



Instant Payments: Webinar for Risk & Fraud Managers

Christopher Koch, Project Head SIC5
Bruno Kudermann, Senior Product Manager
Romano Ramanti, Certified Ethical Hacker

February 28, 2024



Agenda

01

Introduction

- › Goal of todays webinar
- › Timeline IP Service
- › Action required by SIC participants

02

How the SIC IP Service works

- › Basic principles of the SIC IP Service

03

IP: Learning from other countries

- › Main challenges Instant Payments
- › Example from the UK
- › EU Regulations
- › PAV
- › Overview Fraud Working Groups

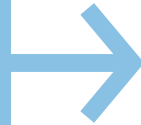
04

Discussion

Goal of Today's Webinar

Situation

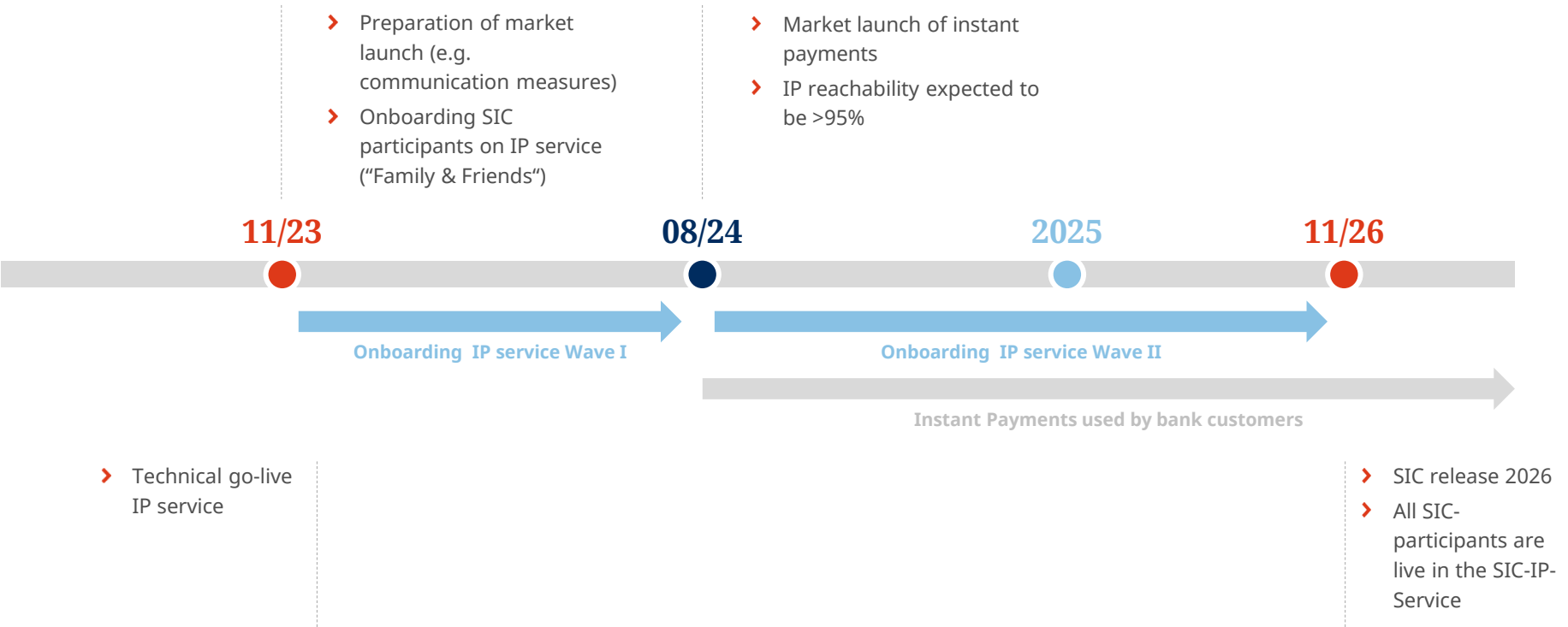
- As of August 2024, Instant Payments will be a reality also in Switzerland
- The introduction of the new Instant Payment service (IP Service) requires changes at all participating institutions
- We have heard from market participants that especially in the area of risk and fraud management there is not yet full clarity on the impact of instant payments



Goal

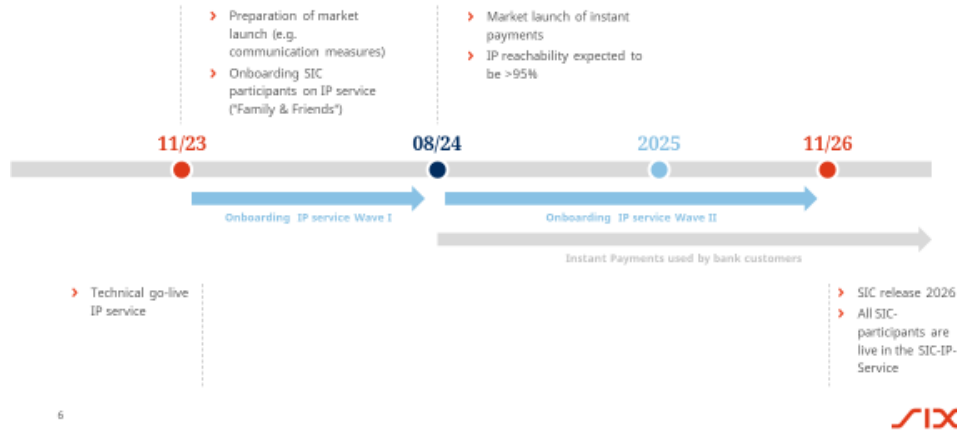
- Participants know the timeline of the introduction of Instant Payments in Switzerland
- Participants understand what the difference is between Instant Payments and (traditional) RTGS-Payments
- Participants can evaluate the potential impact of Instant Payments to their organisations in respect to Fraud and Risk Management and know where they can obtain further information

Instant Payment Are Live!



Be Prepared: Volume of Instant Payments Will Increase as of August 2024

Instant Payment Are Live!



Market launch August 20, 2024

- Up until August, some 65 SIC participants are expected to onboard onto the IP Service
- As of August, we expect a significant increase in Instant Payment Transactions, as a number of SIC participants have indicated that they will also have client offerings
- SIC participants are advised to ensure that processing of Instant Payments can be performed, including all related services such as fraud and risk management aspects

Agenda

01

Introduction

- › Goal of today's webinar
- › Timeline IP Service
- › Action required by SIC participants

02

How the SIC IP Service works

- › Basic principles of the SIC IP Service

03

IP: Learning from other countries

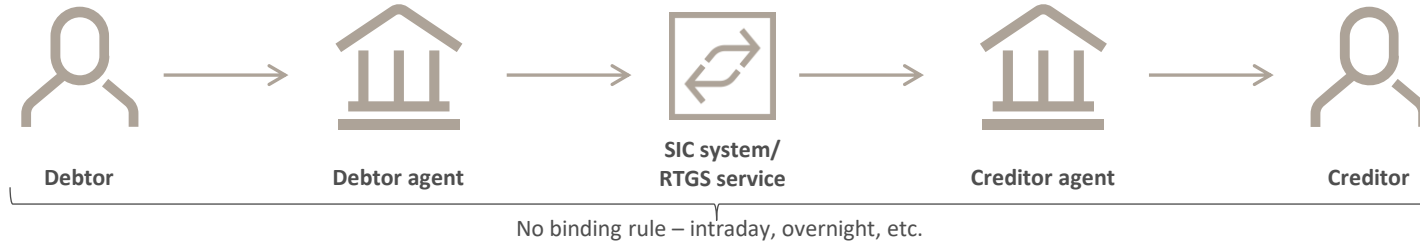
- › Main challenges Instant Payments
- › Example from the UK
- › EU Regulations
- › PAV
- › Overview Fraud Working Groups

04

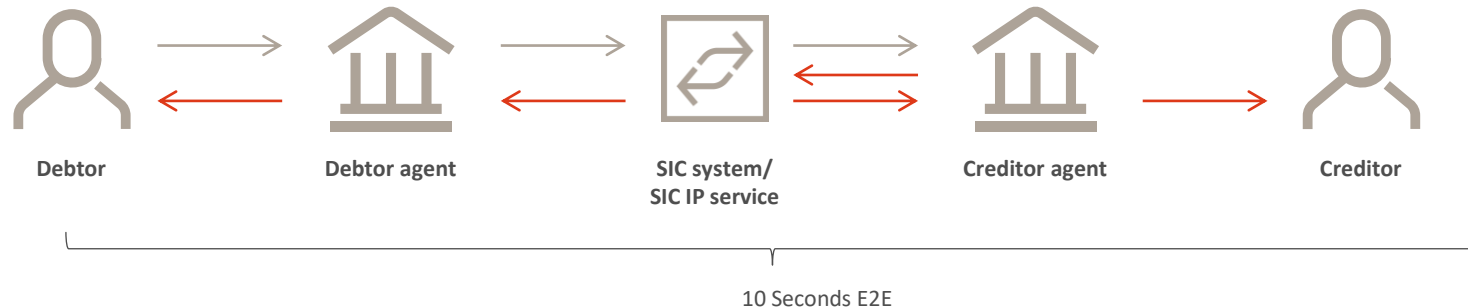
Discussion

Instant Payments Flow Differs from RTGS Flow

RTGS payments flow



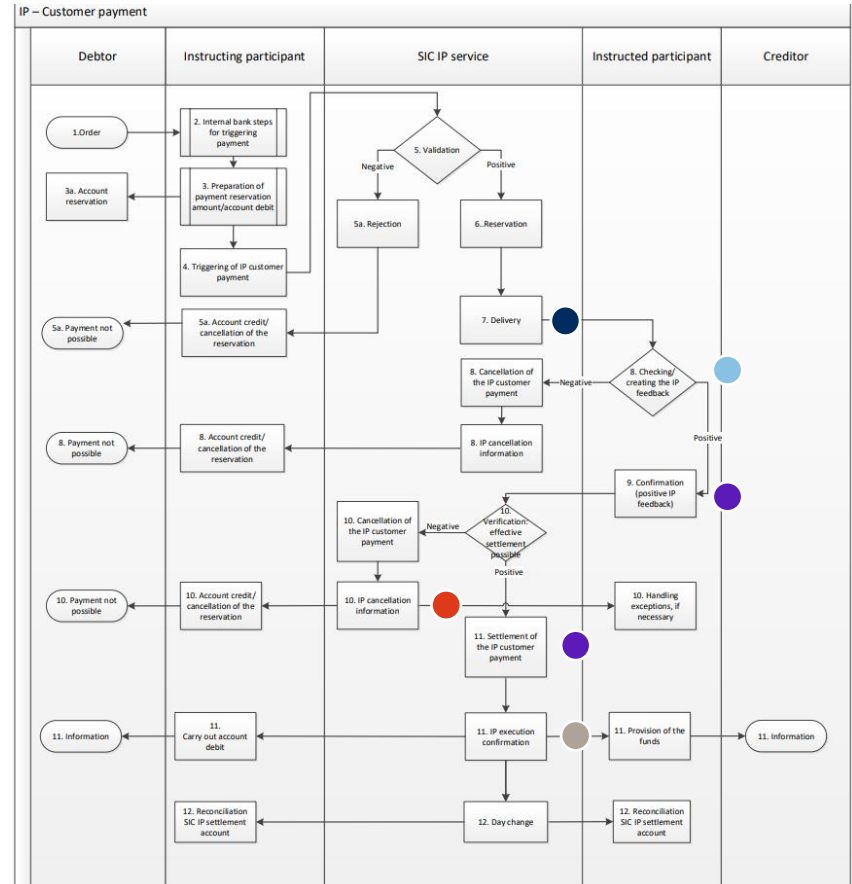
Instant payments flow






Market Launch
2024.08.20




Important Steps for Instant Payments

- Payment delivery happens before settlement
- Checks necessary before giving positive IP-Feedback
- Positive IP-feedback triggers Settlement
- IP-execution information is the confirmation that settlement took place
- No Feedback after max 20 sec. = cancellation



FI's Do Not Have Much Time for Checks....

-  Checks necessary before giving positive IP-Feedback
-  Positive IP-feedback triggers Settlement
-  No Feedback after max 20 sec. = cancellation

Party	Max. time in sec.	Total in sec.	Time-out deadline in sec.	Parameter or note
Instructing participant	3	3		Maximum time for instructing participants
SIC IP service	2	5	Start time > 3 sec.	SIC Acceptance Time Out
Instructed participant	4	9	Start time > 5 sec.	Participant Acceptance Time Out 
Instructed participant	0.5	9.5		Time to create positive or negative IP feedback 
SIC IP Service	0.5	10		Standard Execution Time In the standard process, a maximum of 10 seconds may elapse between the start time and the time at which the IP execution confirmation is received by the instructing participant. 
Instructed participant	10	20		Maximum Execution Time 
SIC IP Service			Start time > 20 sec.	Hard Time Out On reaching the deadline: cancellation due to "Hard Time Out"
SIC IP Service	5	25		Overall Execution Time Time window for sending the IP execution confirmation or IP cancellation information

Informations Are Available Online

SIC5

08 NOV 2023 - ENTRY INTO FORCE DATE: 20 NOV 2023

FAQ – Instant payments

Version 1.0

[Open document](#)

20 OCT 2023

SICS Project Phase 2

Version 1.0

[Open document](#)

29 SEP 2023

Registration for onboarding in the productive SIC IP service

[Open document](#)

03 JUL 2023


Information about the acceptance and integration tests in SIC IP service

Version 1.0

[Open document](#)

Handbooks


28 FEB 2024

 **SIC IP Service Handbook**

Version 2.2, valid from 20 February 2024

[Message flow diagrams from chapter 8 \(ZIP\)](#)


29 FEB 2024

 **SIC IP Service: External Test Environments and Onboarding**

Detailed Information – Version 2.1

[Example CSV upload from chapter 6](#)

15 SEP 2023 - ENTRY INTO FORCE DATE: 05 SEP 2023

 **Test Case Specification for the SIC IP Service**

Version 1.1

Contact Details of SIC5 Software Partners

Information about the categories can be found below the table.

Company	Categories	Link, E-Mail
Avastq Evolution AG	Banking Software Provider	www.avastq.com info@avastq.com
Acquire SA	Service Bureau	www.acquire.com albin.kury@acquire.com
Bottomline Financial Messaging	Banking Software Provider Banking Software Operator Service Bureau	www.bottomline.com lgurnas@bottomline.com
EFIS Swiss AG	Service Bureau	www.efiswiss.com info@efiswiss.com
Ergon Informatik AG ¹	Banking Software Provider	www.ergon.ch rafael.kalwender@ergon.ch
Finastra Switzerland GmbH	Banking Software Provider Service Bureau	www.finastra.com
Finova AG	Banking Software Provider	www.finova.com andrea.trevisan@finova.com
FIS (Fidelity Information Services LLC)	Banking Software Provider	www.fisglobal.com gru.mironov@fis.com
Headlight GmbH ¹	Banking Software Provider Banking Software Operator	www.headlight.de info@headlight.de
Hypothekbank Lenzburg AG ¹	Banking Software Provider Banking Software Operator Service Bureau	www.hbl.ch bernd.moser@hbl.ch
Icon Solutions Ltd	Banking Software Provider	www.iconsolutions.com info@iconsolutions.com
Incentage AG	Banking Software Provider	www.incentage.com info@incentage.com
INTERCOPE International Communication Products Engineering GmbH	Banking Software Provider	www.intercope.com buenden@intercope.com
Logsoft AG	Banking Software Provider	www.logsoft.ch info@logsoft.ch
Mtg GillardentM AG	Banking Software Provider	www.mtg-gillardentm.de info_banking@mtg-group.com
WPE	Banking Software Provider	www.pgi.asteris.ch info@ppi.schweiz.ch
Swit ⁴	Banking Software Provider	www.swit.com AMM-GSK.partners@swit.com
Swisscom (Schweiz) AG	Banking Software Operator Service Bureau	www.swisscom.ch/de/business.html blago.ueber@swisscom.com
Tata Consultancy Services Switzerland Ltd	Banking Software Provider Banking Software Operator	www.tcs.com/names u.s.maler@tcs.com
Worldline (Schweiz) AG	Banking Software Provider Service Bureau	www.worldline.com pietra.zalwer@worldline.com

Agenda

01

Introduction

- › Goal of todays webinar
- › Timeline IP Service
- › Action required by SIC participants

02

How the SIC IP Service works

- › Basic principles of the SIC IP Service

03

IP: Learning from other countries

- › Main challenges Instant Payments
- › Example from the UK
- › EU Regulations
- › PAV
- › Overview Fraud Working Groups

04

Discussion

Instant Payment and Fraud

Romano Ramanti, 28.02.2024



Main Challenges Instant Payment

Instant Payment = Instant Fraud

- Since the introduction of instant payment, fraud cases have increased massively
- Availability 24/7/365
- PSPs can agree between themselves on a shorter execution time
(Example Netherland – Instant Payment within 5 seconds)
- Increased payment volume
- Fraud Detection Systems need to be adapted
- EU is pushing instant payment
- Redirect of payments to additional money mules increased
- Shift from credit cards to instant payments

Faster Payments Service Fraud – Example from the UK

In 97% of the fraud cases Faster Payments was used

The U.K. has been experiencing a widespread payments fraud epidemic in recent years.

Authorized push payment (APP) fraud, for example, increased 40% between 2020 and 2021 and amounted to £583 million (\$706 million) in losses in 2021, nearly half of the £1.3 billion (\$1.57 billion) lost to overall fraud incidents that year, per UK Finance.

Pay.UK on Striking the Balance Between Fast and Friction in Stopping UK Fraud Epidemic

The Payment Systems Regulator (PSR) is committed to fighting APP fraud and, in a world first, we are introducing a new reimbursement requirement. We are:

- incentivising the payment industry to invest further in end-to-end fraud prevention by making every payment firm meet the cost of reimbursing
- increasing customer protections so most victims of APP fraud are swiftly reimbursed, boosting confidence in the UK payment ecosystem
- pursuing our long-term ambition for Pay.UK to take on a broader role and actively improve the rules governing Faster Payments to tackle fraud

2 Sharing the cost of reimbursement. Receiving PSPs must pay sending PSPs 50% of the reimbursement that the sending PSP paid to the customer. A time period will be set by Pay.UK with an ultimate backstop to ensure receiving PSPs reimburse sending PSPs.

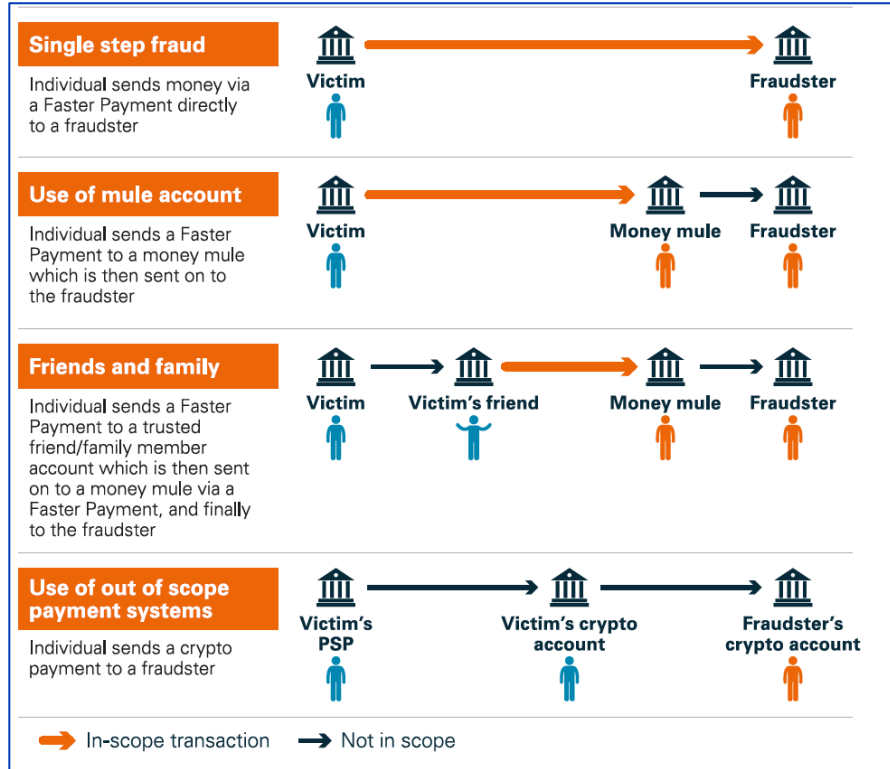
3 Exceptions for APP fraud claims. There are two exceptions to reimbursement (noting the other policies) under the new reimbursement requirement:

Where the customer has acted fraudulently ('first-party fraud')

Where the customer has acted with gross negligence. This is the customer standard of caution for APP fraud claims.⁸

- 8 There is a potential risk that, if customers are more confident of being reimbursed, they will take less care in ensuring that their payee is not a fraudster (the risk of moral hazard). Since we cannot, at present, rule out this risk, as part of our mitigations we have considered an exception to reimbursement to incentivise customers to continue to exercise caution (see Chapter 4, Table 4). This is the customer standard of caution. Gross negligence is a high bar and, where suspected, the burden of proof is on the PSP (see Chapter 5).

In Scope Transaction for Reimbursement



EBA CLEARING issues specifications and runs analytical pilot for pan-European fraud pattern and anomaly detection

Nine banks from six countries are engaged in the data model training for the new fraud-fighting functionality in STEP2 and RT1

EU Regulations

DRAFT COMPROMISES

Payment Services Regulation (PSR)

Draft report on the proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010

11 JANUARY 2023

Proposal for a regulation

Article 59 – paragraph 1

1. Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider **or any other relevant entity of public or private nature** using the name or e-mail address or telephone number of that **payment service provider entity** unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider, **electronic communications service provider or online platform, as applicable**, shall **swiftly take all the necessary measures to eliminate or mitigate the consequences** of the **fraud** and refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, **submitted documentation to prove the**

1 b. All providers involved in the fraud chain shall act swiftly to ensure that the appropriate organisational and technical measures are in place to safeguard the security of payments users when making transactions. Payment service providers, electronic communication service providers and digital platform service providers shall have in place fraud prevention and mitigation techniques to fight fraud in all its configurations, including non-authorized and authorized push payment fraud.

Proposal for a regulation

Article 83 – paragraph 3

3. To comply with paragraph 1, point (c), payment service providers **shall** exchange the unique identifier, ***name, personal identification number, organisation number, modus operandi and other transaction information*** of a payee with other payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, when the payment service provider has sufficient evidence to assume that there was a fraudulent payment transaction. Sufficient evidence for sharing unique **information** shall be assumed when at least two different payment services users who are customers of the same payment service provider **or a consumer organization** have informed that a unique identifier of a payee was used to make a fraudulent credit transfer. Payment service providers shall not keep **information** obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c).

Proposal for and Instant Credit Transfer Regulation



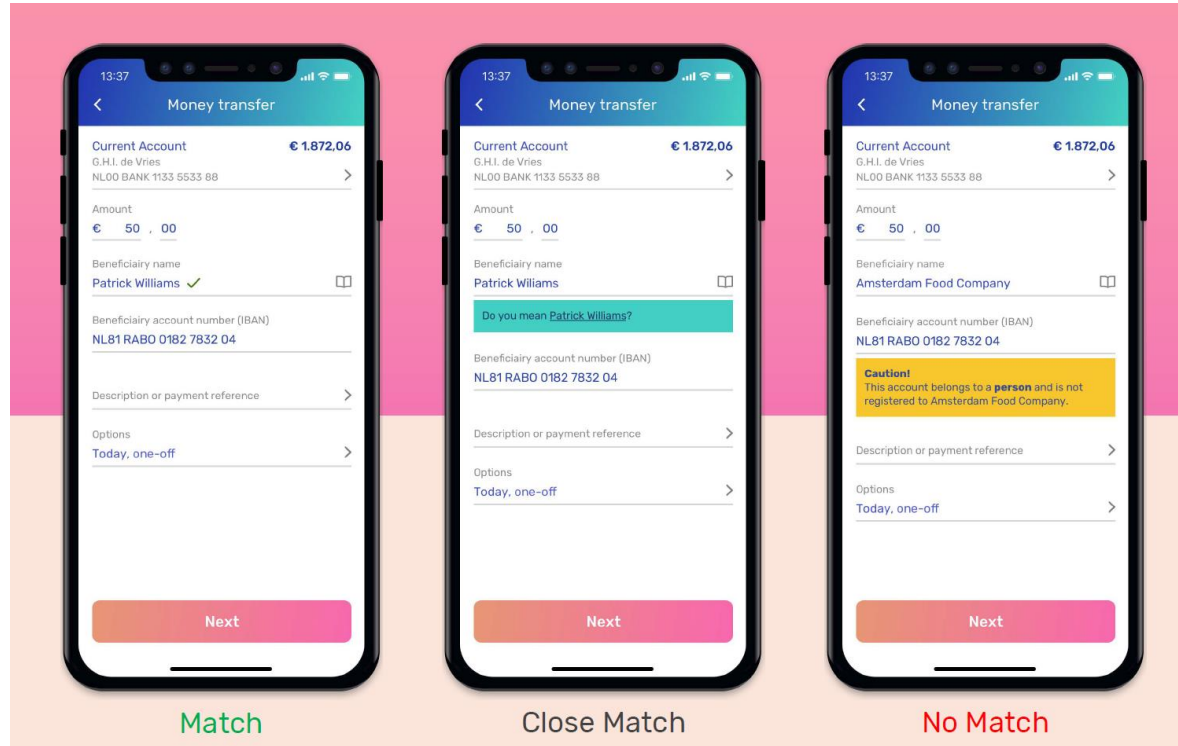
a requirement for PSPs to offer a service enabling customers to be notified when a mismatch is detected between the payee's name and international bank account number (IBAN), as supplied by the payer;

The European Parliament has formally approved legislation that will force banks and other payment service providers to offer EU citizens and businesses the option of performing virtually instantaneous credit transfers.

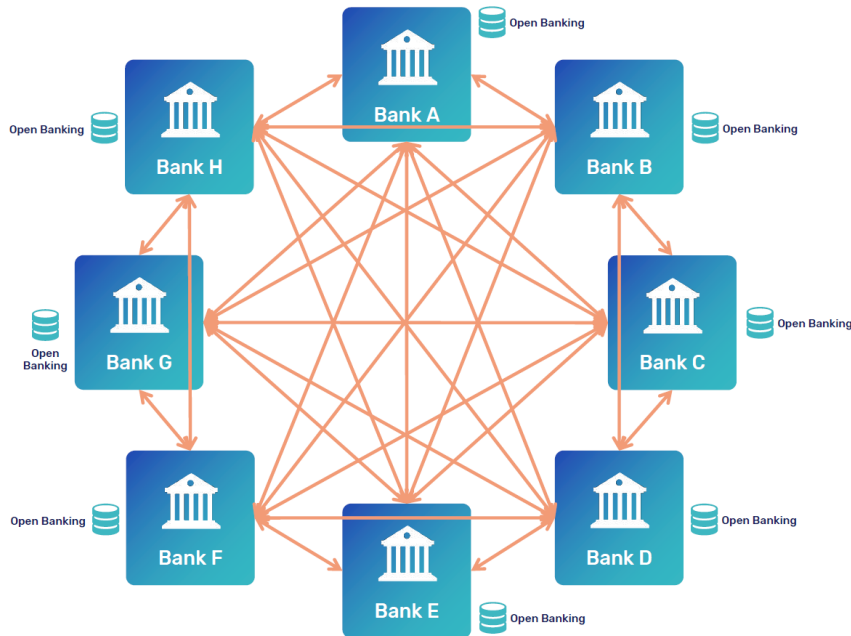
The law, which was passed by an overwhelming majority of MEPs on Wednesday (7 February), follows a Commission [proposal](#) in October 2022 to make so-called “instant payments” available across the EU, as part of wider efforts to deepen the bloc’s [Capital Markets Union](#) (CMU) and strengthen its [strategic autonomy](#).

Payment Account Verification

Payment Account Verification

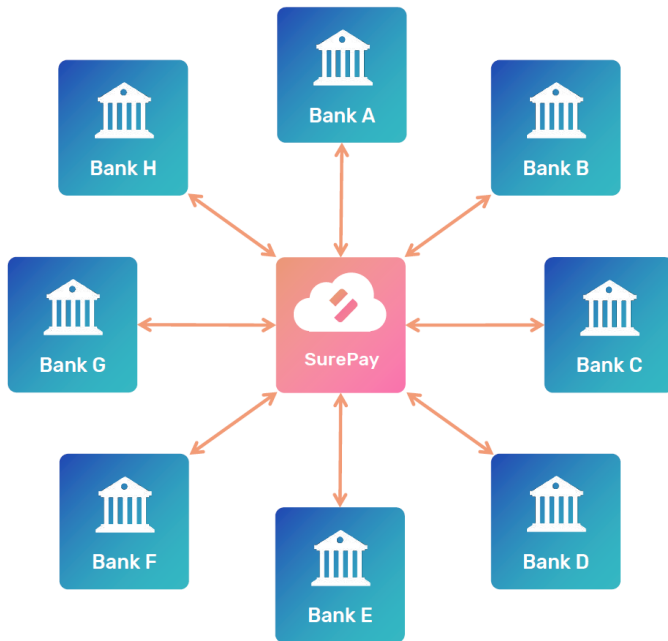


Decentralised matching (UK example)



- ❖ Every bank needs to develop (or buy) and maintain their own algorithm
- ❖ Algorithms behave differently and they don't have equal quality
- ❖ Every bank must onboard with Open Banking and run an authorisation server
- ❖ Every bank needs to onboard every bank in order to be able to send CoP requests to the bank
- ❖ Every bank needs to whitelist every bank in order to accept incoming CoP requests to respond to
- ❖ Every bank needs to solve every edge case, e.g. when an account holder is not the beneficiary

Centralised matching (NL example)



- ❖ Banks don't need to develop and maintain an algorithm, they use the central one that has already proven itself (x3 billion)
- ❖ New banks connect to the central hub for sending and responding; are thereby also connected to every bank
- ❖ Edge cases need to be solved only once
- ❖ Bank customer data doesn't need to be stored centrally
- ❖ Possibilities to discover anomalies or fraudulent behaviour based on matching results across banks (helicopter view)
- ❖ SurePay takes care of connecting to other initiatives, eg SWIFT BAV

Separate PAV (Payment Account Verification) Scheme

- The development of an EPC CoP concept by the CoP TF is done under the form of a standalone EPC scheme;
- A public consultation of three months will be organised for the proposed EPC CoP scheme rulebook subject to the final deadlines set by the EU legislators;
- the PSMB supports the launch for a public Request-for-Proposal (RfP) to select a Directory Service Provider to play the role of a default EPC Operational Service Manager (OSM) to store and maintain all details about future CoP scheme participants;

In a first step the scheme will focus on EU and EEA members only

Working Groups on Fraud

Working Groups

Exchange of fraud-relevant information and patterns

ERFA Zahlungsströme

Participants: Swiss Banks

SwissParticipants: Swiss Banks

Payment Council

SWITCHCert

Participants: Swiss Banks

European Payment Council

- Payment Scheme Fraud Prevention Working Group
- Taskforce Payment Account Verification

Participants: European Banks

SWIFT

Swift Anomaly Detection Working Group



Zürcher
Kantonalbank

Agenda

01

Introduction

- › Goal of today's webinar
- › Timeline IP Service
- › Action required by SIC participants

02

How the SIC IP Service works

- › Basic principles of the SIC IP Service

03

IP: Learning from other countries

- › Main challenges Instant Payments
- › Example from the UK
- › EU Regulations
- › PAV
- › Overview Fraud Working Groups

04

Discussion

Disclaimer

This material has been prepared by SIX Group Ltd, its subsidiaries, affiliates and/or their branches (together, "SIX") for the exclusive use of the persons to whom SIX delivers this material. This material or any of its content is not to be construed as a binding agreement, recommendation, investment advice, solicitation, invitation or offer to buy or sell financial information, products, solutions or services. It is solely for information purposes and is subject to change without notice at any time. SIX is under no obligation to update, revise or keep current the content of this material. No representation, warranty, guarantee or undertaking – express or implied – is or will be given by SIX as to the accuracy, completeness, sufficiency, suitability or reliability of the content of this material. Neither SIX nor any of its directors, officers, employees, representatives or agents accept any liability for any loss, damage or injury arising out of or in relation to this material. This material is property of SIX and may not be printed, copied, reproduced, published, passed on, disclosed or distributed in any form without the express prior written consent of SIX.

© 2024 SIX Group Ltd. All rights reserved.

