
FOCUS NOTE

# PROXY IDENTIFIERS AND DATABASES IN PAYMENTS

## Part of the World Bank Fast Payments Toolkit

SEPTEMBER 2021

WORLD BANK GROUP

# CONTENTS


1. SETTING THE CONTEXT 1
2. BACKGROUND 2
   - 2.1. Benefits of Proxy Identifiers 2
   - 2.2. Types of proxy identifiers 3
3. PROXY DATABASES 5
   - 3.1. Centralized Database 6
   - 3.2. Decentralized Database 6
4. EXAMPLE OF ALIASES USED IN FAST PAYMENTS 9
5. CONSIDERATIONS FOR DESIGNING A PROXY IDENTIFIER 13
6. CONCLUSION 15
7. ACKNOWLEDGMENTS 16

NOTES 17



**FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE**

*Payment Systems Development Group*




1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

# 1 SETTING THE CONTEXT

The World Bank has been monitoring closely the developments of fast payment systems (FPS) by central banks and private players across the globe.[1] This comprehensive study of FPS implementations has resulted in a policy toolkit. The toolkit was designed to guide countries and regions on the likely alternatives and models that could assist them in their policy and implementation choices when they embark on their FPS journeys. Work on the FPS Toolkit was supported by the Bill and Melinda Gates Foundation. The toolkit can be found at ***fastpayments.worldbank.org*** and consists of the following components:

1. The main report *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*
2. Case studies of countries that have already implemented fast payments
3. A set of short focus notes on specific technical topics related to fast payments

This note is part of the third component of the toolkit and aims to provide inputs on proxy databases from a payments perspective, with a focus on fast payments. This topic is of relevance as proxy identifiers or aliases have played a major role in enhancing the payment experience of end customers.

# 2 BACKGROUND

In payment transactions, to identify the receiver of a payment, the sender must know and input into the access channel from where the transaction is being initiated the beneficiary's information, such as the name of the payment service provider (PSP), the PSP identifier, the branch identifier, the transaction account number, and name. This requires the beneficiary to share sensitive information with the payer and the payer to input several data points into the access channel, which adds friction to the payment flow, as it is susceptible to error. In an in-person transaction, such as one carried out at merchants, the user experience can be hampered if the merchant's account information needs to be shared in full and if the payer needs to input different data points to complete a payment. In the context of an fast payments, the overall efficiency provided by these systems will be affected if the payer and payee need to complete several steps to instruct and receive a payment. QR codes seek to address this issue by removing the need to enter these details manually.

Proxy identifiers, or aliases, link the payer's or payee's transaction account information with a short identifier that is easy to remember, allowing the public and the business sector to transact in a seamless manner without needing to know and input the beneficiary's bank account details while initiating a payment or reading a QR code.

## 2.1 BENEFITS OF PROXY IDENTIFIERS

In an increasingly digital world, customers are interacting by using proxy identifiers/aliases to access electronic services provided by different industries, such as payment, social media, financial services, and government.[2] The simplicity associated with aliases has been a major driver for their widespread adoption, as a transaction account number is difficult to remember (10 digits long or longer) and inputting it into an access channel, such as a mobile device, during an in-person transaction adds friction to the payment flow. For the payee, using a proxy identifier removes the need to memorize an account number and other information associated with an account, so when requesting a payment, the payee can provide to the payer a simple identifier. Further, in the context of bulk payments such as transfers of government benefits and salaries, proxy identifiers simplify the maintenance of beneficiary information and keep the payer from having to make any changes if the beneficiary decides to receive the transfers into a different account. Proxy identifiers mask a transaction account number and hence help prevent the theft of transaction-account information, reverse lookup attacks, and the automated skimming of customer information.

**FIGURE 1** **Prominent Proxy Identifiers/Aliases Used for Initiating Payments**


*Source:* Own elaboration

## 2.2 TYPES OF PROXY IDENTIFIERS

A proxy, or alias, identifies recipients and their payment accounts using a simple unique alternative for payment services such as person-to-person (P2P) money transfers, merchant payments, cash deposits, and cash withdrawals. It protects their sensitive account information and makes sending payments more intuitive and in line with other means of social interactions.[3] Some of the common proxy identifiers have been listed in figure 1.

### 2.2.1 Mobile-Phone Number

A mobile-phone number is one of the most popular proxy identifiers/aliases because of its high accessibility among end customers. End customers are required to link their mobile numbers with financial institutions to use the numbers as proxies to their transaction account numbers. Due to the high penetration of mobile phones, they can facilitate broad participation of end customers in the payment system. Many countries, such as Australia, Bahrain, Chile, China, Europe, India, Kenya, Malaysia, Mexico, Singapore, and the United Kingdom, allow use of mobile numbers as proxy identifiers.

In developed economies, mobile numbers offer consistency as proxy identifiers, as customers generally use the same phone number for a long time. However, in developing economies, mobile-number turnover is relatively high, due to the prevalence of prepaid connections and a lack of telephone-number portability. Therefore, it is important for system participants to establish mechanisms to update their proxy databases in case customers change their mobile numbers. In Thailand, to ensure that the database is updated, telecom companies provide banks with updates on the termination of mobile numbers, changes in ownership, and number portability.[4] In the initial years, customers were unable to link their mobile numbers with PromptPay when the numbers were still tied to the PromptPay and banking accounts of the previous owners of the numbers. To resolve this issue, National Broadcasting and Telecommunications Commission, along with banks and telecom companies, launched a USSD service. New owners can use this service to obtain a reference code that can be used by the banks to verify the identity of new applicants.[5]

Additionally, the robustness of mobile phones as proxy identifiers can be underpinned by the physical mobile device through their International Mobile Equipment Identity number. Customer identity linked to the mobile number is also verifiable against databases, such as a national identity database. In countries where the sharing of mobile-phone numbers is prevalent, the privacy of confirmation text messages might be undermined when the mobile number is used as an alias. Also, in case of fraudulent access through a swapped SIM card, details about the underlying financial transaction would also be compromised.[6] According to GSMA, mobile-network operators need to adopt additional security measures to mitigate the fraudulent swapping of SIM cards. In the event of a SIM swap, the mobile-network operator can also indicate SIM swap requests or transactions that have been made to the PSPs. These PSPs can then take additional security measures and ask consumer to verify the SIM swap—for example, completing additional checks over a different channel.[7]

### 2.2.2 Email Address

Email addresses provide high user-friendliness to end customers, as an individual can open different email accounts using the same or different servers. A customer must register an email address with a financial institution, a government agency, and/or an online platform that facilitates payments. Additionally, PSPs might ask for additional information, such as the customer's address and mobile-phone number to ensure verifiability.

In developed economies, high internet penetration and high smartphone penetration facilitate the use of email addresses as proxy identifiers. Countries such as Australia

and Hong Kong SAR, China have extended support for email addresses as proxy identifiers. Europe's SCT Inst allows the transfer of funds using the email ID of the recipient. However, it is difficult to ensure uniqueness while using email addresses as proxy identifiers, as no clear underlying identities are associated with them. An individual can easily open an email account using the name of another person or well-known institution. This might lead to confusion about the real identity behind the proxy identifier. Through impersonation, criminal elements can carry out fraudulent transactions. To mitigate this situation, customers can be provided additional details, such as the full name of the account holder, so that the sender can verify the identity of the beneficiary. Using email addresses as proxy identifiers also presents potential privacy concerns and increases susceptibility to cyberattacks, as the addresses can be readily accessed employing telco-to-telco back-end communication channels, including SIM swaps and the interception of one-time passwords.[8]

#### 2.2.3 National ID Number and Corporate Registration Number

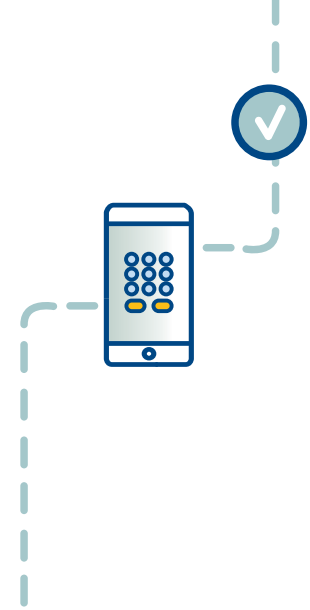
Apart from mobile numbers and email IDs, other prominent proxy identifiers used globally by PSPs are national ID numbers (for individual customers) and corporate registration numbers (for businesses), due to their uniqueness. More importantly, these proxy identifiers allow governments to ensure that social-welfare payments or refunded taxes reach the intended individuals. This also allows government entities to become more transparent and have supporting data to launch effective welfare schemes and services for the public and the business sector.[9] Aliases tailored to corporations and governments provide greater simplicity, flexibility, and security when managing accounts-payable and accounts-receivable functions. Additionally, using corporate ID numbers as aliases simplifies person-to-business use cases, as it removes the need to provide corporate account information to end users. Countries such as Australia, Malaysia, Hong Kong SAR, China, and Thailand are using national ID numbers and corporate registration numbers as proxy identifiers. In Australia, the addressing service PayID allows businesses to receive payments into their accounts without needing to reveal the BSB (Bank-State-Branch) Code and account number. Corporations can be paid by their customers using their Australian Business Number (ABN) in addition to their email IDs and mobile-phone numbers.

#### 2.2.4 Scheme-Specific Proxy Identifier

In addition to such common proxy identifiers as mobile numbers, email addresses, national ID numbers, and corporate registration numbers (business tax IDs), some payment systems also extend support for scheme-specific proxy identifiers while launching proxy services. In Hong Kong SAR, China, FPS ID is a string of numbers generated by the FPS system to link up with a bank or e-wallet account. Each FPS ID is unique and can be linked with only a single participant. Currently, the FPS ID is a seven-digit number, but the system has been designed to prepare for the issuance and use of nine-digit FPS IDs to meet future needs. In India, the Unified Payment Interface (UPI) uses the Virtual Payment Address (VPA), which acts as a unique identifier. The users can set their custom VPAs—for instance, "username@handle" or "username@bank" or "username@upi"—which can then be used to send or receive funds. In the VPA, "username" refers to the user's name, which customers can set in the UPI app, whereas "handle," "bank," and "upi" are the identifiers of banks or third-party applications and are called "handles."

#### 2.2.5 Proxy Identifiers for Cross-Border Payments

Proxy identifiers can also support cross-border payments and facilitate use cases such as international remittances. Xoom, a remittance service provider owned by PayPal, allows money to be sent from the United States, Canada, and Europe to India by identifying the recipient with the VPA—that is, only by giving the receipt's VPA ("username@handle," "username@bank," or "username@upi"). In Europe, the SEPA Proxy Lookup (SPL) service will support interoperability of different European mobile P2P payment schemes and provide the necessary data for inter-scheme P2P payment. This lookup service will provide a mapping of a mobile number to an International Bank Account Number (IBAN), so the P2P scheme of the payer (debtor) can retrieve the payee's IBAN (creditor).



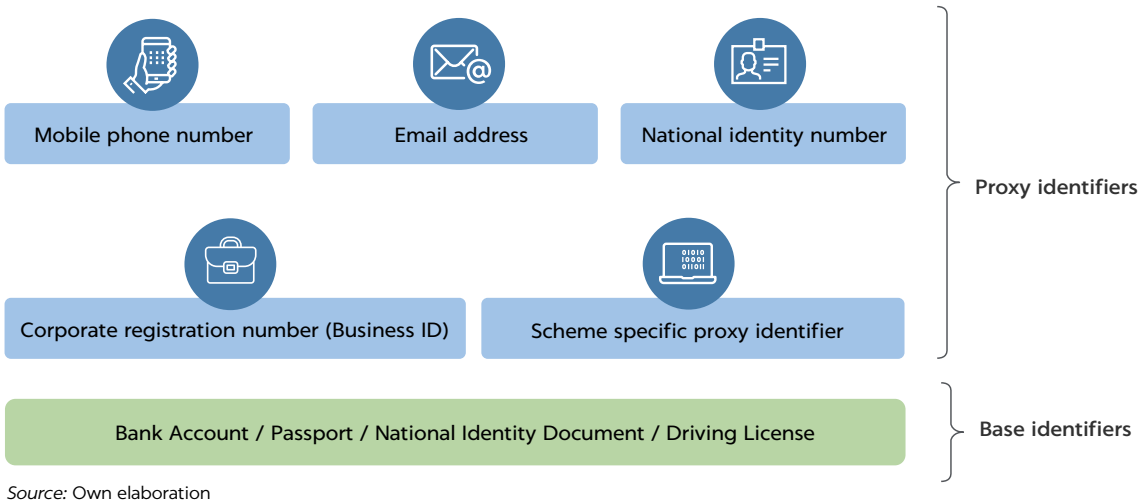
# 3 PROXY DATABASES

Payment system operators are required to establish proxy databases[10] to facilitate alias mapping. Base or reference identities act as the underlying verified identifier that forms the foundation of any proxy service. Base identity documents or know-your-customer documents registered with either the national identity database or the PSP's database can serve as primary identifiers linked to proxy identifiers. These base identifiers are used to verify proxy identifiers during the registration process. PSPs need to verify identities to prevent criminal elements or hackers from taking over accounts or creating accounts with fake credentials. Proxy identifiers can be verified through several methods, such as biometrics (when smartphone capabilities are available) and the verification of SMS and one-time passwords (when biometrics are unavailable). The use of biometric authentication provides superior security, as it is extremely difficult to fake.

Proxy identifiers can be stored on centralized or decentralized databases that are encrypted and used to map proxy identifiers or aliases. Globally, payment systems have adopted the following two different approaches in terms of proxy databases:

**Centralized database:** The mapping of a proxy identifier with a transaction account takes place through a central repository. The central domestic database offers the most straightforward implementation of the proxy service. Figure 3 shows the common process of registering a proxy identifier that is stored in a centralized database.

**FIGURE 2** **Base Identifiers and Proxy Identifiers**




*Source:* Own elaboration

**FIGURE 3** **Typical Process for Registering a Proxy Identifier or Alias**


*Source:* Own elaboration

**Decentralized database:** An authentication message is sent to the beneficiary's PSP to map the proxy identifier with the beneficiary's bank account. In Thailand, alias mapping is done through a decentralized database in which participants are required to map the customer ID with a bank account number. Even though alias mapping is decentralized, customers can use only a mobile number registered with a bank account as an alias.

## 3.1 CENTRALIZED DATABASE

In case of alias mapping through a centralized database, the mapping of a proxy identifier with a bank account takes place through a central alias directory. If the alias mapping is executed through a centralized database, the process creates a single source of information and does not result in synchronization issues. It also ensures that all registered proxy identifiers are unique and there cannot be any duplications. From a customer perspective, the trustworthiness and security of the proxy service is most important. While implementing a centralized database, it is important to establish secured access (that is, who has access to the data, particularly in terms of being able to register and create aliases). Centralized databases might be vulnerable to potential cybersecurity threats; due to this, privacy concerns might arise. Hence, payment system or proxy service operators need to put sufficient controls and processes in place to monitor the database and enumeration controls. Enumeration controls limit how many alias lookups can be conducted within a particular session or period. They also need to test the security of third-party end points to ensure that participant controls are in place and working as intended, so that the addressing service cannot be misused and data is not being inappropriately disclosed. It is also important to have data encryption and cybersecurity controls to ensure data privacy and secured access to the database.

A centralized database is easier to implement, though it is not always possible to establish such a database, due to competition among PSPs and prevalent market conditions. For example, Europe currently has seven different payment system operators, as automated clearinghouses were created to facilitate domestic payments before the Single Euro Payments Area was created.

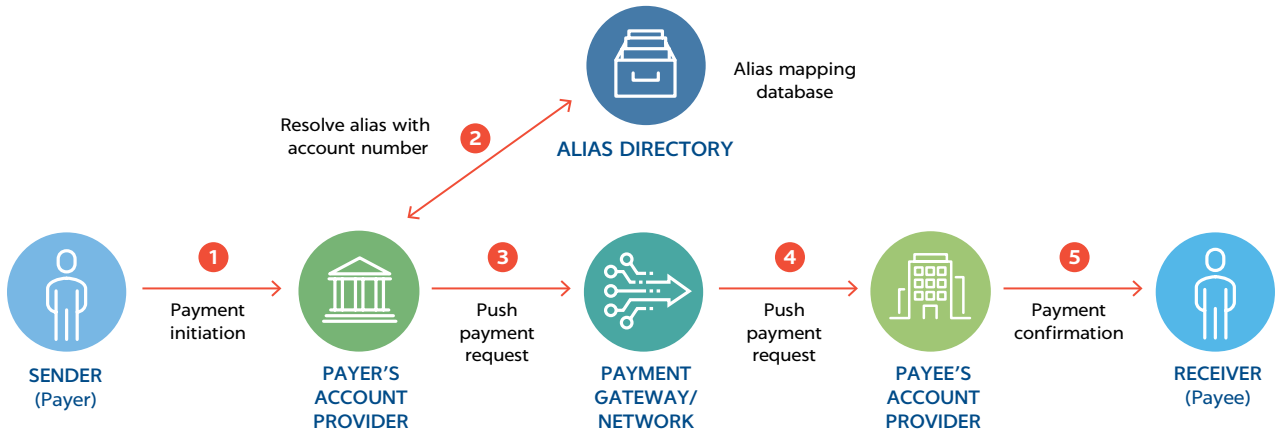
The process flow reverses when a request-to-pay transaction is involved. In this transaction, a receiver sends a collect request by entering the proxy identifier of the payer. In case of a centralized database, address resolution is carried out with the central repository by the payee's account provider. After this, the payee's account provider sends a request-to-pay message to the system operator, which forwards this request to the payer's account provider. The payer receives a notification for authorization of the debit request. The payer can either confirm this request by using secure credentials or chose to decline it. After getting a confirmation from the payer, the payer's account provider debits the account (or rejects, if the payer has declined) and sends a confirmation message to the system operator.

## 3.2 DECENTRALIZED DATABASE

Payment systems can sometimes adopt decentralized databases for alias mapping in which a confirmation message is sent to the payee's bank to map the proxy identifier with the receiver's bank account. One of the key reasons for using decentralized databases is that PSPs are sometimes uncomfortable with sharing customer information in a centralized database because of privacy concerns. Additionally, in a region-specific scheme, PSPs might not be willing to share this information outside their jurisdictions. In countries with large populations, decentralized database might be useful because of the large number of PSPs involved in the payment system.

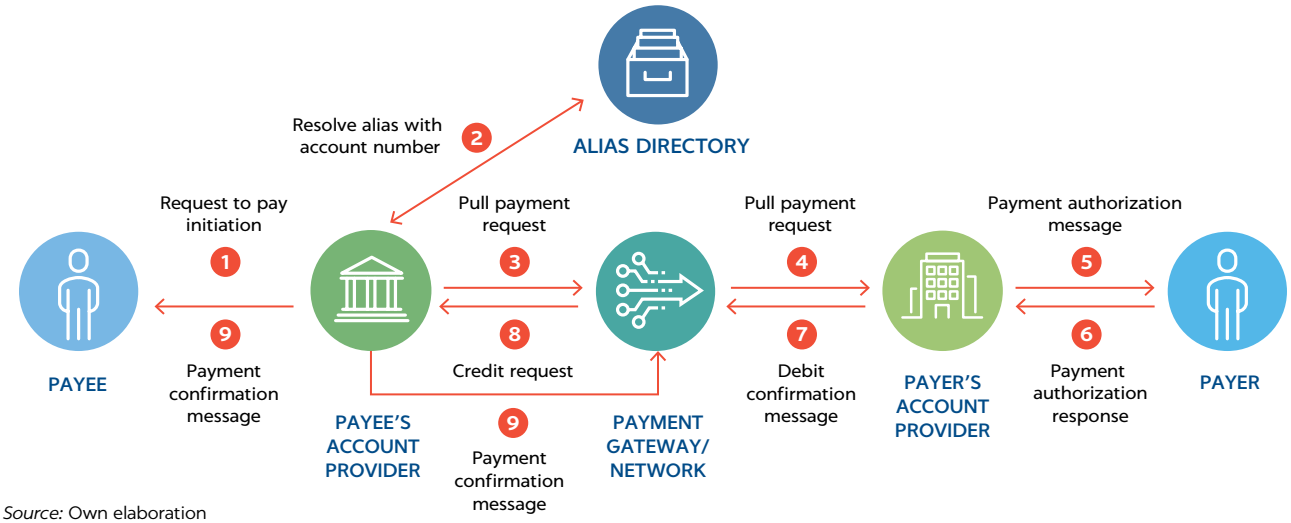
A centralized database enables the sharing of more data with the payment system for address resolution and routing. In comparison, a decentralized database limits the options available for identifying a customer.[11] Alias mapping can be either one to one (where only a single proxy identifier can be linked with an account) or one to many (where multiple

**FIGURE 4** **Centralized Database Process Flow**



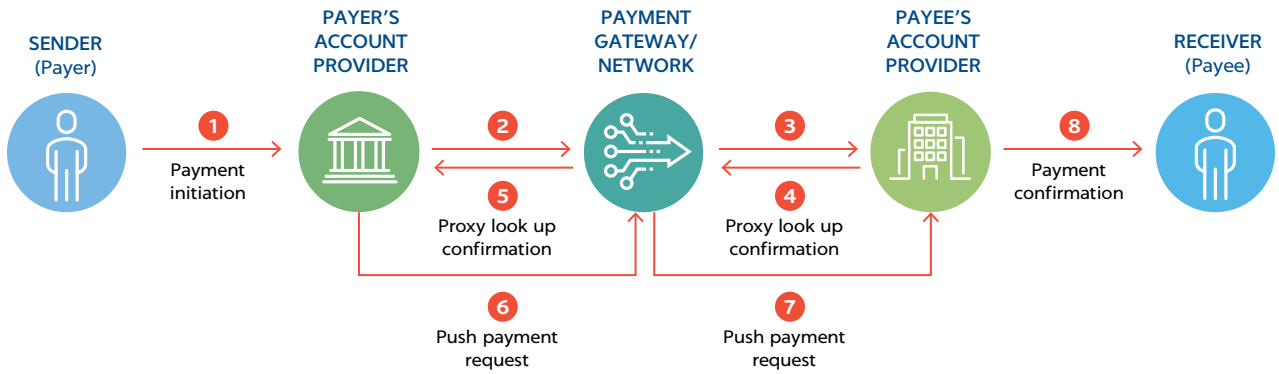

*Source:* Own elaboration

**FIGURE 5** **Process Flow for a Request-to-Pay Transaction (Centralized Database)**




*Source:* Own elaboration

**FIGURE 6** **Decentralized Database Process Flow**




*Source:* Own elaboration

proxy identifiers can be linked to an account). The storage of proxy service data depends on regulatory guidelines, business requirements associated with data localization, and the service providers that can be chosen to host data. When a country/jurisdiction mandates that data be stored within the jurisdiction, dedicated servers are established for storing the data. To ensure data security, strict access control and tracking mechanisms (to trace the source of information) need to be established. Apart from these, validating the identity of the beneficiary before initiating a payment instruction could also help in preventing erroneous transactions. While launching the proxy service, guidelines regarding fraud risks and liability need to be put in place.

It is important to ensure that the data source used to confirm identities is correct, transparent, and updated on a regular basis. Participants should also have a suitable verification processes in place when customers are registering an alias. Most of the systems depend on PSPs to update the database information. Usually, customers are provided secure channels, such as mobile and internet banking, to update their information as and when required. Security layers are used in these applications to protect the information around proxy identifiers as well. In Australia, customers can update and cancel the PayID by logging in to a financial institution, either online or through a mobile-banking app. A similar process is followed in countries such as Mexico and India. In the United Kingdom, customers need to contact the participating financial institution to update or deregister an alias.

# 4 EXAMPLE OF ALIASES USED IN FAST PAYMENTS

**Australia:** PayID is the addressing service that enables users, through their financial institution, to link their transaction account to a simple, easy-to-remember unique identifier called a PayID, such as an email address, phone number, or ABN. PayID has a secure central database to store all PayID information and is operated by SWIFT as part of the New Payments Platform (NPP). PayID sits in the infrastructure of the NPP—that is, it is a part of the core capability of the platform and is an enabler that can be used by any overlay service. However, New Payments Platform Australia does not have access to personal information in the addressing service. Only financial institutions participating in the NPP have access to PayID information.

The types of PayID are an email address, phone number, ABN, Australian Company Number, Australian Registered Body Number, or Australian Registered Scheme Number. However, the type of PayIDs available vary from financial institution to financial institution; most offer a phone number, an email address, ABN, or an organization identifier, such as the company's name. A user needs to register a PayID with his/her financial institution. The process for registering a PayID could differ between financial institutions, but in most cases, a user can create a PayID within the financial institution's usual mobile or internet banking platforms. For privacy and security reasons, PayIDs can be registered and managed only by participating financial institutions. This service also provides confirmation of the payee's legal account name when a PayID is entered, which reduces the risk of misdirecting a payment payment.

When an alias is registered, it is linked with a particular bank account that the customer selects. During payment initiation, the sending participant performs an API lookup to verify that the PayID exists (is registered) and that the account is reachable and then retrieves the BSB (or sort code) and account number details required to send the clearing message to the receiving bank.

**Bahrain:** Initially, Fawri+ transactions were processed only through the customer's IBAN. An IBAN contains 22 alphanumeric characters standardized for all the banks in the country. Since 2018, users of BenefitPay can carry out Fawri+ transactions by entering the receiver's mobile number.

**China:** The People's Bank of China has developed the "mobile phone number payment" function to provide a directory service of mobile-phone numbers and related account information. To ensure that the new function provides a safe and secure payment experience to the public, the bank has formulated the following clear risk-control measures:

- Users are required to register their mobile-phone number in line with the mobile-phone number registered with the bank.
- Upon registration, the bank account should have been open for more than six months with actual transactions, and the registered mobile-phone number should have been used for more than six months before registration.
- The People's Bank of China mandated the use of at least two dynamic authentication factors—that is, face, voice, short messages, and so forth—to ensure the authentic identity of the customer when processing a registration, change, or cancellation.

- IBPS carries out an online check of the payee's name with the input of a mobile-phone number to prevent the wrong payment due to the incorrectly typed number.

**Europe:** The European Payments Council has set up the SPL scheme, which operates based on a dedicated scheme rule book. The scheme is limited to a lookup function with the aim of initiating a payment. The SPL scheme currently allows mobile numbers and email addresses as proxy identifiers. Additionally, local proxy lookup solutions also exist as part of the local P2P payment solution. The scope of the SPL scheme is to make these local solutions interact with each other to support cross-border proxy lookup across local solutions.

**Hong Kong SAR, China:** Hong Kong's FPS follows a one-to-many addressing design—that is, one proxy can be linked to multiple banks, but within one bank, one can link to only one account. The first participant account registered for a proxy identifier will become the default account to receive payments. Customers can change default accounts at their own discretion if they register more than one account. Currently, mobile numbers, email IDs, and FPS IDs are supported as aliases. A central registry in FPS maps proxy identifiers to the specific customer of a bank/e-wallet. The centralized database registry can be accessed by FPS participants and is subject to tariff.

**India:** In India, the UPI system uses VPA or UPI ID, which acts as a unique identifier independent of the bank account number and other details. The system allows customers to set a custom UPI ID, which can then be used either to send or to receive money. It is in the format of "username@handle," "username@bank," or "username@upi." In the VPA, "username" refers to the user's name, which customers can set in the UPI app, whereas "handle," "bank," and "upi" are the identifiers of banks or third-party applications and are called "handles." In case a customer doesn't create a custom VPA in the UPI application, the application creates a VPA automatically in the format of "username@handle" or "username@bank." The "username@upi" VPA is created while using the overlay service BHIM, which the National Payments Corporation of India (NPCI) launched in December 2016.

A key success factor in UPI has been the use of UPI ID. While the Immediate Payment Service (IMPS) also allowed mobile numbers and mobile-money identifiers (MMIDs) as aliases, it faced challenges during its initial years owing to the complexity of MMID (difficult to remember) and its creation process. Subsequently, the MMID format was simplified. For UPI, obtaining a UPI ID has been simplified, and its seamless creation process has led to quicker adoption.

NPCI stores the mapping of mobile numbers to UPI handles. The UPI ID data is mapped at the PSP's end for address resolution. The UPI handle is issued at NPCI with multiple levels of linking. Saved contact numbers can be utilized to send money or raise collect requests; the mobile number can be added as a prefix to the @UPI handle to act as a UPI ID or to check whether the mobile number is available with the same PSP. Addressed with the suffix "@UPI," the handles act as global identifiers for which address resolution is performed at NPCI end. Functionality to pay using Aadhaar number was discontinued, as it is sensitive information, and the framework about its usage in the payment landscape is still evolving.

**Mexico:** The Interbank Electronic Payment System (*Sistema de Pagos Electrónicos Interbancários,* or SPEI) allows mobile numbers and debit card numbers (permanent account numbers, or PANs) as aliases or proxies for the completion of payments. This is done in a decentralized database, as customers have to link their mobile numbers

**FIGURE 7** **Proxy Identifiers in Hong Kong's FPS**

| | |
|---|---|
| 1 **Mobile number** | • Customer can register multiple banks/ e-wallets with the same mobile number<br>• Customer to designate a default bank/e-wallet to receive money |
| 2 **Email address** | • For each bank/e-wallet, one email address for one customer only<br>• Customer to designate a default bank/e-wallet to receive money |
| 3 **FPS identifier** | • Unique ID generated by FPS<br>• Mainly for merchant/corporate as payee (but also support individuals)<br>• One FPS ID mapped to one customer of one bank/e-wallet only<br>• Assigned FPS ID cannot be transferred to another bank/e-wallet |
| 4 **HKID number** | • Facilitate payments using HKID number as payee identifier<br>• To be used only for G2P & B2P payment<br>• Only bank account can register for HKID number addressing proxy, SVF's e-wallets are not eligible to register for the same addressing proxy<br>• Cannot be used for P2P payments |

*Source:* Primary interviews with Hong Kong Interbank Clearing Ltd.

**FIGURE 8** **Proxy Identifiers in India's IMPS and UPI**

| | | IMPS | UPI |
|---|---|---|---|
| **Mobile number and MMID** | MMID is a 7-digit number, first four digits of which are participant identifier and last 3 digits are unique to user. | ✔ | |
| **UPI number** | Virtual address in the format—username@psp. UPI also allows mobile number as an alias. | | ✔ |
| **Aadhaar number** (discontinued) | Individual Identification Number isued by Unique Identification Authority of India | ✔ | ✔ |

*Source:* NPCI

with their bank. To complete a transaction, customers also have to input a reference number, the name of the beneficiary bank, and the concept/reason for payments. Banco de México issued no additional rules and regulations for payments through aliases, as it already follows two-factor authentication. Each participant is free to determine its own linking procedure. However, in general terms, the procedure to link a mobile-phone number to a bank account includes the following steps:

- The user must request the service directly at the bank branch or by electronic media, such as internet or mobile banking. In case of mobile banking, the request must be made from the number that is going to be linked to the account. This request is free of charge.
- The bank has to notify the user that the mobile-phone number has been linked to the account no later than one business day after the request is received.

Participants are also required to fulfill the following obligations while linking a mobile-phone number to a bank account:

- Notify the customer when the mobile-phone number registered to the account has been linked, canceled, or changed.
- Participants cannot request that the mobile-phone service be provided by a specific company to link the mobile-phone number to an account.

Banco de México designed the overlay service CoDi to simplify and homogenize the experience of requesting a payment or answering a request to pay for the final user. It also allowed mobile numbers to be used as aliases. While the platform was not designed with a specific payment use case in mind, such as P2P or person-to-government, the clearest use cases currently are person-to-business as well as e-commerce transactions.[12] Banco de México is considering allowing national ID numbers to be used as aliases for CoDi transfers.

**Poland:** Express Elixir uses IBAN for all types of transactions initiated on its platform. IBAN has certain advantages over other aliases. For example, a single IBAN can provide various details, such as bank name, bank account number, customer details, and so on. System operator KIR believes market players are in the best position to decide various use cases that best meet customer needs. While Express Elixir is the underlying platform, the banks can innovate to develop various use cases. Making mobile P2P payments is the most popular use case for the Express Elixir system enabled by the BLIK services using mobile numbers as aliases.

**Sweden:** In Sweden, the Bankgiro number is used as the payment address, instead of a customer's current account number. These numbers are not issued by banks but by Bankgirot, the national payments processor. Most Bankgiro numbers are used by businesses. In communications with their customers, such as invoices, businesses can state their Bankgiro number, a self-authenticating number that is linked—in Bankgirot's central back office—to the relevant company's account number. This alias has a favorable effect on barriers to switching bank accounts, as it removes the need for businesses to notify their customers of new account numbers.[13]

**Singapore:** PayNow, the overlay service, enables retail customers to send and receive funds in Singapore dollars from one bank to another in Singapore through FAST by using just their mobile number or Singapore NRIC/FIN, almost instantly. PayNow also allows use of a company registration number as a proxy address for the recipient, enabling businesses to migrate from traditional checks and cash to electronic payments and collections.

**Thailand:** PromptPay has enabled faster and more convenient fund transfers among individuals and businesses by using easier-to-remember numerical IDs, such as national IDs, mobile numbers, corporate registration numbers (tax ID numbers), or e-wallet IDs as proxies for traditional bank account numbers.

Technically, PromptPay can support any alias. Mobile numbers and national IDs are aliases that customers have adopted most readily. As an email ID did not provide any additional benefits compared with mobile number, it was not enabled as an alias. A customer can only use a mobile number that is registered with the bank account as an alias. In case a customer decides to use any other ID as an alias, a verification message is sent to the mobile number registered with the bank account for confirmation. Alias mapping is decentralized in PromptPay. Banks are required to map the proxy identifier with a bank account number.

Using aliases has allowed e-payments in Thailand to grow significantly. From 2016 to 2017, the first year of introduction, the volume of mobile payments grew 110 percent.[14] Accumulated registered PromptPay users amounted to 54.7 million as of May 2020. In July 2016, the first month that registration opened, there were 13 million registered PromptPay users; the number has increased more than four times.

**United Kingdom:** The overlay service Paym uses mobile numbers as aliases for the bank account details. A customer enters the receiver's mobile number and authenticates to complete the transaction.

The customer needs to register only to receive funds. Once customers register for Paym in their mobile-banking app, they can open the application, enter details of the individual, and confirm the payment. Banks can decide to register corporate customers and enable payments for them through an alias (mobile number). Customers can transfer money directly to their contact by choosing it from the drop-down menu. If the receiver does not have Paym, an SMS is sent to the number to contact the bank and register with the application. Once the payment is completed, both the payee and the payer receive the confirmation message. Currently, 15 banks accept transactions through Paym.

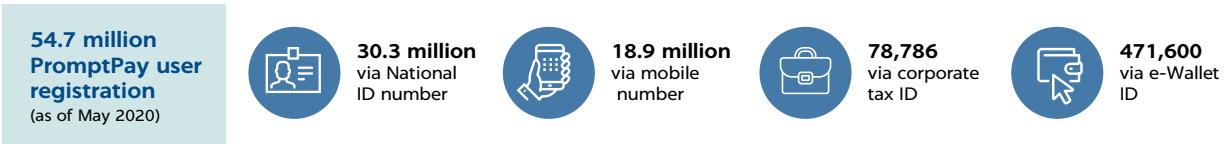
Following the introduction of Paym in 2014, which allowed the use of mobile numbers for P2P payments, replacing the recipient's account number/sort code, payments using the new service saw year-on-year growth from 2015 to 2016 of 259 percent, from approximately 775,000 to over two million. Consumers cited the improvements in ease of use for P2P mobile payments: 27 percent highlighted the ease of using a phone number over inputting account information, 24 percent mentioned the ease of receiving payments, and 20 percent suggested that Paym meant "one less job to do."[15]

**United States:** The core infrastructure of the Real-Time Payments (RTP) system inherently doesn't support the use of aliases or proxies for payments, although the network allows third parties to enable alias or proxy payments. PSPs such as PayPal and Venmo currently use the RTP network for transfers to their clients' bank or credit-union accounts using aliases.

The PSP Zelle enables the use of mobile numbers and email addresses to send P2P payments. TCH has entered into a partnership with Zelle to provide settlement services. Currently, integration of RTP and Zelle is in progress. Zelle allows the use of mobile numbers or email addresses as aliases.

There are no plans to launch RTP's own social alias/proxy service because the market is already well served and existing alias/proxy services might transition to RTP payments to clear and settle transactions. The RTP network will support tokenization of account numbers, which could be a way to allow payment originators and PSPs to replace account numbers with tokens, mitigating the threat of a data breach.

**FIGURE 9** **Breakdown of User Registration in Thailand's PromptPay**




*Source:* National Interbank Transaction Management and Exchange

# 5 CONSIDERATIONS FOR DESIGNING A PROXY IDENTIFIER

Proxy identifiers should be easy to remember, easy to share without risk, and interoperable.[16] Some of the key considerations for choosing proxy identifiers are showcased in figure 10.[17]

Other considerations for implementing a proxy identifier include the following:

- **Easy registration:** The customer-registration process needs to be simple and easy to complete and should be visible within the participant's access channels, such as internet banking or mobile banking.
- **Implementation cost:** Payment systems generally offer proxy lookup service as a key offering to enhance customer convenience apart from these parameters. It is also important to evaluate implementation cost and infrastructure requirements while choosing the proxy identifiers. The implementation cost for a proxy service depends on its construction, capacity requirements, and data-storage requirements. Significant investment in data security and encryption is also required. If implementation costs are significant, then options include using decentralized databases. For example, Chile and the United States don't offer a proxy service as the core functionality of payment system; rather, this service is extended to customers through financial institutions and third-party service providers.
- **Data privacy and security:** While launching a proxy service, it is important to establish data security and privacy measures. In addition, PSPs need to obtain consent from customers to use a particular proxy identifier. Payment system operators also need to put in place rules regarding fraud risk management and liability, and to ensure that registering parties have suitable verification processes in

**FIGURE 10** **Key Considerations for Choosing Proxy Identifiers**

**ACCESSIBILITY**

- Proxy identifier or alias should be readily accessible to a large number of customers in order to ensure traction for the proxy service.

**VERIFIABILITY**

- Proxy identifier must be verifiable through another proxy channel or medium. It is important to ensure a secondary means of verifying the link between the proxy and transaction account holder, especally when there is no single national identity database.

**TRUST**

- End-customer must have perceived sense of reliability, regarding the proxy identifier. Proxy identifiers need to be unique to each customer, must protect customer privacy and must facilitate a friendly and seamless customer experience.

*Source:* Own elaboration

place when customers are registering an alias. Furthermore, it is important that the proxy identifier used does not constitute an authentication mechanism—for example, a username to access internet or mobile banking—or that it requires the user to reveal sensitive information, such as using a primary account number as an alias.

- **Standardization:** It is important that the proxy identifier supports a vast number of use cases, for which consensus with PSPs and standardization are required to avoid fragmentation and facilitate a seamless user experience. For example, global PSPs such as PayPal and Apple Pay are also offering customers a choice to use proxy identifiers (mobile numbers or email addresses) as a substitute to card numbers while making payments. If these aliases are not supported by a fast payment system, then users would need to use a separate alias for transactions that are supported by such a system.

# 6 CONCLUSION

A proxy or aliasing service helps to enhance the user experience, as it enables the use of proxy identifiers such as mobile-phone numbers or email addresses when receiving payments into their bank account, rather than having to remember and share bank account numbers. When choosing a proxy identifier, it is important that it is easy for a customer to remember, as the intention is to simplify the payment experience. The uniqueness of the proxy identifier is important from a technical perspective, so that the payment system accurately identifies where to send the payment or request for payment. If the capability is introduced as a core functionality, there is more flexibility in how the capability can be used. While launching the proxy service, strong customer-verification standards need to be put in place to prevent the registration of fraudulent aliases. It is also critical to ensure that necessary controls are in place to prevent cybersecurity breaches and to establish independent testing of end points to ensure that controls are working as intended in all channels.

A centralized database was put in place in Australia, as it had a centralized regulatory authority along with a single payment system operator, whereas in a scheme such as SCT Inst, where multiple countries are involved, it is quite difficult to establish a centralized database. The choice of proxy database varies across different payment systems based on the regulatory environment, competition, and prevalent market practices in a particular jurisdiction.

# 7 ACKNOWLEDGMENTS


| Organization | Contributor |
|---|---|
| Deloitte India | Deloitte India |
| New Payments Platform Australia (NPPA) | Katrina Stuart |
| SWIFT | Carlo Parmers |
| | Saqib Sheikh |
| World Bank | Harish Natarajan |
| | Nilima Ramteke |
| | Holti Banka |
| | Guillermo Galicia Rabadan |

## NOTES

1. According to the Committee on Payments and Market Infrastructures, a fast payment can be defined as a payment in which the "transmission of the payment message and the availability of 'final' funds to the payee occur in real time or near-real time on as near to a 24-hour and seven-day (24/7) basis as possible."
2. https://developer.visa.com/images2/products/visa_direct/ads_technical_specifications_v3.0.pdf
3. https://www.vocalink.com/payment-processing/multi-proxy-service/
4. https://www.bot.or.th/English/ResearchAndPublications/Report/DocLib_AnnualEconReport/AnnualReport2018_En.pdf
5. https://www.nationthailand.com/Corporate/30357692
6. https://cenfri.org/wp-content/uploads/An-analysis-of-ID-proxy-initiatives-across-the-globe_Cenfri_BankServAfrica.pdf
7. gsma.com/futurenetworks/wp-content/uploads/2020/02/RCS-and-Payments-Whitepaper-1.pdf
8. https://cenfri.org/wp-content/uploads/An-analysis-of-ID-proxy-initiatives-across-the-globe_Cenfri_BankServAfrica.pdf
9. https://www.bot.or.th/English/PaymentSystems/PolicyPS/Documents/PaymentRoadmap_2021.pdf
10. A database is an organized collection of structured information, or data, typically stored electronically in encrypted form. The main purpose of a database is to operate a large amount of information by storing, retrieving, and managing data.
11. https://www.cgap.org/blog/comparing-indias-upi-and-brazils-new-instant-payment-system-pix
12. https://cenfri.org/wp-content/uploads/An-analysis-of-ID-proxy-initiatives-across-the-globe_Cenfri_BankServAfrica.pdf
13. https://www.dnb.nl/en/binaries/Reflection%20on%20the%20use%20of%20aliases%20and%20customer%20mobility%20in%20the%20payments%20market%20NFPS%202018.docx_tcm47-375820.pdf
14. Mastercard, Economic Impact of Real-Time Payments (Deloitte, July 2019).
15. Mastercard, Economic Impact of Real-Time Payments (Deloitte, July 2019).
16. https://pay.google.com/about/business/static/data/GPay_RTP_2019.pdf
17. https://cenfri.org/wp-content/uploads/An-analysis-of-ID-proxy-initiatives-across-the-globe_Cenfri_BankServAfrica.pdf


WORLD BANK GROUP