list-style-type: none"> ○ IBAN ○ BIC ○ Recipient Name ○ Matching Result 	<ul style="list-style-type: none"> ○ Account holder name ○ Business/individual ○ Account status ○ Match score and algorithm used 	<ul style="list-style-type: none"> ○ Definition of what the EPC would recommend as a rich European CoP scheme

Figure 8: Potential building blocks of a European CoP scheme

from countries that have instituted CoP or analogous solutions underscores its capacity to foster consumer trust.

The underlying *raison d'être* of CoP lies in the enhancement of consumer confidence during transactions. In this regard, the inclusion of name suggestions for partial matches and business accounts becomes a crucial feature for effectively establishing trust with customers. By implementing CoP and effectively communicating its purpose, banks can not only bridge the existing gap in credit transfers but also strengthen customer trust and bolster overall transaction security.

Recognise CoP's global relevance

Issues of fraud, payment failures and evolving customer expectations are not confined to the EU's boundaries. Ensuring the safety of transactions beyond the eurozone becomes especially paramount for a number of reasons:

- Once intra-EU payments are made safer thanks to the mandatory IBAN–name check, fraudsters will move to the next-most-easy approach: non-EU payments;
- There is a higher risk of errors; many non-EU countries use complicated banking details, which might be alien to European customers as they diverge from the standardised IBAN format;
- The process to return a non-EU payment is complex and costly; reversing a payment involving multiple intermediaries, jurisdictions, regulators and currencies is far more intricate and expensive than reversing a SEPA transaction;
- The lucrative nature of cross-border payments incentivises financial institutions to provide premium offerings;
- Extra-EU commerce holds substantial weight for the majority of European nations. Barring Luxembourg, Czech Republic and Slovakia, all EU nations engage in more than 20 per cent of their trade with non-EU counterparts.⁶

European CoP solutions ought to champion global interoperability, either through their central hubs or individual participant connections.

THE WAY FORWARD

We strongly believe that European consumers will experience significant benefits from the CoP requirement, similar to the advantages of instant payments at the same cost as other credit transfers in euro, as outlined in the Proposal of European Regulation.

While the potential is vast, the complexities cannot be understated. Whereas the infrastructure for instant payments is already in place, CoP solutions remains to be developed in most countries.

Owing to their expansive reach, both TIPS (ECB) and RT1 (EBA Clearing) are strategically positioned to be part of the solution, particularly if crafted to be payment rail-agnostic. Nonetheless, it is unlikely that they will act as the single European solutions.

Following the principle of subsidiarity, local automated clearinghouses will also play a pivotal role in developing local solutions and enabling interoperability. The EPC can play a significant role in defining a multi-layered European CoP scheme that facilitates interoperability without compromising on effectiveness.

The new trends in the huge cross-border payment market offer opportunities along the length of the value chain, which will eventually include new partnerships and acquisitions strategies that will facilitate the creation of new infrastructures on a global scale. New solutions integrated into the technology platform will allow an end consumer with a bank account to track a payment until it reaches the beneficiary and to check details in advance. These partnerships will accelerate time-to-market, reduce costs and provide access to one of the most modern money transfer technologies.

Finally, when well designed, CoP should not be seen as a loss-making project by banks. Their business customers are willing to pay for account verification services, especially when integrated as an application programming within their back-office applications. This revenue stream, combined with a higher customer satisfaction for retail users, a reduction in misdirected payments and a reduction in fraud cases will make a positive business case for each financial institution and the industry overall.

REFERENCES

- (1) European Central Bank (2023) 'Confirmation of Payee (CoP) initiative', available at: https://www.ecb.europa.eu/paym/target/tips/profuse/shared/pdf/tipsmeetdoc/ecb.tipsmeetdoc230705_Confirmation-of-Payee-initiative_TIPSConsultativeGroup.en.pdf (accessed 3rd November, 2023).
- (2) ACI Worldwide (2023) 'It's prime time for real-time 2023', available at: <https://insiderealtime.aciworldwide.com/prime-time-report-23> (accessed 10th October, 2023).
- (3) ACI Worldwide (2023) 'Growth in APP scams expected to double by 2026 — Report by ACI Worldwide and GlobalData', available at: <https://investor.aciworldwide.com/news-releases/news-release-details/growth-app-scams-expected-double-2026-report-aci-worldwide-and> (accessed 10th October, 2023).
- (4) UK Finance (2023) 'Over 1.2 billion stolen through fraud in 2022, with nearly 80 per cent of app fraud cases starting online', available at: <https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app> (accessed 10th October, 2023).
- (5) strategy& (2023) 'IBAN-name check', available at: <https://www.strategyand.pwc.com/de/en/industries/financial-services/iban-name-check.html> (accessed 1st September, 2023).
- (6) euro stat (2022) 'Highest ever EU trade deficit recorded in 2022', available at: <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20230331-1> (accessed 1st September, 2023).

Copyright of Journal of Payments Strategy & Systems is the property of Henry Stewart Publications LLP and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.