UK Confirmation of Payee:
Mandate, Details and Challenges

March 2023

Authored by: Atmaram Parameshwara,
Synechron Payments practice, Bangalore, India

Table of Contents

1. Confirmation of Payee in the UK

The UK payments industry is at the forefront of innovation and best practices, be it for Open Banking or Real-time payments. Of the many standards and innovations being created in the UK's payments landscape, **Confirmation of Payee (CoP)** is one of the overlay services defined by Pay.UK

1.1. About Pay.UK

Pay.UK runs the UK's retail payments operations, which includes the BACS Payment System[1], the Faster Payment System[2], CHAPS[3], and the Image Clearing System[4]. They also deliver a variety of services relating to payments, such as the Current Account Switch Service, Confirmation of Payee and Request to Pay.

Through its infrastructure and services, Pay.UK enables billions of pounds in payments to be made safely and securely every single day. At the same time, it is creating common standards for the industry and working to modernize the UK's national payments infrastructure through the New Payments Architecture program and multiple overlay services.

Confirmation of Payee is one such initiative mandated by Pay.UK.

1.2. About Confirmation of Payee (CoP)

Confirmation of Payee allows payers to check the details of who they are paying before they confirm the transaction. It was launched in 2020 and has now been successfully implemented by a number of UK banks, building societies, and other payment service providers (PSPs). The aim of the service is to reduce certain types of fraud, like the Authorized Push Payment (APP) scam as well as prevent misdirected payments.

Before the introduction of CoP, a payer would provide their Payment Service Provider with all of the payee's details, including their bank sort code and account number, together with the name of the person or organization they intended to pay. The sort code and account number were then used to route the payment in accordance with the instructions given. However, there was no facility for the payer to check and confirm the name of the account holder before the payment was sent.

Authorized Push Payment (APP) scams occur when a person or business is tricked into sending money to a fraudster posing as a genuine payee. These types of scams can have a devastating impact on the people who fall victims to them. According to research conducted by the banking industry organization UK Finance, the amount lost to APP fraud is as follows:

Losses Due to Authorized Push Payment Scams

2018	£354.3 million
2019	£456 million (a 29% increase from the previous year)
2020	£479 million (a 5% increase from the previous year)
2021	£583.2 million (a 21.7% increase from the previous year)
	The latest figures show that £249.1 million was lost to APP scams in the first half of 2022.

Confirmation of Payee provides payers with greater assurance that their payments are being routed to the intended recipient and, therefore, are not being accidentally or deliberately misdirected.

In particular, it addresses certain types of Authorized Push Payment fraud by providing a platform for Payment Service Providers (PSPs) to give effective warnings to payers about the risks associated with proceeding with a payment to an account where the name does not match.

Greater adoption of Confirmation of Payee will likely reduce the overall Authorized Push Payment scams in years to come.

Also, CoP has been mandated for all UK banks and payment service providers that offer Faster Payments, BACS and CHAPS payment services. This means that all major banks in the UK are required to implement CoP and other financial institutions that offer payment services to their customers.

2. How Confirmation of Payee Works

CoP operates by verifying the recipient's information against the data stored by their financial institution:

→ When a payer initiates a payment, they are prompted to enter the recipient's name, account number, and sort code.

→ This information is then transmitted to the recipient's financial institution, which verifies the details against its records.

→ If the information is a match, the financial institution confirms that the payment can proceed.

→ If the information does not match, the financial institution will notify the payer that it cannot authenticate the recipient's identity and that they should verify the details before proceeding with the payment.

There are four possible outcomes for a Confirmation of Payee request:

Yes – If the customer has used the correct account name, the customer will receive confirmation that the details match, and can proceed with the payment.

Close match – If the customer has used a similar name to the account holder, that customer will be provided with the actual name of the account holder to check. They can update the details and try again or contact the intended recipient to check the details.

No match – If the customer has entered the wrong name for the account holder, they will be told that the details do not match and they will be advised to contact the person or organization they are trying to pay.

Unavailable – This occurs when it is not possible to check the name due to technical issues, for example, as a result of a timeout, customer opt-out, or if the account doesn't exist.

3. Other Use Cases of Confirmation of Payee

The Confirmation of Payee is not limited to the prevention of fraud between payers and payees. Apart from the banking industry, CoP can also be used in other industries or sectors where there is a need for verification of recipient details before making payments. It has many other use cases, including:

- **CoP could be used by online retailers or e-commerce platforms** to verify the identity of their sellers before processing payments.

- **CoP can also be used in any organization that processes payments**, such as charities or non-profits. Essentially, any organization that processes payments electronically and wants to ensure that payments are made to the correct recipient can benefit from using CoP.

- **CoP could be used by all financial institutions** to verify the name of the recipient of an international payment, which could help reduce the risk of errors or fraud in cross-border transactions.

- **CoP could be used by insurance companies** to verify the name of the policyholder or beneficiary before making payments, which could help reduce the risk of fraudulent claims.

- **CoP could be used by healthcare providers** to verify the name of the patient and reduce the risk of fraud in medical billing and claims processing.

- **CoP could be used by educational institutions** to verify the name of the student and reduce the risk of errors or fraud in tuition payments and financial aid disbursements.

There can be many more use cases where Confirmation of Payee can be used effectively across industries.

4. What Confirmation of Payee Means for Consumers and Financial Institutions:

Confirmation of Payee provides consumers with an additional layer of security when making payments. By verifying the identity of the recipient, consumers can have confidence that they are sending their money to the intended recipient and not to a fraudster. This can give consumers peace of mind and help to reduce the risk of financial loss.

For financial institutions, implementing CoP requires changes to their existing payment systems. They will need to update their systems to support CoP and train their staff on how to use it. Financial institutions will also need to ensure their systems are able to communicate with each other to check the recipient's details (typically using Open Banking directory services). Although implementing CoP requires an initial technical setup, the benefits of reduced fraud and increased customer confidence would likely outweigh these costs.

5. Components Involved in CoP

UK's Open Banking and Pay.UK have partnered to provide and manage the CoP service as part of the Open Banking Directory. All participants of CoP need to onboard the Open Banking directory.

CoP implementation requires every financial institution to build CoP requester and responder modules.

The CoP requester needs to build new APIs to furnish the required details, like username, account number, and sort code, which would be needed to match the intended recipient's identity.

The CoP responder holds user data and will implement matching logic to match the username with the account number with the information sent by the CoP requester and respond back.

CoP implementation includes the below steps/implementations:

Common implementation/steps to be done/followed by both CoP requester and responder:

- Onboarding to Pay.UK

- Onboarding to Open Banking (to use Open Banking directory)

- Securing the CoP solution to avoid misuse

- Providing channels to raise issues and the steps to resolve them

- Hosting of the secure solution to interact with the requester and responder

- Authentication and Authorization solutions to validate the requester and responder

As a Requester:

- Implementation of requester APIs as defined by the regulators

- Implementation of Dynamic Client Registration to register responders before invoking APIs

- Caching data of responders and other details to reduce calls to the Open Banking Directory

- Modifying all of the channels where customers make payment to display CoP result

CoP Requester Model
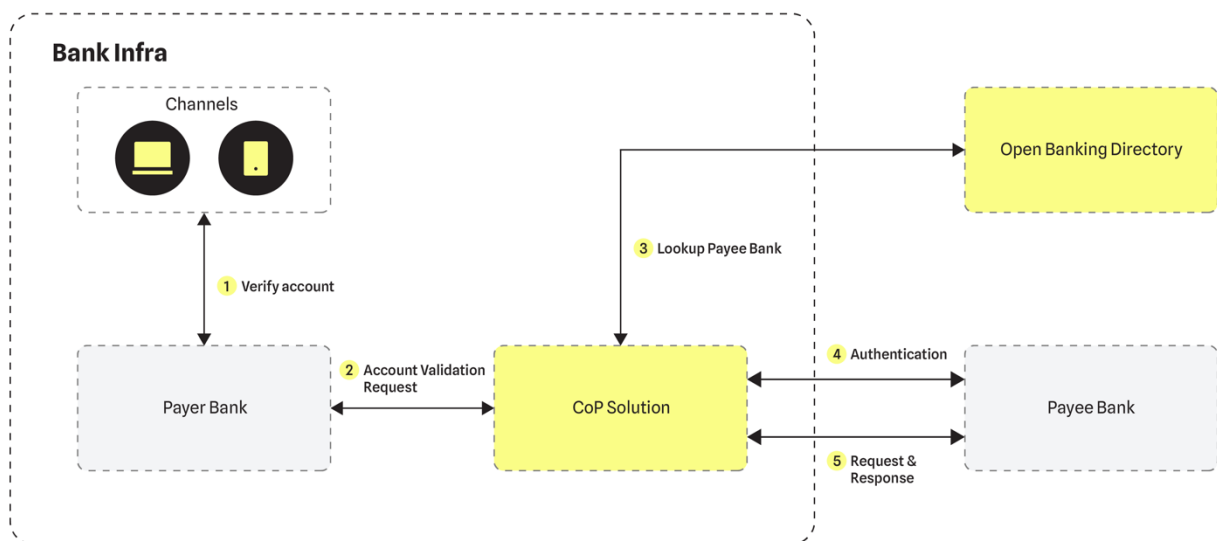
As a Responder,

- Upload the data to regulators (example: Sort code list) which will identify them as a CoP responder

- Implementation of a Dynamic Client Registration module to validate the requester before providing data

- Implementation of the Matching rule engine

- Providing an option to opt-out and the decision-making around each opt-out

- Reporting module and providing regular reports to the regulators

CoP Responder Model
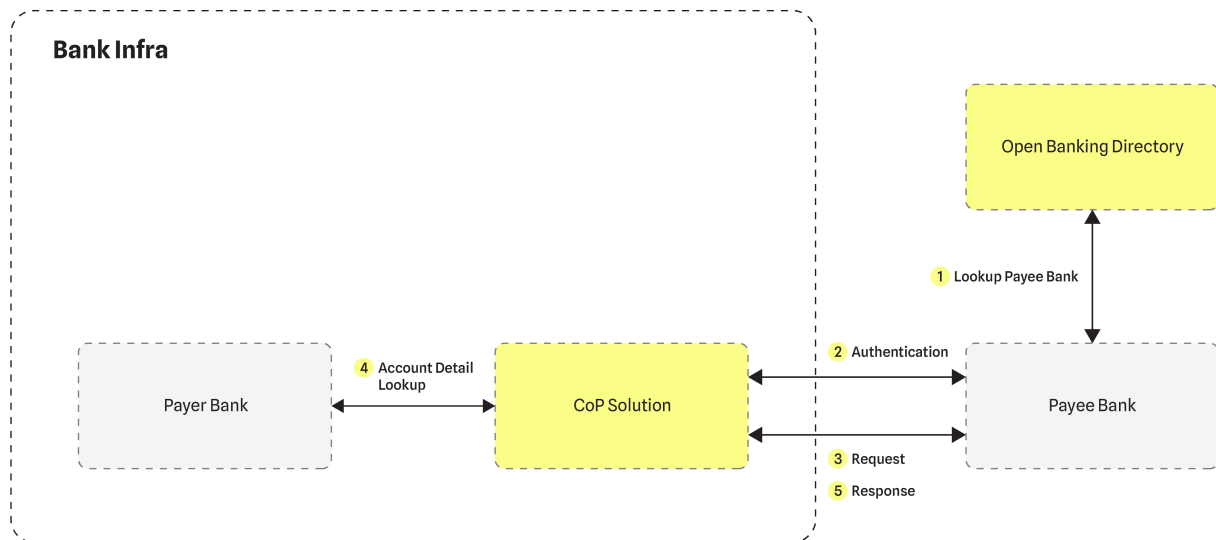
CoP requesters use the Open Banking directory to find the CoP responders using the sort code provided. The Open Banking directory provides a secure environment for both CoP requester and responders to trust and share data between each other.

CoP responders have customer data and have to respond whether the payee account number and name matches. If the CoP responder matches incorrectly the payee account number and name, the payer completes the transaction, which ends up in the wrong recipient, and the CoP responder is liable.

The expectation from the CoP responders is a balancing act of maximizing the positive matches along with making sure that they are not liable for false transfers.

6. Challenges to Consider

- **Technical Integration --** Integrating CoP into existing payment systems can be a complex and time-consuming process. Financial institutions need to update all their systems and channels involved in transactions between the payer and payee.

- **Data Accuracy --** If the recipient's financial institution has incorrect information, then CoP will not be able to verify their identity, which could result in a payment being made to the wrong person. Financial institutions need to ensure that they have accurate and up-to-date information on all of their customers to ensure that CoP works effectively. The CoP responder is liable if they provide incorrect information that results in transferring money to the wrong person.

- **Data Privacy --** When a payment is initiated, the payer's financial institution needs to share the recipient's details with the recipient's financial institution. This raises concerns about data privacy and the protection of sensitive information. Financial institutions need to ensure that they have appropriate security measures in place to protect the privacy of their customers' data.

- **Cost --** Implementing CoP requires financial institutions to invest in new technology and train their staff

on how to use it. This can be a significant cost, particularly for smaller financial institutions. Financial institutions need to weigh the benefits of CoP against the costs of implementation to determine whether it is a worthwhile investment.

6.1. Deep Dive Into Two Major Challenge

One of the important components of Confirmation of Payee is the matching rules. Pay.UK, as the Payment Systems Operator, has laid down a very basic set of rules and standards related to matching criteria. These matching rules are a set of high-level guidelines on how to match, but they do not provide comprehensive matching rules. It is up to each financial institution to build these matching rules as per their individual risk appetite. This results in not having a uniform standard for matching rules across the industry.

The other component -- which is complex and tedious to implement -- is connectivity to Open Banking and Dynamic client registration.

Open Banking connectivity is not simple. Financial institutions that have implemented it have spent thousands or even millions of pound sterling and taken a long time to implement it. Many have failed multiple times before getting it done properly.

6.2.Why Connectivity to Open Banking is Complex

To ensure a safe and secure ecosystem for financial operations, Open Banking has set strict requirements for its participants to connect to it.

Many financial institutions, whose main business is banking and offering its products, might not have the technical staff or manpower to spend on the implementation of complex Open Banking connectivity. Additionally, some financial institutions may lack the required infrastructure to implement such a complex solution.

Another complex implementation for every financial institution participating in CoP is Dynamic Client Registration (DCR).

6.2.1. Dynamic Client Registration (DCR)

New CoP responders are regularly added to the Open Banking directory, making manual client registration impractical. Dynamic Client Registration (DCR) enables clients to register themselves at runtime using a dynamic registration endpoint provided by the authorization server. The endpoint allows clients to provide information such as a client ID, client secret, redirect URIs, and other details required for authentication and authorization.

DCR provides several benefits, including simplifying the client registration process by enabling clients to register themselves without intervention from the authorization server, and reducing the potential for errors during registration. It also allows clients to obtain access tokens more quickly since they do not have to wait for the registration process to complete before making requests.

However, smaller financial entities who are required to implement Confirmation of Payee may find it difficult to implement due to the complexity of DCR and the lack of technical staff or infrastructure to support it.

7. Considerations/Resolution

To ensure a uniform standard for matching rules across the industry, the open-source community can be of extensive help.

The open-source community can develop the basic matching logic and publish it. Contributors from across the industry can help improve it. This would lead to a standardized algorithm that can be used by any CoP responder API across different industries.

However, it is important to consider that this open-source matching rule should be managed by an accredited organization within the financial institution to avoid misuse by malicious entities.

Regarding connectivity to Open Banking, it is the responsibility of the UK Open Banking regulator to provide a

simple way to integrate and implement the solution. One way to achieve this would be to provide an SDK or a simpler API layer on top of the existing Open Banking connectivity implementation. This way, it would not impact the existing implementers and would be easy for new joiners to adapt and connect to Open Banking.

Another solution to address both the uniform matching rules and the complexity around connectivity to Open Banking is through accredited non-banking third-party technical solution providers who provide this solution on behalf of multiple institutions. They can implement the entire solution and host it, eliminating the need for institutions to build solutions individually and providing a cost-effective solution with economies of scale.

Third-party technical solution providers have the technical capabilities and talented workforce to implement any complex, safe, and secure implementation mandated by Open Banking. They can also quickly respond to any new regulations and compliance changes. Being accredited with Open Banking and Pay.UK, they can be trusted to follow all the guidelines mandated by regulators.

At the time of writing this article, Pay.UK has not yet allowed non-banking third-party technical solution providers to provide and host solutions for Confirmation of Payee.

8. Conclusion

In conclusion, Confirmation of Payee is a valuable initiative by Pay.UK to reduce a certain type of fraud in the financial industry. It ensures peace of mind for payers when transferring money, knowing that it will reach the intended payee. The use cases are not limited to payments between payer and payee, and adoption and usage will likely increase not only in the UK but also in other countries worldwide. Similar to Open Banking, this feature will be adopted across the world in the future.

However, there are multiple challenges within the UK that prevent all participants from implementing the same. Two main challenges are the complex connectivity to Open Banking and the lack of an industry standard in matching logic.

The industry's expectation is to make an early decision on allowing accredited third-party technical service providers to host and run the CoP solution on behalf of multiple financial institutions. The industry also expects to reduce the complexity of open banking connectivity implementation. Doing this will benefit financial institutions to comply with CoP faster which, in turn, benefits end customers of these features. It also benefits regulators to push this compliance industry-wide in a shorter period.

As previously mentioned, the open-source community of the industry also has a responsibility to help in CoP adoption by providing a platform to define and improve matching logic, which serves to benefit all participants.

9. Contact Synechron to learn more:

Atmaram Parameshwara Atmaram.Parameshwara@synechron.com

_____

10. Appendices

10.1. Details

[1] Bankers' Automated Clearing System - an electronic system to make payments directly from one bank account to another. They're mainly used for Direct Debits and direct credits from organizations.

[2] Electronic payments that can be made online, over the phone, in a branch or using self-service machines. The payment will arrive almost immediately (though sometimes, it can take up to 2 hours).

[3] Clearing House Automated Payments System: used to settle high-value wholesale payments as well as

time-critical, lower-value payments like buying or paying a deposit on a property

[4] Digital images of cheques to be exchanged between banks and building societies across the UK for clearing and settlement.

10.2. Appendix A – Authors

The auther would like to thank **Aravind Irodi <aravind.irodi@synechron.com>; Sudeep Chakravarthy <Sudeep.Chakravarthy@synechron.com>; and Tuhinabhra Mahapatra** Tuhinabhra.Mahapatra@synechron.com for their contributions to this white paper publication.

10.3. Appendix B

10.3.1.1. All material, books, websites, research papers, and other resources, are listed by title, along with the name of the author, and publisher.

10.3.1.2. References
https://www.wearepay.uk/what-we-do/overlay-services/confirmation-of-payee/
https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/authorised-push-payment-scams-annual-figures

To reach the author of this Synechron White Paper, please contact:

Atmaram.Parameshwara@synechron.com