Payee Verification: Overview of Approaches used by Credit-Push Payment Systems

Interim Report

P20 Regulation Working Group

June 2020

INTRODUCTION

P20 is delighted to release this Interim Report, ***Payee Verification: Overview of Approaches used by Credit-Push Payment Systems***, which has been prepared by our Regulation Working Group. It examines the early approaches that are being used to reduce fraud in this growing method of payment. In 2021, the Regulation Working Group will release a final report on Payee Verification having had the opportunity to assess the early operation of Confirmation of Payee in the UK.

This analysis examines how confidence can be given to the Payer that the Payee is the bone fide intended recipient of their monies. It covers the two main check methodologies of Payee Institution Verification and Directory Verification. The former procedure is used in the UK, the latter in Australia and USA.

It is still early days in assessing which methodologies are more successful at fraud reduction. The recognition that financial systems comprised of limited number of banks holding the vast majority of accounts may benefit from one approach, where a market made up of a large number of banks holding fewer accounts will benefit from another. P20 considers this essential reading for all those who are in the battle against this type of fraud which has seen a significant increase during Covid-19.

G20 countries have pledged $7 trillion in fiscal support, of which $3.5 trillion is direct government spending. This is money which criminals are attempting to intercept through fraudulent methods, demonstrating the vital importance of payee verification.

The Regulation Working Group is now examining **Authorized Payment Fraud** and will be making best practice recommendations later in 2020. The initial specific issues are:

- Customer Warning Messages
- Criminal Account Targeting
- Mule Account Identification

EXECUTIVE SUMMARY

A key risk management element of a modern credit-push payment system, particularly with the growth in faster and real-time payments, is providing assurance to the payer that the payee is in fact who the payer intends to pay. This fraud prevention element is referred to here as "Payee Verification" and occurs to varying degrees and in different ways across countries and payment systems.

There are two main approaches to Payee Verification reviewed here:

(1) ***Payee Institution Verification*** by directly querying the potential receiving bank regarding the name of its customer (by sending the payee name given by the payer);

(2) ***Directory Verification*** by querying a common directory of payees against similar criteria.

In the different approaches, the payer provides the name or the alias of the potential payee, and receives in return some form of confirmation or actual information about the payee account holder. Payee institution verification is being rolled out for UK Faster Payments in the form of Confirmation of Payee, while directory verification is similarly being rolled out by the Australian NPP system in the form of PayID. In the U.S., the Zelle P2P payment system now provides directory verification of the payee and the rules of The Clearing House's real-time RTP system require presentment of the payee name in some form to a consumer payer, and permits directory verification for that purpose.

While both approaches – whether via payee institution or directory – can help payers avoid unintended payees (whether erroneous or fraudulently misidentified), the payee verification approaches being adopted do not address other forms of fraud such as authorized[1] payment fraud.

[1] For this paper, terms ending in "ize" in the U.S. and "ise" in the U.K. are spelled with "ize," e.g., authorized.

BACKGROUND ON PAYMENT SYSTEMS, FASTER PAYMENTS AND FRAUD

Payment systems are generally classified into two main types: "credit-push" and "debit-pull." In a credit-push system, the payer directs its bank to send a payment to the payee, and the payment is "pushed" or credited to the payee's account. Examples include bank wire systems, ACH credit, and most "faster payment" systems.[2] In a debit-pull system, the payee directs its bank to remove funds from the payer's account, and the payment is "pulled" or debited from the payer's account. Examples include standard card payments, ACH debits, and paper cheques/checks.

Fraud involving a payment is generally classified into two main types: "unauthorized" and "authorized" – in terms of whether the payer authorized the payment. The payee verification approaches under evaluation in this paper focus on authorized payments. An "unauthorized" payment is one where the payer did not authorize the payment made from the payer's account. As a result, an unauthorized payment itself is either erroneous or fraudulent. In contrast, an authorized payment is one where the payer authorized the payment. Fraud involving an authorized payment relates to the circumstance where the payer is fraudulently induced to make the payment. In this situation, the payment itself is not fraudulent.

In a credit-push system (including faster payment systems), one of the primary risks of fraud involves account takeover, or some other fraudulent access to an account resulting in an unauthorized payment. Once an account is taken over, the fraudster can push funds out of the account. Sending banks in credit-push systems focus fraud prevention efforts on authenticating the account holder, to ensure that payment accounts are accessed only by actual account holders or their authorized users. Liability for an unauthorized consumer payment typically lies with the sending bank, which incentivizes banks to

[2] The term "faster payment" refers to payments from systems that provide real-time or nearly real-time notification and settlement of payment (e.g., UK Faster Payments, Australian NPP, U.S. RTP and elsewhere), but also payments from systems with somewhat longer settlement, e.g., U.S. Same Day ACH or payments that rely on eventual ACH settlement. For this discussion, we will treat all faster payment systems as credit-push systems (notwithstanding Same Day ACH debits).

implement strong authentication controls and mechanisms to prevent the usage of mule accounts. While faster payment systems reduce the time available to block a fraudulent payment, they otherwise do not change the nature of the risks or prevention tools that can be adopted in a credit-push system.

In a debit-pull system, one of the primary risks of fraud involves a fraudulent payment instruction, where a defrauding payer offers a false payment account, e.g., a stolen credit card. While there is a risk of a defrauding payee presenting a fraudulent payment instruction, the vetting of payees helps to minimize this risk, e.g., mandate management for ACH debits. Debit-pull systems focus fraud prevention efforts on authenticating the presented payment instruction. For in-person and online commerce, where the purchaser is typically unknown to the seller, the debit-pull card schemes have a higher unauthorized loss rate than other payment systems, but offer a payment guarantee to payees, which is compensated by interchange fees.

Fraud involving an authorized payment occurs in both credit-push and debit-pull systems, since the payment itself is not the fraud, but rather the means to transfer funds once the fraudster has convinced the payer to make a payment. Liability for an authorized consumer payment also typically lies with the sending bank. This contrasts with the UK Contingency Reimbursement Mechanism which involves shared liability for authorized payment fraud. The principle of a payee's bank co-operating with the payer's bank in its efforts to recover funds paid in error, is also found in the Payment Services Directive 2017. This includes requiring the payee bank to provide the payer's bank with all relevant information for the collection of funds.

Fraud involving an authorized payment can be classified into two categories, based on whether defrauding payee misrepresents:

- **Who** they are, e.g., claiming to be a charity or a company CEO
- **What** goods, services or personal commitments they are to provide in return, e.g., selling an investment, or promising affection.

Only in the case of an authorized payment involving misrepresentation of who the payee is (and also for erroneous payments) does a mechanism of Payee Verification assist in reducing fraud.

PAYEE VERIFICATION – DEFINITION, RELEVANCE AND APPROACHES

Bank payment instructions rely on a bank identifier (sort code in the UK; bank routing number in the U.S.) and an account identifier (an account number in both the UK and U.S, International Bank Account Number (IBAN) in the EU); for cards, the Permanent Account Number (PAN) is both the bank and account identifier). Typically, the payer is only familiar with the name of a beneficiary, not the designated bank/account numbers. **"Payee Verification" refers to methods by which the payer can determine whether the name/alias of the intended payee, prior to initiation of a credit-push payment, matches the name of the beneficiary of the payment to whom the payer intends to make the payment**.[3]

A Payee Verification method for a credit-push payment system can be useful to help prevent a payer from sending an authorized payment:

- **In <u>error</u>**, i.e., entering the wrong payment instruction data; or
- **To a <u>payee who misrepresents who</u>** they are, i.e., payee provides name that does not reconcile to bank credentials;
- **<u>But not</u>** to an intended **<u>payee who misrepresents what</u>** they provide in return.

Please note:

1. A Payee Verification method helps reduce the chances of a payee being misidentified – whether by payer's error or payee's intentional misrepresentation – it does not reduce fraud related to an authorized payment.
2. Payee Verification is being introduced to reduce fraud in faster payment systems for several reasons:

[3] To be clear, no current Payee Verification method replaces the bank and account identifiers used by existing payment systems in the payment instruction.

a. lack of consumer awareness of more limited recourse options in newer faster payment countries;

b. relatively low rates of account takeover leading fraudsters to focus on authorized payments;

c. better bank monitoring of and increased reporting of fraud involving authorized payments.

There are two basic methods of Payee Verification prior to payment, one involving the payee institution and the other involving a common directory.

1. **Payee Institution Verification** In this method, prior to a payment, a query is made directly to the prospective payee's institution, which includes the payee account number and name; if successful, the payer is presented with confirmation that the name or alias provided matches that held by the payee bank or directory. The Confirmation of Payee service does not present the name except where the payer has achieved a close match i.e., did you mean Sarah Smith, when the name quoted is Sara Smyth? The service is an example of Payee Institution Verification (detailed below).

2. **Directory Verification** In this method, prior to making a payment, a query is made to a central directory, which includes a payee alias, name and/or other information, and a response is returned either confirming whether there is a match or providing a payee name. The PayID directory for the Australian New Payments Platform and the Zelle directory in the U.S. are examples of Directory Verification (detailed below).

CONFIRMATION OF PAYEE IN THE UK: EXAMPLE OF PAYEE INSTITUTION VERIFICATION

The UK Faster Payments system, which has been around for more than ten years, is introducing a method of payee verification. In late 2017, the UK Payment Systems

Regulator's (PSR) Payments Strategy Forum published the results of its consultation on the implementation of a New Payments Architecture for UK retail payments, which included proposals to improve the end user experience. Confirmation of Payee ("CoP") was one of these proposals.[4] Designed with the consumer in mind, CoP is expected to help provide greater assurance payers are sending payments to their intended recipient. The task to deliver CoP was passed to the new payment system operator, Pay.UK, to develop the proposition and the underlying standards. CoP went live in the UK in early 2020.

The CoP service is embedded into the payment process itself. In addition to the bank sort code and customer account number needed for a credit-push payment, CoP uses a third piece of payer-supplied information, the prospective payee name. The payer provides the payment instruction data, along with the intended payee's name. The payer's bank sends a message to the payee bank to request confirmation that the payee name given by its customer matches the account owner of the supplied sort code and account number. The payee bank replies, either confirming an exact match of the account holder, a near match or a non-match (the information is exchanged in a matter of seconds/fractions of a second).

Upon receipt of this information, and prior to sending the payment, the payer has additional information to determine whether to proceed with initiating the payment to the sort code and account number provided, or to make further checks before proceeding. If the name provided is erroneous, there will clearly not be a match of provided payee name to account holder. If a fraudster has misidentified themselves, there will also not be a match, or at least very likely not an exact one. Where the provided name is close to the account holder name, the payer will need to make a judgment call as to whether to proceed with the payment or not based on the available information. While the CoP service will not guarantee the elimination of all erroneous or fraudulent misidentified payees, it should reduce the number of erroneous and misidentified authorized payments. Implementation in the UK has been driven by regulatory and political expectations, the

[4] https://www.wearepay.uk/confirmation-of-payee/

consumer benefits will be assessed once CoP is rolled out and measured in implementation.

PayID FOR THE AUSTRALIAN NPP SYSTEM: EXAMPLE OF DIRECTORY VERIFICATION

Australia launched its faster payment scheme – the New Payments Platform (NPP) – in 2017. Shortly thereafter, the NPP scheme introduced "PayID" – which is both a simpler way for payers to identify the intended payee, and also a method of confirming the identity of the payee. In terms of Payee Verification, the NPP PayID addressing service takes a Directory Verification approach to validating payees.

The term PayID specifically refers to a unique identifier (or NPP alias) that each consumer account holder enrolling in PayID chooses, which counterparties can use to identify that account holder. The account holder signs up for PayID through its financial institution, and chooses a unique PayID from among several options, e.g., email address, mobile number, account number. Once the consumer selects the PayID they wish to connect to their account, their financial institution will verify the user's identity, as well as the authenticity of the relationship between the user and the account information provided. Upon successful verification of the account holder and their chosen PayID, the financial institution registers the PayID on the platform for use by all participating NPP banks.

Once a consumer's PayID is in place, they can provide their PayID to any paying counterparty. The payer populates the PayID field in the NPP payment instruction, which the sending institution delivers to NPP. The NPP system looks up the owner of the given PayID and presents the corresponding name to the payer. The payer then chooses whether to execute the payment, based on whether the displayed payee name aligns with the payer's expectations. This process can thereby reduce payments made to the wrong payee, whether due to error or misrepresentation of identity by the payee.

In addition to providing a verification of the Payee, Australia's PayID is also eliminating the need for a payer to provide the payee's bank and account data, replacing that with a more readily known alias. This serves to reduce numeric key stroke errors, as well as reducing friction in the payment system.

U.S. ZELLE DIRECTORY AND TCH RTP SYSTEM: DIRECTORY PAYEE VERIFICATION

In the U.S., there are several faster payment options. The Clearing House's RTP system, which is a 24/7 real-time bank account network, was introduced at the end of 2017 (about the same time as Australia's NPP system). The Zelle P2P payment system, which began in 2011 as a consortium of three banks and is now owned by Early Warning Services, has gained extensive acceptance and volume; it involves immediate notification but generally has deferred settlement. In terms, of payee verification, the discussion will focus on these two arrangements.[5]

The Clearing House's RTP system does not have a built-in mechanism for payee verification. RTP rules do require that a consumer (as opposed to commercial) payer must be presented the payee's name prior to the consumer sending a payment; RTP rules also permit directory verification for the purpose or presenting the payee's name. At present, there are some consumer-initiated payments for A2A payments, relying on directories developed by sending banks for use by their customers. The growth in RTP consumer-sent payments is expected to come from RTP being used to settle Zelle-initiated payments and the Zelle directory.

The U.S. Zelle system uses a directory for payments, which did not initially provide ongoing payee verification, but has been recently configured to do so via Directory Verification (akin to Australia's NPP). Deposit account owners signing up for Zelle provide

[5] In addition, the U.S. ACH batch payment networks instituted same day ACH, at first credit-push but now also debit-pull. The card networks also offer the ability to send a credit-push payment to a bank account via a debit card. There are also various fintech payment providers such as PayPal and Venmo, which provide P2P payments that generally settle on ACH rails.

an alias – either a mobile number or an email address – to associate to their deposit account for receiving Zelle (an alias can only be used for one account). Account owners can then receive Zelle payments sent using their alias, and can send payments to payees enrolled in Zelle, typically by way of a payee directory in their online or mobile bank account application. With the payee verification capability, when the deposit account holder adds a new payee to its payee directory, the account holder is presented with the common name of the intended recipient (typically the recipient's first name as listed in the Zelle directory. Thereafter, when sending a payment to that payee, the payer is presented with the name in their own payee directory (or the Zelle directory). When Zelle transactions settle on RTP, the payee's name will be presented to consumer or small business senders.

ASSESSING PAYEE VERIFICATION VIA PAYEE INSTITUTION VS. DIRECTORY

Early payee verification services favored the directory verification approach and examples include those operated by NPP in Australia, Zelle in the U.S. and PayM in the UK. Confirmation of Payee by the payee institution has been implemented in the UK for FPS under regulatory encouragement and due to the limited take-up of PayM. The Australian system has at least one identified drawback, which relates to the provision of the actual payee name associated with the alias being provided back to the payer. In contrast, the UK CoP service will not return the actual payee name, but rather will confirm the match to the account holder name with the name provided or provide information to assist a payer to make a decision regarding whether or not to initiate the payment where the name does not match.

The identified shortcoming of PayID is resolvable by responding not with the account holder name but rather with a confirmation of a match/close match, similar to the UK CoP solution. The directory approach has the added benefit of offering the option of an alias in lieu of payment instruction data. To provide payee confirmation, the alias and payee name would need to be provided to avoid the identified PayID issue.

As new payee verification services are still in early adoption phase, the industry will track their success in reducing the error and fraud type that they aim to mitigate. Lessons learned may help provide guidance on individual country approaches. Early findings suggest the adoption of Payee Verification for markets comprised of limited numbers of banks holding the vast majority of deposit accounts (e.g., UK), and a Directory approach for markets made up of larger numbers of banks, where the cultural norms of the region are better aligned with the use of an alias over another credentials (i.e., a Directory system using an alias to address the payment instruction rather than account number).

Regulatory conditions governing liability also need to be taken into consideration. In the US, the liability for misdirected payments, in general, lies with the sender; in some directory-based systems, the bank that enters their customer's credentials into the directory provides the warranty that the data are correct.

At the current time, in relation to the implementation of payee verification services, the sample is insufficient to evaluate the benefits as most countries are in the planning or early implementation phase nor provide any conclusive recommendation.

This paper will be reviewed in 2021 to reassess the findings from current and emerging services, and consider which solution, if any, performs better or is adopted more easily by customers, depending on the way they pay.

REFERENCES

CoP References:

https://www.wearepay.uk/wp-content/uploads/2019/10/Confirmation-of-Payee-brochure.pdf
https://www.wearepay.uk/confirmation-of-payee/#confirmation-of-payee-report
https://bank-code.net/uk-sort-code/608371-starling-bank-limited

PayID References:

https://payid.com.au/
https://nppa.com.au/payid/

FUTURE WORK

The Regulation Working Group is now examining Authorized Payment Fraud and in particular, the following issues:

Customer Warning Messages

Banks and remittance companies warn their customers to duly authenticate all new payees before initiating a first automated payment. However, these warnings on their internet and mobile channels vary considerably in their clarity between institutions. P20 believes a global standard should be adopted.

Criminal Account Targeting

In order to muddy the trail and lessen the likelihood of seizure, criminals immediately forward and disperse monies they receive through their fraudulently opened accounts across banks and borders. These payments usually happen within minutes of cleared funds being credited to the fraudulent account. While P20 does not advocate slowing down the payments system to allow more time to examine such transactions, P20 believes that more can be done as an industry to identify and stop these fraudulent payments.

Mule Account Identification

Many banks around the world are increasingly identifying mule accounts and closing them down, causing fraud and criminal activity to move to the weaker links in the banking system. P20 believes that more collaboration between regulated financial entities to identify accounts held by the same criminal gangs across multiple institutions will enable law enforcement agencies to act.

In 2021, the Regulation Working Group will release a final report on Payee Verification having had the opportunity to assess the early operation of Confirmation of Payee in the UK.