TECHNICAL REPORT

ISO/TR 21941

First edition
2017-07

Financial services — Third-party payment service providers

Services financiers — Prestataires de services de paiement tiers

Reference number
ISO/TR 21941:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **1**
4 Overview of the current TPP landscape **3**
4.1 General 3
4.2 Europe 5
4.2.1 Europe and the revised Payment Services Directive 5
4.2.2 Advantages of a common standard 5
4.2.3 Contents of the standard 6
4.3 Asia 6
4.3.1 Korea 6
4.3.2 Japan 7
4.3.3 China 7
4.4 America 9
4.4.1 Canada 9
4.4.2 Brazil 10
4.4.3 USA 12
4.5 Oceania — Australia 13
4.6 Africa — South Africa 14
5 Reference models and architecture **15**
5.1 General 15
5.2 Example from Norway 16
6 Further potential developments **17**
Bibliography **19**

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial Services, security*.

Introduction

This document was initiated 2 years ago with the aim of conducting research into the interface between third-party payment (TPP) and account servicing payment service providers.

As TPP is a fast-developing area, it was critical to provide guidance quickly.

This document gives an overview of the situation in different regions as it was at the end of 2015 and the beginning of 2016. There have been new developments in several of the regions since then.

For the purposes of this document, payment initiation service providers (PISP) and account information service providers (AISP) are commonly named as TPPs. Furthermore, while there could be other relevant documents to choose from in other markets with regard to terms, definitions and abbreviated terms, the choice has fallen on PSD2[2], as a key reference, as this document can be seen as a good place to start. It should also be noted that the verbal forms are used and interpreted as follows:

— “should” indicates a recommendation;

— “can” indicates a possibility or a capability;

— “must” indicates an external constraint.

NOTE External constraints are not requirements of the document. They are given for the information of the user. Examples of external constraints are laws of nature and legal requirements.

Financial services — Third-party payment service providers

1 Scope

This document reports the findings of research into the interface between third-party payment service providers (TPPs) and account servicing payment service providers (ASPSPs).

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1.1
account information service
online service to provide consolidated information on one or more *payment accounts* (3.1.7) held by the *payment service user* (3.1.2) with either another payment service provider or with more than one payment service provider

[SOURCE: Directive (EU) 2015/2366, definition 16]

3.1.2
payment service user
natural or legal person making use of a payment service in the capacity of payer, payee, or both

[SOURCE: Directive (EU) 2015/2366, definition 10]

3.1.3
account servicing payment service provider
payment service provider providing and maintaining a *payment account* (3.1.7) for a payer

[SOURCE: Directive (EU) 2015/2366, definition 17]

3.1.4
authentication
procedure which allows the payment service provider to verify the identity of a *payment service user* (3.1.2) or the validity of the use of a specific *payment instrument* (3.1.9), including the use of the user's *personalized security credentials* (3.1.6)

[SOURCE: Directive (EU) 2015/2366, definition 29]

3.1.5
strong customer authentication
authentication (3.1.4) based on the use of two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data

[SOURCE: Directive (EU) 2015/2366, definition 30]

3.1.6
personalized security credentials
personalized features provided by the payment service provider to a *payment service user* (3.1.2) for the purposes of *authentication* (3.1.4)

[SOURCE: Directive (EU) 2015/2366, definition 31]

3.1.7
payment account
account held in the name of one or more *payment service users* (3.1.2) which is used for the execution of payment transactions

[SOURCE: Directive (EU) 2015/2366, definition 12]

3.1.8
payment initiation service
service to initiate a payment order at the request of the *payment service user* (3.1.2) with respect to a *payment account* (3.1.7) held at another payment service provider

[SOURCE: Directive (EU) 2015/2366, definition 15]

3.1.9
payment instrument
personalized device(s) and/or set of procedures agreed between the *payment service user* (3.1.2) and the payment service provider and used in order to initiate a payment order

[SOURCE: Directive (EU) 2015/2366, definition 14]

3.1.10
sensitive payment data
data, including *personalized security credentials* (3.1.6) which can be used to carry out fraud

Note 1 to entry: For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.

[SOURCE: Directive (EU) 2015/2366, definition 32, modified — Part of the definition has been formatted as Note 1 to entry.]

3.1.11
third-party payment service provider
payment service provider offering *payment initiation services* (3.1.8) or *account information services* (3.1.1) on accounts where they are not the account-servicing payment service provider themselves

3.1.12
interface
device or program for connecting two items of hardware or software so that they can be operated jointly or communicate with each other

3.1.13
gatekeeper
function that ensures that admittance is limited to *third-party payment service providers* (3.1.11) who comply with regulatory and technical requirements

Note 1 to entry: This function can be provided by individual banks or a common actor within finance industry.

Note 2 to entry: The third-party payment service provider itself can provide the gatekeeper function if certified.

3.2 Abbreviated terms

ACH	automated clearing house
AISP	account information service provider
API	application program interface
ASPSP	account servicing payment service provider
ATM	automated teller machine
EFT	electronic funds transfer (or e-funds transfer)
OAuth	open authentication
PISP	payment initiation service provider
PSD2	Payment Services Directive II
PSP	payment service provider
PSU	payment service user
SAML	security assertion markup language
TPP	third-party payment service provider

4 Overview of the current TPP landscape

4.1 General

There are two main types of third-party payment service provider:

a) payment initiation service providers (PISPs);

b) account information service providers (AISPs).

Much taxonomy describing third-party services also consider payment instrument issuing providers, who are financial institutions other than those servicing the account of the customer, and who issue a payment card or a payment instrument.

The idea behind third-party providers is for customers (payment service users) to perceive them as added value to the service of their account servicing payment service provider. Added value could be new online payment services and more variety in payments instruments, better or simpler user experience, etc.

One of the main points of attention is related to security, especially strong customer authentication and secured communication, which is key to achieving the objective of enhancing consumer protection and promoting innovation. Ensuring the security of payments and the protection of sensitive payment data are a critical part of the infrastructure of robust payment systems knowing all actors should act on

the same level playing field, i.e. the new players should ensure the actual highest levels of security are implemented. Security recommendations are designed for TPPs and ASPSPs and include matters, such as

— segregation of duties in information technology,

— hardening servers with secure configurations,

— applying “least privilege” principles to access control,

— limiting login attempts,

— end-to-end encryption, and

— non-sharing user credentials.

One of the key points is that strong authentication for customers when registering cards, making credit transfers and/or making card payments should be implemented.

Third-party access to accounts, the use of APIs to connect merchant and the bank directly and the ability to consolidate account information in a unique portal are likely to affect payment services around the world. With external APIs, customers will have more options to interact with their TPPs or ASPSPs, next to usual online and mobile banking applications.

PISPs and AISPs can be any type of PSP authorized to offer payment initiation services or account information services and thus could be, for example, a credit institution or a payment institution. TPPs in the context of payment initiation services and account information services are not just the ASPSP in terms of the accounts to which they are obtaining access. In other markets, TPPs may not themselves offer payment accounts, but gather information or perform payment initiation functions where they require access to the payment account. The interface between the TPP and the ASPSP is considered security sensitive; this applies both to AISPs and PISPs. This is due to the following.

a) Entity authentication: the PISP and AISP should provide authentication ensuring that the TPP trying to access an account is an agreed TPP and is approved by the ASPSP in advance based on a contractual relationship or listed on a public authority white list.

b) Strong customer authentication: the PSU should be authenticated in a way that ensures the account servicing payment service providers that the correct PSU is present and has given its consent to the transaction and given access to its account to a third party. The split of information and authentication functions between TPP and ASPSP might be organized in several ways. Nevertheless, user credentials should always be protected and should never be stored. Security standards and protocols such as OAuth or SAML can be used, without the need to store credentials.

c) Authorization: the ASPSP should authorize the PSU’s transaction or operation request before execution.

d) Confidentiality: the TPPs get lots of information about the PSUs and this should be handled according to privacy laws and good practice for banking.

e) Integrity: deletion, manipulation or insertion of information should not occur. In particular, a payment transaction submitted by a PSU should be protected all the way from initiation to ASPSP.

f) Availability: the TPPs should not influence negatively upon availability and uptime of the ASPSP.

The relation between TPP and ASPSP may be bilateral using a contractual agreement between the parties, it may be part of a multilateral scheme or an alternative. A multilateral scheme should give the ASPSP full control and knowledge about which TPPs have access to which types of services.

Management of the multilateral scheme may be performed by the financial supervisory authority of a jurisdiction, by the ASPSPs themselves or by another body. To be approved as a participant in the scheme may require a formal evaluation of the third party, licensing based on a self-assessment or simply a registration. A number of models are possible for this. If the scheme is managed by a financial

supervisory authority, it is likely that they will give a set of rules with supplementary technical regulatory guidelines.

A working paper from SWIFT[6] points out that there is currently no global unified approach regarding regulatory initiatives concerning TPPs. The first challenge is getting to a common understanding of terminology and characteristics of the various TPPs as a foundation for future standardization and definition of regulatory environment.

4.2 Europe

4.2.1 Europe and the revised Payment Services Directive

The revised EU Payment Services Directive (PSD2) entered into force in January 2016 and is intended to be transposed into member states' national law and applied by 13 January 2018. It will enable third-party payment service providers to access customer payment accounts. Account-servicing payment service providers will be required to make available access and all relevant information to third-party payment service providers. Specifically, this covers the following three services:

a) payment initiation services;

b) account information services;

c) "confirmation on the availability of funds" checking services.

With regard to the electronic interface, the European Banking Authority (EBA) is required to draft and present to the European Commission regulatory technical standards (RTSs) for strong customer authentication and secure communication within 12 months after the entry into force of PSD2. Following their adoption by the Commission, the market will have a period of 18 months to implement them. In this regard, the EBA sent out a discussion paper[3] in December 2015, inviting stakeholders to submit their views on a number of identified issues key to the development of the technical standards. Among the stakeholders consulted were the European Payments Council (EPC) and the European Banking Federation (EBF). Their replies to the discussion paper may be of interest for further reading. An official consultation will follow this summer.

There are several options when it comes to implementation. Uniform and interoperable communication between third-party payment service providers and banks in Europe would be preferable. However, this, in turn, presupposes a common interface standard or schema.

4.2.2 Advantages of a common standard

Recital 93 of PSD2 says: "In order to ensure secure communication between the relevant actors in the context of those services, EBA should also specify the requirements of common and open standards of communication to be implemented by all account servicing payment service providers that allow for the provision of online payment services. This means that those open standards should ensure the interoperability of different technological communication solutions." Ideally, interoperability of interacting market participants is achieved through standardization. Open standards are standards that can be developed jointly by all interested market participants.

As there is no international account interface standard at present and EBA will merely define generic requirements, uniform EU-wide implementation cannot be ensured. There are no plans either for EBA to mandate a standard-setter such as European Committee for Standardization (CEN) or International Organization for Standardization (ISO) to draft specifications for an interface.

Implementation of the technical requirements will ultimately be left to the market. This harbours the danger that both banks and third-party payment service providers would have to support several different standards, which immediately raises the question of interoperability. While external parties could provide appropriate transmission services, they would certainly not do so free of charge. In a worst-case scenario, there could, however, be a large number of different interfaces if banks and third-

party payment service providers offer proprietary solutions that meet EBA's generic requirements. This would not be in the interests of either banks or third-party payment service providers.

Standardization makes sense whenever it is a question of uniting many different parties to form a networked industry, for example, the payments sector. Communication via a common interface cuts development, maintenance and enhancement costs for every single party and only requires one-time implementation. All banks in Europe could be reached with a standard. The aim of standardization is thus not walled-off markets but uniform access to these markets.

4.2.3 Contents of the standard

An interface standard should cover the following points, among others:

— the legally defined business transactions;

— formats needed for the exchange of messages;

— security requirements.

The purpose of the standard would be to meet the statutory requirements of PSD2. At the same time, it should be designed openly enough so that further services based on it are possible and it can be adapted to accommodate future extensions or requirements.

4.3 Asia

4.3.1 Korea

The Korean "e-Financial Transaction Act" (Article 28) allows the third-party payment service provider, which is defined as an "e-financial business operator" in Korea, to undertake the following:

— e-funds transfer (EFT) services;

— issuance and management of e-debit payment means;

— issuance and management of e-prepayment means;

— e-payment agent services (e.g. payment gateway services for internet shopping mall);

— other e-financial services determined by presidential decree.

The third-party payment service providers have to register for the above services via the banks' sponsoring relationship.

The relationship between the banks and the third-party payment service providers can be described as follows.

— The third-party payment service provider must become a corporate client of the bank.

— When a customer gets a loss due to an incident, the bank or the third-party payment service provider is liable for indemnifying the customer for the loss (Article 9). Who is responsible for the loss depends on the cause of the incident and the contract between the bank and the third-party payment service provider.

— Both the bank and the third-party payment service provider must fulfil the duty of good management to ensure the safe processing of e-finance transactions and they must meet the government standards (Article 21).

Article 21 of the e-Financial Transaction Act is very important to the third-party payment service provider in terms of information security in Korea.

4.3.2 Japan

Table 1 gives an overview of major third-party payment services in Japan.

Table 1 — Major third-party payment services in Japan

	Payment gateway service	Personal finance management
Service overview	Provides e-commerce merchants with a gateway for payments via credit cards. Some of the TPPs provide a service which enables payments using a proxy (e.g. email address, ID for the TPP's service) of a payer's credit card number.	Aggregates balance/transaction information on various accounts (e.g. banking accounts, credit card accounts, electronic money accounts, investment accounts) and provides it to the account holder in a single table.
Relationship with ASPSP	TPPs transfer payment information from an e-commerce merchant's website to the relevant ASPSP (a credit card acquirer of the merchant).	TPPs collect balance/transaction information from the ASPSPs which have been registered beforehand by the account holder. Some ASPSPs offer an API to TPPs.
Example of the service	PayPal LINE Pay PAY.JP	Money Forward Moneytree Freee Zaim
Security	PCI-DSS Version 3.0	PCI-DSS Version 3.0

With regard to regulation, the TPPs must adhere to the Act on the Protection of Personal Information[7] but they are not supervised by a competent authority. ASPSPs are supervised by the Financial Service Authority or the Ministry of Economy, Trade and Industry. Examples of regulations in force are as follows.

— Bank: The Banking Act[8];

— Credit card: The Installment Sales Act[9];

— Electronic money: Payment Services Act[10].

4.3.3 China

4.3.3.1 Requirements and conditions of business permission

The People's Bank of China (PBC) has formally issued the "Administrative Measures for the Payment Services Provided by Non-financial Institutions" [PBC Decree No. 2 (2010) hereinafter referred to as "Decree No. 2"] in June 2010, which has established a supervision and administration mechanism for the payment services provided by non-bank financial intermediaries from the perspective of business permission, clients' reserves and service specification.

The term "payment services provided by non-bank financial intermediaries" as mentioned in these measures refers to the monetary capital transfer services provided by non-financial institutions as the middlemen between payers and payees. Business types are as follows:

— payment through the network;

— issuance and acceptance of prepaid cards;

— bank card acquiring;

— other payment services as specified by the PBC.

Concerning the requirements for payment business permission, the non-financial institutions to provide payment services must meet the following conditions.

a) Commercial presence: it is a limited liability company or joint-stock company legally formed inside the People's Republic of China and it is the corporate body of a non-financial institution.

b) Capital strength: the minimum registered capital for an applicant that intends to operate the payment business countrywide is 100 million Yuan, while that for an applicant that intends to operate the payment business in a province (autonomous region or municipality directly under the Central Government) is 30 million Yuan. The minimum registered capital must be paid-in monetary capital.

c) Major investors: the major investors (including an investor which actually controls the applicant or an investor which holds more than 10 % of the applicant's equity) of the applicant must meet the qualification requirements on the nature of corporation legal personality, working experience in related areas and profit ability, etc.

d) Anti-money laundering measures: the applicant must possess the anti-money laundering measures as specified by national anti-money laundering rules and provisions and submit checking materials on anti-money laundering measures upon application.

e) Payment facilities: the applicant must submit its technical safety certifications on its payment facilities.

f) Credit requirements: the applicant, its senior managers and major investors must have good credit status and provide their clean criminal records.

"Payment Business Permits" are valid for a period of 5 years from their issuance date. Payment institutions must apply to the local branches of the PBC for renewal within 6 months before the expiry date of the "Payment Business Permits". Upon approval by the PBC, the duration of each renewal period is 5 years.

4.3.3.2 Administration of clients' reserves

The PBC implemented supervision and administration on third-party payment businesses with the core purposes of strengthening capital supervision and safeguarding the legitimate rights and interests of clients. Decree No. 2 specifies the ownership of clients' reserves, makes it explicit that the payment institutions are not allowed to possess the clients' reserves as their own property and that they are only allowed to transfer the reserves upon the payment order given by the clients. It is prohibited that payment institutions misappropriate the clients' reserves in any form.

The "Measures for the Custody of Clients' Reserves of Payment Institutions" specifies and concretizes the supervising and managing request of the PBC for clients' reserves, strengthens consciousness and responsibilities for fund safety protection and responsibilities for supervision of reserves bank and ensures the legitimate rights and interests of clients. The measures regulate in detail the deposit activities of clients' reserves such as deposit, collection, use and transferring.

The following are the setting conditions for reserves bank of payment institutions:

a) the total asset is not less than 200 billion Yuan;

b) the risk control indicators related to capital adequacy ratio, leverage ratio and mobility meet the regulations.

The total assets of a reserves bank, in which a payment institution only opens a remittance account for reserves in this bank, are not to be less than 100 billion. Meanwhile, the reserves bank must be regulated to supervise the deposit, use and transferring of clients' reserves and the payment institution must cooperate with this supervision.

On the aspect of the use of clients' reserves, when the daily requirements of payment business are met, namely the liquidity requirements are met, payment institutions may deposit clients' reserves by

means of corporate deposit, corporate notice deposit, agreement deposit and other forms approved by the PBC.

4.3.3.3 Regulation practices

By means of on-the-spot supervision and inspection, and off-the-spot supervision and inspection, establishing and perfecting the industry self-regulation system, the People's Bank of China supervises and controls the payment institution.

On-the-spot inspection

a) Study and prepare the on-the-spot inspection manual for payment institution.

b) Organize and inspect the card issuing spot condition of prepaid card and bank card.

Off-the-spot inspection

Establish a series of off-the-spot supervision and administration mechanisms, including

— classification supervision,

— supervision and administration running by the local authorities,

— annual report on supervision and administration,

— quarterly report on supervision and administration, and

— report on significant issues and verification mechanism of reserves, to strengthen the dynamic inspect of business operation of payment institution.

The PBC guides and supports the Payment and Clearing Association of China to focus on establishing the system of self-regulation and industrial service, formulate an industry self-regulation convention, and set up working committees for special projects. Therefore, the main business area of payment and clearing is basically covered, and the system of self-regulation is to be completed. At present, the multi-dimensional system of "Government Supervision, Self-regulation, Corporate Governance, Self-discipline" has basically been formed. The vertical regulation system from head office to branches of the PBC has also basically been formed.

4.4 America

4.4.1 Canada

This issue is in flux in Canada as a full review of the payments ecosystem is currently being undertaken. The information below may therefore change significantly in the next few years. At present, the structure of regulation is as follows.

a) Government of Canada: Bank Act, Bank of Canada Act, Canadian Payments Act (CP Act), Bills of Exchange Act, Payment Clearing and Settlement Act (PCSA), plus various voluntary codes, regulations and agreements.

b) The CP Act provides that the Canadian Payments Association (CPA) is responsible for operating the national clearing systems and for making rules/standards regarding the clearing system. Additionally, the Bank of Canada under the PCSA is responsible for ensuring the management of systemic, prominent, etc., risks in the system. Generally, Bank of Canada PCSA requirements are incorporated into the CPA rules.

c) Generally, an entity that wishes to make a payment in Canada (which does not include drawing down on a credit card line) must settle through the payment rails provided by the CPA. Under the CPA, direct clearers and large value transfer system (LVTS) participants have access to the CPA payment rails. Thus, for standard payments (i.e. non-credit card drawdowns also known as "credit card payments"), TPPs go through their CPA member to access the payment rails.

d) Credit/debit card networks operate under the Code of Conduct for Debit and Credit Cards in Canada along with the private contracts and network rules. The Code is specialized and determines scheme activities and relationships (specifically with acquirers, functions, etc.).

Note that the above does not talk to various other regulation sets such as Anti-Money Laundering (AML), Know Your Customer (KYC), privacy laws, etc.

In addition, APIs in Canada have been in existence for about 30 years. They are the Canadian standard automated funds transfer (AFT), card scheme, etc., formats. That allows submission of payments to a CPA financial institution. The PSD2 environment does not exist in Canada; the financial institutions are responsible for their customer's information and do not provide open access to them as contemplated by PSD2.

4.4.2 Brazil

4.4.2.1 General

Table 2 gives an overview of the actors in the Brazilian payment service provider environment as stated by the Brazilian regulators.

Table 2 — Actors as stated by Brazilian regulators

Term	Definition
Payment arrays	Set of rules and procedures that govern the provision of certain payment service to the public and accepted by more than one recipient through direct access by the end users, payers and payees.
Payment array establisher	Legal entity that is responsible for a determined payment array and the brand associated with the said array, if applicable.
Payment institution	Legal entity that adheres to one or more payment array, whose core business is associated with the following activities: — enable payment account funds withdrawal; — execute or facilitate payments instructions (payment initiation and delivery); — manage payment accounts; — payment instrument issuance; — accredit payment instruments; — remittance; — physical to digital currency conversion.

The PSP environment in Brazil is regulated by law no. 12.865, from 2013, on a federal level. This broad-level regulation describes the actors to be regulated and monitored by the Brazilian Central Bank, and the national telecommunications agency, when applicable. The only exceptions to Brazilian Central Bank regulations are the private label arrays and payment arrays that are meant exclusively for the payment of public services (i.e. electric bills, transport, etc.).

Under the mandate of the 12.865 federal law, the Brazilian Central Bank published a series of regulations[1)] that aim to set the criteria for two separate categories in the PSP environment: payment arrays that are integrated with the Brazilian Payments System (that includes all Brazilian Market Infrastructures) and independent payment arrays. The categories and their regulation requirements are defined by the parameters in Table 3.

1) For research matters, the aforementioned regulations are 3.765, 3.735, 3.724, 3.721, 3.705, 3.682, 3.705, 3.684 and 3.656.

Table 3 — Parameters used to define the payment array categories

Parameter	Initial	From Jan/2018	From Jan/2019
Financial volume (USD millions)	125	62,5	12,5
Number of transactions (millions)	25	12,5	2,5
Funds kept in payment accounts (USD millions)	12,5	6,25	1,25
Number of users (thousands)	2,500	1,250	250

Members of the Brazilian payment system are those that present greater numbers (for 12 consecutive months) than one or more of the listed parameters. Payment arrays that do not exceed the following numbers are considered independent payment arrays.

4.4.2.2 Independent payment arrays

A payment array that exceeds the values listed in Table 3 can also be considered an independent payment array when the array is destined to entities from the same partnership or for entities that clearly present the same visual identity, such as franchises.

Even though, in this modality, PSPs are not considered members of the Brazilian payment system, they are entitled to deliver the following information for the Brazilian Central Bank:

— the nomination of a director to be responsible for the quality of the information;

— the purpose of the payment array;

— a brief description of the characteristics of the array;

— all statistics regarding each parameter listed in Table 3.

4.4.2.3 Payment arrays members of the Brazilian payments system

Payment arrays that are included in the Brazilian payments system are expected to fulfil all responsibilities of an independent payment array and are subject to further direct controls from the Brazilian Central Bank. According to the Central Bank of Brazil's regulation, a payment array that meets the criteria to be considered a Brazilian payments system member must possess capacities to establish procedures that contemplate the following:

— transparent and accessible risk-management rules and procedures for its participants;

— minimal operational aspects in order to prevent:

  — illicit foreign exchange operations, money laundry and terrorism funding,

  — continuity,

  — business continuity plans,

  — information security management,

  — information conciliation between participants, and

  — service availability;

— minimal provision of information by the PSPs to the end-users;

— fraud monitoring within the array;

— settlement between all PSPs within the array;

— interoperability between participants;

— interoperability between payment arrays.

In this sense, Brazilian regulation rules are focused majorly not in the diversity of the PSP environment but more so towards the interoperability in and between payment arrays. This occurs as a natural trend of the Brazilian Central Bank in ruling towards the end-user, in this case, a merchant or the end consumer.

The modalities adopted by each payment array (and consequentially the relationship between the market participants, i.e. financial institutions, PSPs and TPPs) are not limited by the Brazilian Central Bank regulation, and are accessed ad hoc, through the documentation that is presented to the regulator. This means that payment arrays can have different purposes, scopes, rules, settlement methods, deadlines, risk identification, fares, etc.

Regarding oversight, the Brazilian Central Bank reserves the right to request, when needed, the statistics reports, the list of participants and their activities, fraud registries, dispute resolution registries and audit registry. This oversight can be outsourced if determined by the regulator.

4.4.2.4 Third-party payment service providers

According to Brazilian regulation, TPPs inherit all responsibilities of the contracting institution services that are being handled by the TPP in question. This includes measures regarding integrity, reliability, security and confidentiality of the services provided, as well as to full compliance with laws and regulations applicable to the services being handled.

4.4.2.5 Conclusions and future landscape

There are no distinctions between PSPs and other participants (regulation-wise) within a payment array. TPPs are prone to answer to all rules and regulations that are set to all array participants. All arrays are susceptible to Central Bank monitoring, and the regulator, in an ad hoc basis, assesses each modality. Due to the incipient nature of this payment environment in Brazil, there is still little regulation that rule over specific modalities.

The Brazilian regulators are frequently hosting events regarding the so-called "new" payment networks in order to understand and draw a comprehensive regulation in this market. There are some specific sectors within this market that the Central Bank has expressed more concern (i.e. mobile banking and mobile payments).

For the time being, it seems likely that the Brazilian Central Bank will monitor the development of the "new" payment networks and the instauration of new actors (such as account servicing payment service providers) within the industry.

4.4.3 USA

4.4.3.1 General

TPPs have limited direct access to the payments system in the US. There are only a few TPPs that have direct access to the low-value automated clearing house (ACH) system. Primarily, these would be large payroll processors. To have this direct access, the TPP would have to be sponsored by the financial institution that will settle the activity of the TPP; essentially, this TPP is a client of the financial institution. Financial institutions are required to register direct access TPPs in a National Automated Clearing House Association (NACHA) registry. NACHA is the industry organization that maintains the rules and standards for the ACH network. All financial institutions are required to submit a statement to NACHA about whether they have direct access clients; this is considered prudent because it requires all originating financial institutions to actively consider whether or not the rule applies to them. The files sent by the TPP directly to the ACH market infrastructure operator are encrypted and authenticated. The sponsoring bank is responsible for addressing any encryption/authentication issues, compliance requirements and end-of-day settlement positions.

There are other TPPs who do not have direct access to the ACH network. They send, encrypted and authenticated, origination files to their bank, which then delivers them to the ACH network for processing. NACHA has a pending rule proposal which will be balloted later this year that will require

originating banks to register these TPP clients in a manner similar to what is required for direct access clients. This proposed rule will require a third-party sender to disclose to its originating financial institution any of its customers that are also third-party senders (also known as "nested" relationships). The intent behind the proposed rule is to ensure that all originating banks review existing relationships to confirm whether or not they have third-party sender relationships, so that institutions will be in a better position to manage the risks associated with third-party relationships.

Regardless of the type of third-party relationship (direct access or delivering files through a financial institution), FinCEN Regulation 2006-39 requires due diligence by financial institutions which maintain these types of relationships. The TPP is required to perform their own business validation and Know-Your-Customer (KYC) [and know your customer's customer (KYCC)] reviews. The financial institutions that maintain these types of third-party relationships are required to conduct periodic audits to ensure that these reviews by the TPPs are being done in a satisfactory manner.

For the high-value wire transfer business, third-party relationships and access are not typical.

4.4.3.2 Yodlee

Yodlee is a US-based organization, whose platform allows consumers insight into their finances, including "projected" cash balances based on future, scheduled payments. Yodlee solutions are private labelled and available in hosted or enterprise software editions to financial institutions worldwide. Payments are stored in Yodlee's Payment Warehouse and routed to the appropriate end points, including a proprietary Direct Payment engine, which facilitates payments directly at biller websites or via connections to third-party payment service providers. The Yodlee platform facilitates a number of AIS-type providers to access customer account data. This is done with bilateral arrangements in place with financial institutions. Yodlee will collect (or "scrape") account information from an online banking platform, then save it on Yodlee's servers. Yodlee's data (both the direct bank feeds and its screen scrapes) are updated many times a day and may even be real-time.

4.5 Oceania — Australia

Australia does not have specific legislation that governs the operations of third-party access providers. General consumer and competition legislation provides protection for consumers and businesses and a voluntary ePayments Code deals with the rights of consumers in relation to electronic and online banking.

The key provisions of the Competition and Consumer Act (2010) (administered by the Australian Completion and Consumer Commission) state that in terms of unilateral conduct, it is prohibited for a party with a substantial degree of market power to take advantage of that power for the purpose of eliminating or substantially damaging a competitor, preventing the entry of a person into any market or deterring or preventing a person from engaging in competitive conduct (misuse of market power).

In terms of conduct involving two or more parties, it is prohibited to agree, or give effect to, an agreement that has

— the purpose of restricting the supply (or acquisition) of goods or services, in relation to which those parties compete (exclusionary conduct), or

— the purpose, or would be likely to have the effect, of substantially lessening competition (anticompetitive conduct).

The ePayments Code, administered by the Australian Securities and Investments Commission (ASIC), is a voluntary code that regulates consumer electronic payments including ATM, EFTPOS and credit card transactions, online payments, internet and mobile payments and BPAY.

NOTE 1 Electronic funds transfer at point of sale (EFTPOS) is an electronic payment system involving electronic funds transfers based on the use of payment cards, such as debit or credit cards, at payment terminals located at points of sale.

NOTE 2 BPAY is an electronic bill payment system in Australia which enables payments to be made through a financial institution's online, mobile or telephone banking facility to organizations which are registered BPAY billers. BPAY is a registered trading name of BPAY Pty Ltd, a wholly owned subsidiary of Cardlink Services Limited. Cardlink is owned equally by the four major Australian banks: Australia and New Zealand Banking Group Limited, Commonwealth Bank of Australia, National Australia Bank Limited and Westpac Banking Corporation.

The rules governing liability and customer liability are set out by the ePayments Code in Chapter C. Under Section 11, customers who contribute to fraudulent activity through breach of terms and conditions or negligence are deemed liable for any losses. However, Section 12.9 states that if financial institutions are in any way seen to endorse or facilitate a service that leads to a loss, Section 11 no longer applies and the financial institution is liable. The Code expressly includes, by way of a note, the services offered by account aggregators.

Financial institutions therefore have to balance the risk of being liable for fraudulent activity undertaken through the operations of an account aggregating service or TPP under their ePayments Code obligations with the risk of attracting regulatory interest if account aggregator IP addresses are blocked.

On one level, this is a commercial issue for individual authorized deposit-taking institutions (ADIs); in balancing the risks having regard to commercial objectives, each might take a different approach. The difficulty of balancing competing public policy objectives (promoting competition versus protecting consumers under the ePayments Code) is arguably something on which a coordinated industry position may be desirable.

Authorized deposit-taking institutions (ADIs) are organizations that come under the regulation of the Australian Prudential Regulation Authority (APRA). Any institution or business that holds and lends moneys needs to be licensed by APRA (see Reference [11]).

The Australian Payments Clearing Association (APCA), the self-regulatory body for payments under the ultimate regulatory supervision of the Reserve Bank of Australia, is currently investigating whether there is scope for an industry-led solution that would provide a degree of regulatory certainty for third-party payment service providers, financial institutions and the payments system as a whole. This is based on the view that industry-based solutions are preferable to government-imposed regulation.

Australia's payments system currently operates on a bilateral network, which means that TPPs may need to make individual arrangements with authorized deposit-taking institutions to access customer accounts. At this stage, there are a few operators which engage in facilitating the transferring of funds from savings accounts to either merchants or investment portfolios, as well as some account aggregators which obtain data for consolidation. At least one of these contracts with some authorized deposit-taking institutions to ensure their IP addresses are not blocked when accessing customer accounts and another has a commercial agreement with one financial institution to provide account aggregation services.

4.6 Africa — South Africa

The South African Reserve Bank allows the TPP to undertake the following[12]:

a) money or the proceeds of payment instructions are accepted by a person (a beneficiary service provider), as a regular feature of that person's business, from multiple payers on behalf of a beneficiary (a typical example being the acceptance of money or proceeds of payment instructions by a retailer or other outlets for payment of utility bills);

b) money or the proceeds of payment instructions are accepted by a person (a payer service provider), as a regular feature of that person's business, from a payer to make payment on behalf of that payer to multiple beneficiaries (a typical example being the payment of salaries on behalf of employers to employees).

