ABE EBA

EURO BANKING ASSOCIATION

Participants in the forum are reminded of their responsibility to observe anti-trust laws

The EBA Anti-Trust Policy is available at the EBA website

https://www.abe-eba.eu/media/azure/production/1352/eba_antitrust_policy_20170602_final_clean.pdf

ABE EBA

EURO BANKING ASSOCIATION

The forum is an open group, where interested stakeholders can discuss and exchange information on industry-wide topics.

The content of the slides presented and the views expressed in the context of the activities of the forum are those of the respective participants in the forum, and do not represent the views of the Euro Banking Association (EBA).

ABE EBA
EURO BANKING ASSOCIATION

Open Forum on Digital Transformation

Are fraud and cybercrime creating a significant threat to the financial services community? Join the EBA Open Forum on 11 July to find out how industry initiatives and regulation are helping to master the challenge!

11 July 2024
Digital meeting

Closed user group

Agenda (1/3)

Are fraud and cybercrime creating a significant threat to the financial services community? Find out how industry initiatives and regulation are helping to master the challenge!

Welcome and opening remarks
Thomas Egner, Euro Banking Association

Setting the scene and housekeeping
Kate Pohl, Projective Group

Are fraud + cybercrime creating a significant threat to the financial services community? How industry initiatives and regulation are helping to master the challenge
Andrea Radu, Deloitte
Georges Gehchan, Deloitte

Ethical hacking for financial stability
Dr. Miriam Sinn, Deutsche Bundesbank

Coffee Break

Agenda (2/3)

Are fraud and cybercrime creating a significant threat to the financial services community? Find out how industry initiatives and regulation are helping to master the challenge!

Fraud and cybercrime are today's reality… but what is the industry doing about it? A view from various experts
Dr. Boris Hemkemeier, Commerzbank
Hays Littlejohn, EBA CLEARING
Alvaro Azofra Martinez, Europol
Jan Osenegg, Senior Advisory
David-Jan Janse, SurePay
Brigitte De Wilde, SWIFT
Jörg Wiemer, TIS

What is the Fraud Taxonomy and how can it be implemented by banks? Learnings and best practices
Helene Gertsen, Danske Bank
Annick Moes, Euro Banking Association

Lunch Break

Agenda (3/3)

Are fraud and cybercrime creating a significant threat to the financial services community? Find out how industry initiatives and regulation are helping to master the challenge!

Regulations and regulatory compliance: what are the key themes and issues today? Looking at regulation from a legal perspective
Marcus Columbu, act AC Tischendorf Rechtsanwälte Partnerschaft mbB

The new Instant Payments Regulation: what we know and what is still in the grey zone… reading between the lines
Roderick Kroon, Projective Group

Coffee Break

What is Verification of Payee? Why is it important? And what still needs to be done
David Renault, EBA CLEARING
Ronny Wolf, Commerzbank

Regulating the fraud chain in payments – what is to be expected?
Dr. Matthias Terlau, Görg

Wrap-up

Thomas Egner

Secretary General
Euro Banking Association

ABE EBA
EURO BANKING ASSOCIATION

Kate Pohl

Executive Advisor
Projective Group

ABE EBA
EURO BANKING ASSOCIATION

Andrea Radu

Partner – Financial Services
Deloitte

Georges Gehchan

Senior Manager Cyber Security Strategy
Deloitte

ABE EBA
EURO BANKING ASSOCIATION

Dr. Miriam Sinn

Head of TIBER Cyber Team
Deutsche Bundesbank

ABE EBA
EURO BANKING ASSOCIATION

DEUTSCHE BUNDESBANK EUROSYSTEM

TIBER-DE

Hacking for financial stability!

Miriam Sinn, Head of TIBER Cyber Team Germany

TIBER-DE


RANSOMWARE ATTACK
Your personal files are encrypted
You have 5 days to submit the payment!!!
To retrieve the Private key you need to pay
Your files will be lost

What does the Bundesbank have to do with hackers?

Image: Pixabay

How can we test cyber resilience?

TIBER-DE

Penetration Testing

Red Teaming

TIBER

Increasing intensity

Image: Pixabay

TIBER-DE – Testing Process
Participants in a TIBER-DE test

TIBER Cyber Team - Referee

- Checks and attests compliance with TIBER framework
- Point of contact for the White Team
- Interface to external stakeholders

Tested entity

White Team - Manager

- Main point of contact and decision taker
- Monitoring and risk management

Threat Intelligence provider - Spy

- Collects targeted threat intelligence
- Drafts attack scenarios

Red Teaming provider - Attacker

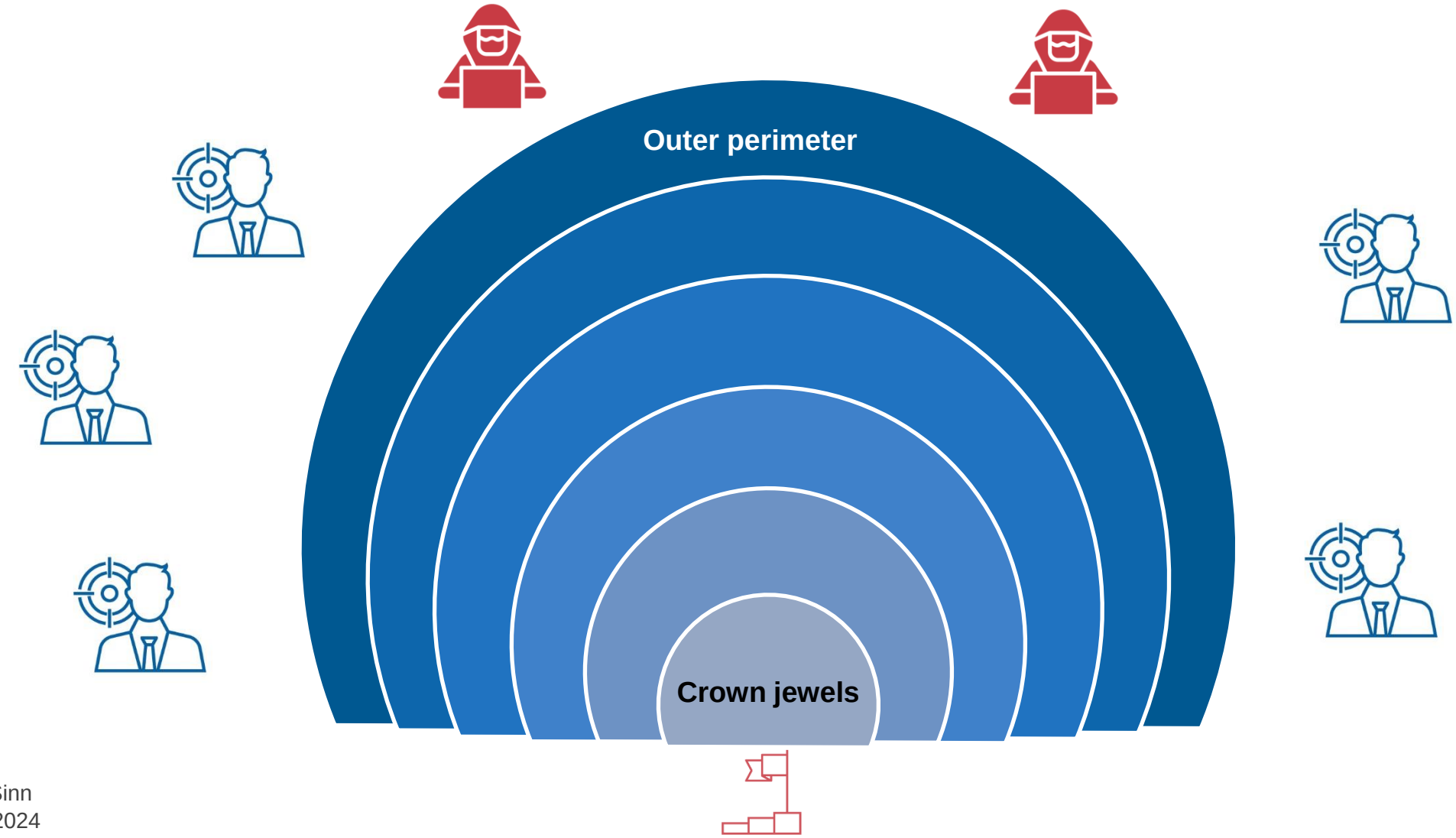
- Implements attack scenarios using threat intelligence

Blue Team - Defender

- Cyber defense (SOC/CERT)
- All employees outside of the White Team
- Not informed about the test

All lines of defence are put to the test

TIBER-DE



And what did we learn?

or

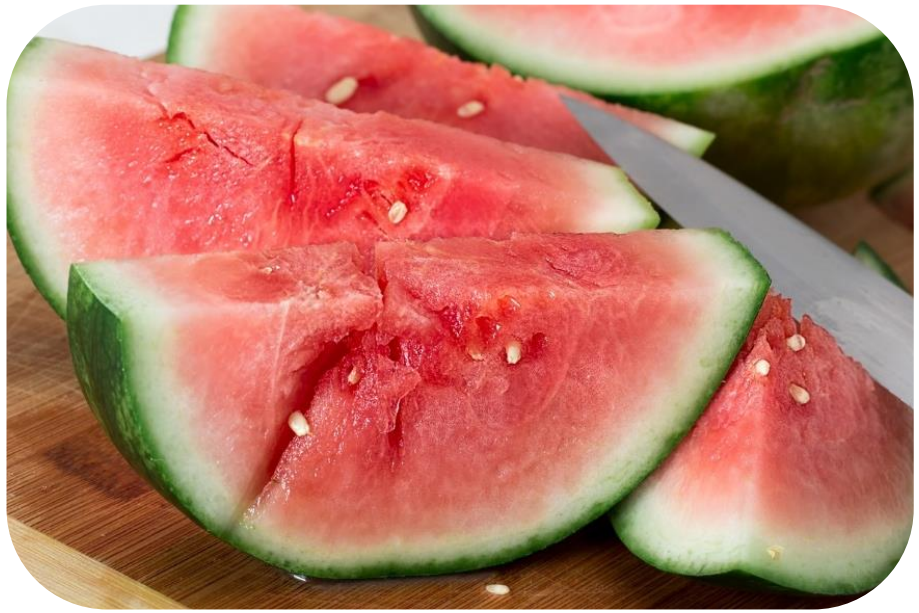


Image: Pixabay

Stories from every day life

TIBER-DE

1

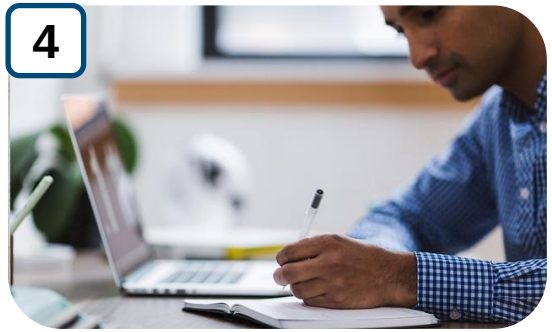
3

5

7

2

4



6

8

Bilder: Pixabay

The world of tomorrow

TIBER-DE

Thank you for your attention!

TIBER Cyber Team

Deutsche Bundesbank
Wilhelm-Epstein-Straße 14
60431 Frankfurt am Main

E-Mail: tiber@bundesbank.de

www.bundesbank.de > Aufgaben > Unbarer Zahlungsverkehr > TIBER-DE

ABE EBA
EURO BANKING ASSOCIATION

Coffee Break
10:20 – 10:35 CET

During coffee break, do not “leave the meeting”
(i.e., stay connected while muting your sound and turning off your camera)

Panel Discussion

ABE EBA
EURO BANKING ASSOCIATION

Annick Moes

Head of Industry Issues and Cooperation Initiatives
Euro Banking Association

Helene Gertsen

Senior Analyst

Danske Bank

ABE EBA
EURO BANKING ASSOCIATION

ABE EBA
EURO BANKING ASSOCIATION

Do you speak fraud?

How the EBA Fraud Taxonomy can help cooperation against fraud

Annick Moes
Euro Banking Association

EBA Open Forum: “Are fraud and cybercrime creating a significant threat to the financial services community?”

11 July 2024

How the EBA Fraud Taxonomy can help fight fraud

European regulators are currently preparing the ground for the introduction of fraud data sharing solutions

European Commission proposes to “combat and mitigate payment fraud, by **enabling payment service providers to share fraud-related information between themselves**”

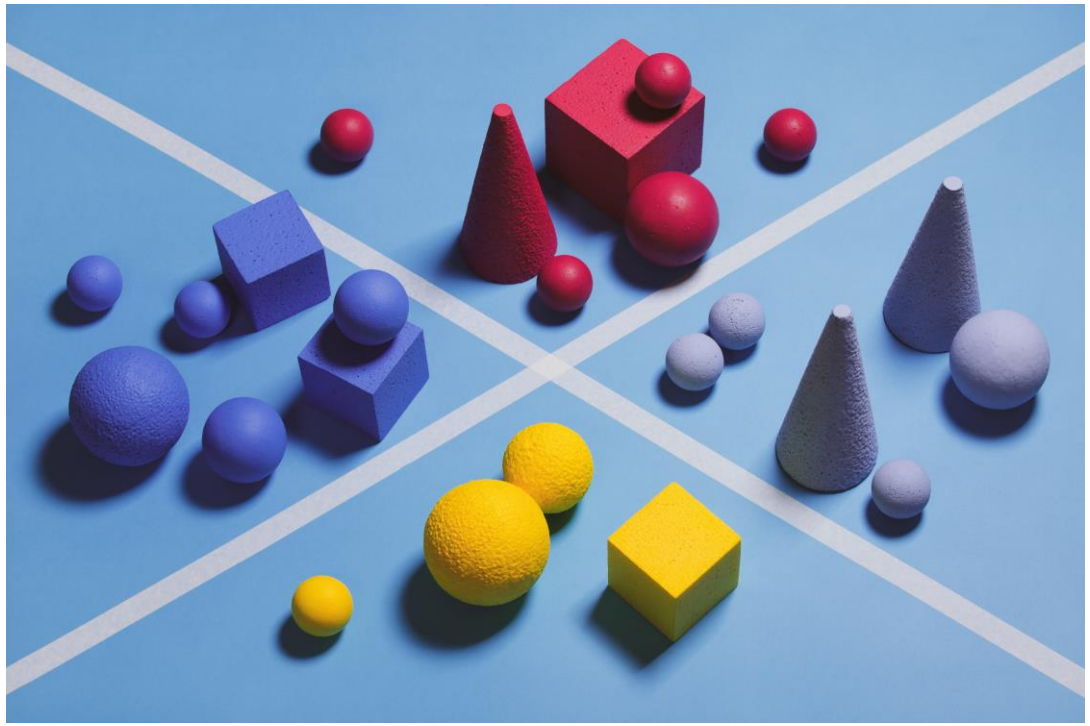
(European Commission press release ‘Modernising payment services and opening financial services data: new opportunities for consumers and businesses’, 28 June 2023)

European Banking Authority advises EU co-legislators and EU Commission to consider strengthening “the PSR proposal with a requirement to have a **single EU-wide platform, to be maintained and run by PSPs**, **for the sharing of fraud data** amongst PSPs”.

(European Banking Authority opinion on new types of payment fraud and possible mitigants, April 2024)

What is the EBA Fraud Taxonomy?

Definition and objective



EBA Fraud Taxonomy

Equips fraud fighters with a pan-European vocabulary and categorisation approach for **naming and organising fraud types** for payments, including card payments

Implementation of the EBA Fraud Taxonomy means

- **one vocabulary set** for European PSPs
- **granular, actionable and comparable data** on payment fraud

Why is the EBA Fraud Taxonomy better?

How does it make a difference?

Top benefit

The common vocabulary and categorisation approach enable European PSPs to join forces in the fight against payment fraud.

Other benefits

- Created and evolved by **30+ fraud experts from 15 European countries**, based on annual change process
- Applies to both **payment fraud and card fraud**
- Relies on **definitions from authoritative and publicly available sources**, wherever possible
- **Aligned with EBA Fraud Reporting Guidelines** under PSD2
- Allows **describing any payment fraud event in a concise manner** based on a standardised approach
  - supporting **easier and faster data point collection**
  - increasing **accuracy and comparability of fraud trend intelligence and data**
  - enabling PSPs to develop **effective fraud prevention campaigns** for their customers
- Can be used by any interested party (request your **free** copy at https://www.abe-eba.eu/publications/)

How does the taxonomy work? Capturing the ‘how’, ‘what’, ‘who’ and ‘what else’

Explaining the different elements

How?

Method:
First point of contact between the fraudster and the victim or the point of compromise

What?

High-level classification:
Indicates strategic approach taken by the fraudster

- Narrative deployed by fraudster that triggers the desired reaction by the victim
- Account takeover by unauthorised party
- First party fraud

Modus:
What trick the fraudster used

- Unauthorised and often manipulative action taken by fraudster

Who?

Initiator of payment transaction (customer or fraudster or 1st party)

What else?

Label/tag:
Additional information to enrich the case – ensures ease of use and maximum flexibility

Payment instrument (optional)

Enables users of the taxonomy to identify whether the fraudulent payment was an account-to-account transaction or a card payment

How does the taxonomy work? Capturing the ‘who’, ‘how’, ‘what’, and ‘what else’

From fraud case to fraud type

Who?

Initiator of payment transaction:
Customer

How?

Method: **Phone contact**

Fraud case description

Fraudster calls bank customer and tells him that she represents his bank

Fraudster tells customer that the bank identified several unauthorised transactions to be debited from customer’s account

Fraudster convinces customer to transfer his funds to a “safe account” indicated by fraudster

What else?

Label/tag:
Fake bank / financial institution Impersonation

What? (and why?)

Why? High-level classification: **“Your money/personal information is at risk”**
What? Modus: “Safe account fraud”

“You’ll usually [be] contacted by someone saying they are from the bank or the police. They’ll (…) ask you to transfer your money to a “safe account” they have set up on your behalf. The account will belong to a fraudster.”

Source: Barclays Bank UK ‘Ten common types of fraud and scam – 9. Safe account fraud’

How does the EBA Fraud Taxonomy ensure better data?

Data quality beats data quantity (but it's good to have both)

Separating the contact methods ("how") used by fraudsters from the actual tricks they apply ("what")

- Better data quality and more granular data, e.g. separate data points on entry door taken and trick applied

Traditional approach	EBA Fraud Taxonomy approach	
No separate categorisation of 'how' and 'what'; no granularity on 'what'	Separate categorisation of method ('how')	Separate categorisation and precise identification of ('what')
Phishing	E-mail contact	E.g. Phoney debt/bill collection
Smishing	Text message contact	E.g. Fake institution
Vishing	Phone contact	E.g. Safe account fraud

EBA Fraud Taxonomy captures complex fraud strategies

The taxonomy identifies the strategic approach taken by the fraudster

Overview of modi

"Your money / personal information is at risk"
- Safe account fraud
- Stop unauthorised transaction fraud
- Stop unauthorised access fraud

"You can earn/save a lot of money"
- Advance fee fraud
- Claim a benefit fraud
- Investment fraud

"I am a seller/buyer"
- Online shopping fraud

"Please help me"
- Emotional manipulation

"Send me money or I'll …"
- Extortion

"We've changed account number"
- Impersonation of creditor

"You owe money"
- Overpayment fraud
- Phoney debt/bill collection

"Can you please sign in / sign this off?"
- Fake institution

Account / card / card details takeover by unauthorised party
- Pure account takeover
- Creditor account data manipulation
- Control of card or card details by unauthorised party

First party fraud
- Fraudulent card application
- Fraudulent card claim
- Fraudulent use of cash back scheme
- Other first party fraud

EBA Fraud Taxonomy identifies the strategic approach taken by the fraudster:

- Narrative that triggers the desired reaction by the victim (social engineering)
- Account / card / card details takeover by unauthorised party
- First party fraud

Thank you!

Annick Moes, EBA Head of Industry Issues and Cooperation Initiatives

Euro Banking Association
40 rue de Courcelles, F-75008 Paris
Tel. +33 1 53 67 07 00

https://www.abe-eba.eu

https://www.linkedin.com/company/euro-banking-association

ABE EBA

EURO BANKING ASSOCIATION

Lunch Break
12:10 – 13:15 CET

During lunch break, do not “leave the meeting”
(i.e., stay connected while muting your sound and turning off your camera)

Kindly reconnect on time for the afternoon sessions

Marcus Columbu

Partner
act AC Tischendorf Rechtsanwälte Partnerschaft mbB

ABE EBA
EURO BANKING ASSOCIATION

act legal Germany

EBA Open Forum on Digital Transformation

11 July 2024 | Marcus Columbu

Agenda

01	Digital Operational Resilience Act (DORA) - Background, Objectives & Use
02	Being ahead of the curve – regulatory as an advantage in competition
03	Remuneration
04	Credit & ESG Risks
05	Compliance Risk Analysis
06	Contact

Digital Operational Resilience Act (DORA)

Background, Objectives & Use

Background & Objectives

Background

- DORA is part of the European Commission's Digital Finance Package of 2020 consisting of:
  - DORA Regulation
  - MiCA Regulation (Markets in Crypto Assets)
  - Retail Payment Strategy
  - Digital finance strategy
- Based on FinTech Action Plan (2018) and ESAs' Joint Advice (2019)

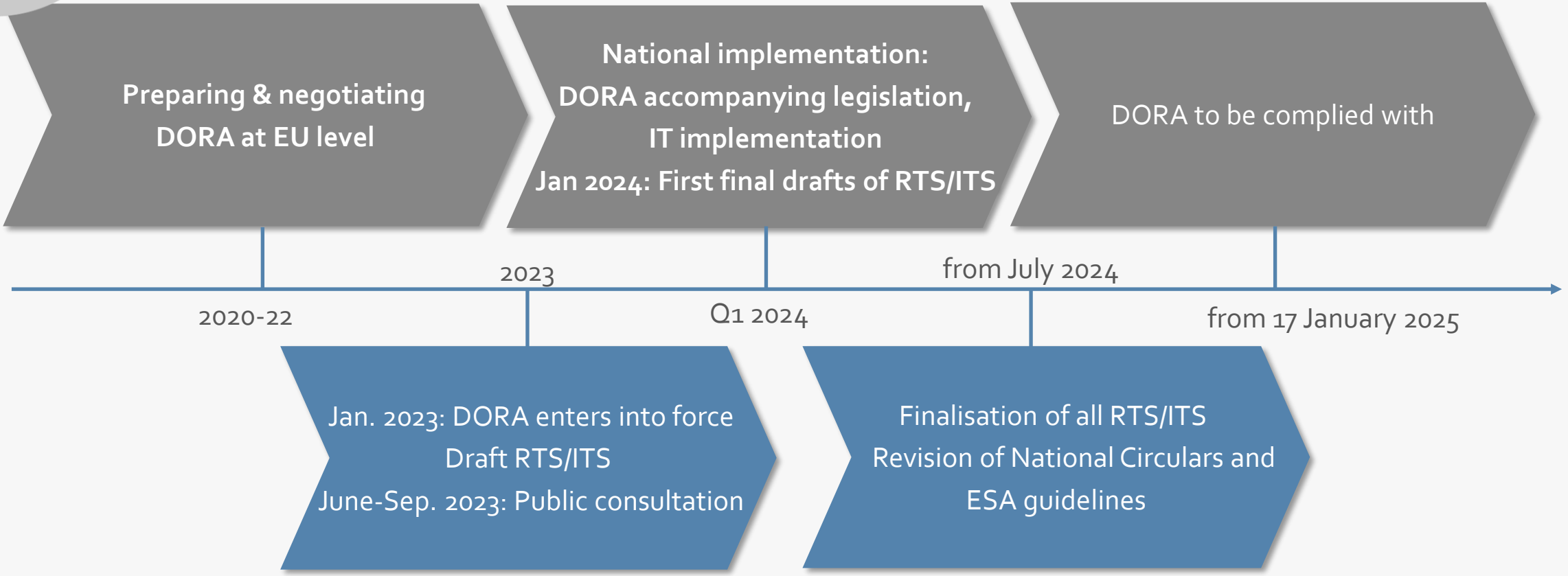
Objectives

- Strengthening the security and operational resilience of the entire European financial sector
- Establish standardised and consistent requirements across the financial sector
- Introducing proportionate requirements (proportionality principle)

Area of application

- Whole financial sector
- CRR Credit institutions, payment institutions (including registered account information service providers), e-money institutions, investment firms, crypto service providers (MiCA), CSDs, CCPs, trading venues, trade repositories, management companies, AIFM, data reporting services, insurance and reinsurance undertakings, insurance intermediaries, institutions for occupational retirement provision, credit rating agencies, administrators of critical benchmarks, securitisation repositories, crowdfunding service providers.
- Exemptions in Art. 2 para. 3 DORA

Schedule


Preparing & negotiating DORA at EU level
National implementation: DORA accompanying legislation, IT implementation
Jan 2024: First final drafts of RTS/ITS
DORA to be complied with
2020-22
2023
Q1 2024
from July 2024
from 17 January 2025
Jan. 2023: DORA enters into force
Draft RTS/ITS
June-Sep. 2023: Public consultation
Finalisation of all RTS/ITS
Revision of National Circulars and
ESA guidelines

DORA's Key Elements

1

ICT Risk Management

- Governance and organisation
- ICT Risk Management Framework
- ICT systems, protocols and tools
- Learning and development
- Communications

2

ICT Third Party Risk Management

- General principles (including information register on contractual relationships with ICT third parties, notifications to supervisory authorities and minimum contract terms)
- Oversight of critical third party ICT service providers

3

ICT incident reporting

- Definition of ICT Incidents
- Classification criteria for ICT incidents
- Reporting process, reporting of ICT-related incidents and cyber threats

4

Digital resilience testing

- Baseline tests
- Entire financial sector
- Vulnerability scanning, source code testing, performance testing, etc.

5

Threat Led Penetration Tests

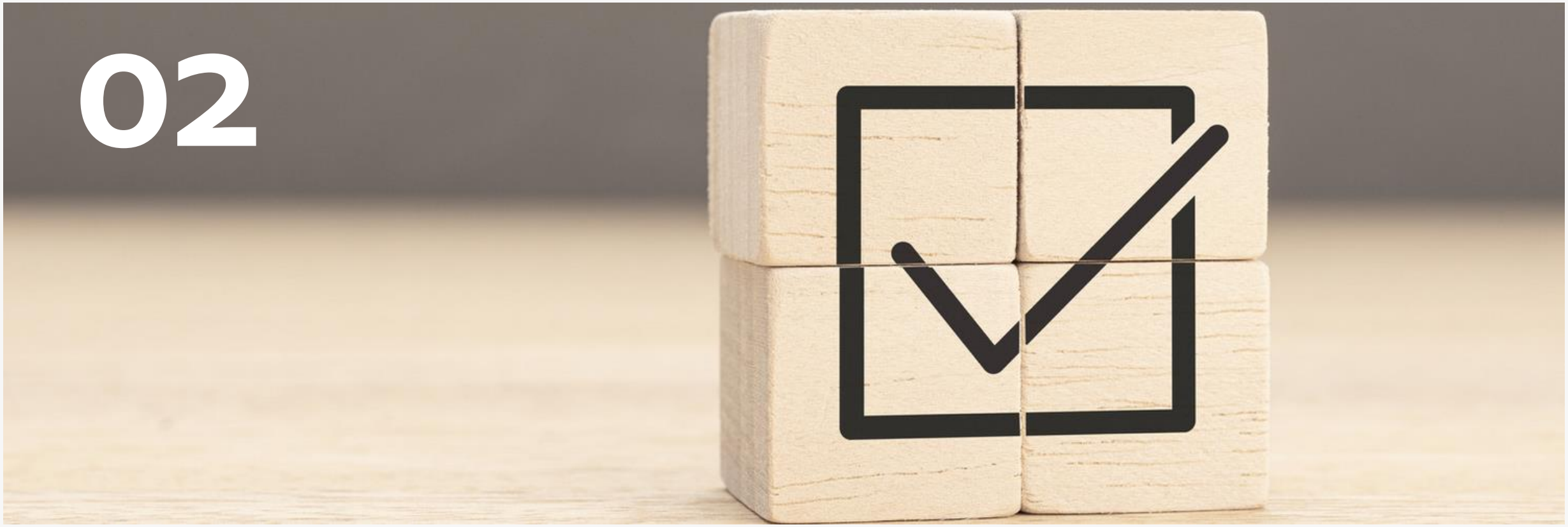
- Advanced tests
- Only "systemically important" financial institutions with a high level of ICT maturity

6

Information Sharing & Cyber Exercises

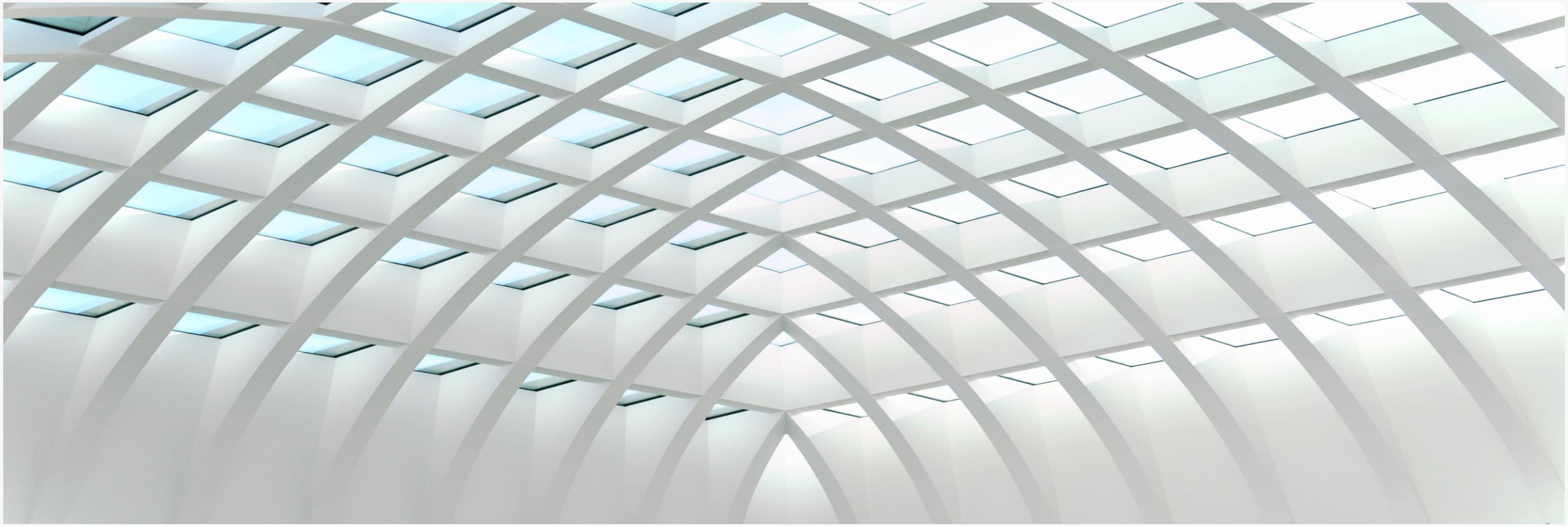
- Voluntary information and knowledge sharing between financial organisations
- Cross-sectoral crisis management and emergency exercises

Being ahead of the curve
Regulatory as an advantage in competition



Case Studies

From being behind of the curve to being ahead of the curve

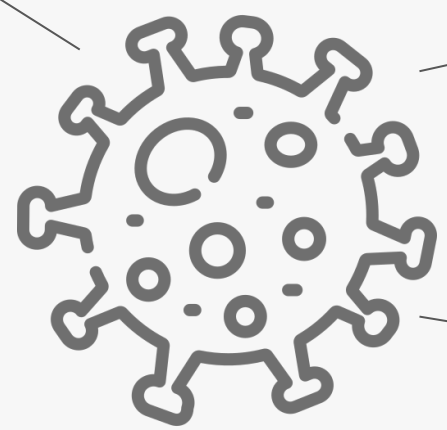


Client #1: Asset Manager

Behind the curve

Hardly any rules & procedures

Lack of qualitative specifications for sales



Purely quantitative, variable salary

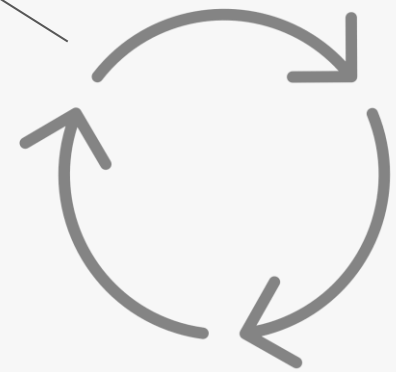
Lack of 4-eyes-principle

Overall neglect of regulatory framework

- → Approx. 100 investor lawsuits in three years
- → approx. EUR 25,000 legal fees per case → i.e. EUR 2.5 million in total
- → Indirect reputational damage EUR >10 million
- → Approximately 15 to 20% higher cost to implement compliance structures

Client #1: Asset Manager

Ahead of the curve



Qualitative and quantitative, variable salary

Anticipated implementation of new regulations

Sales guidelines, both qualitative and quantitative

Principle of dual control in relevant areas

Sustainability strategy defined and implemented

Clear set of policies, rules and procedures

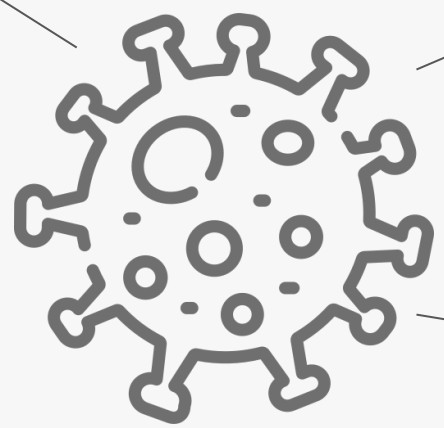
- → Fewer than 5 investor claims in 10 years
- → AuM and clients more than doubled in 5 years
- → Higher salaries and employee satisfaction
- → EBITDA almost tripled

Client #2: Real Estate Fund Manager

Behind the curve

Compliance as a “fig leaf”

No "Tone from the Top"



Purely quantitative, variable compensation

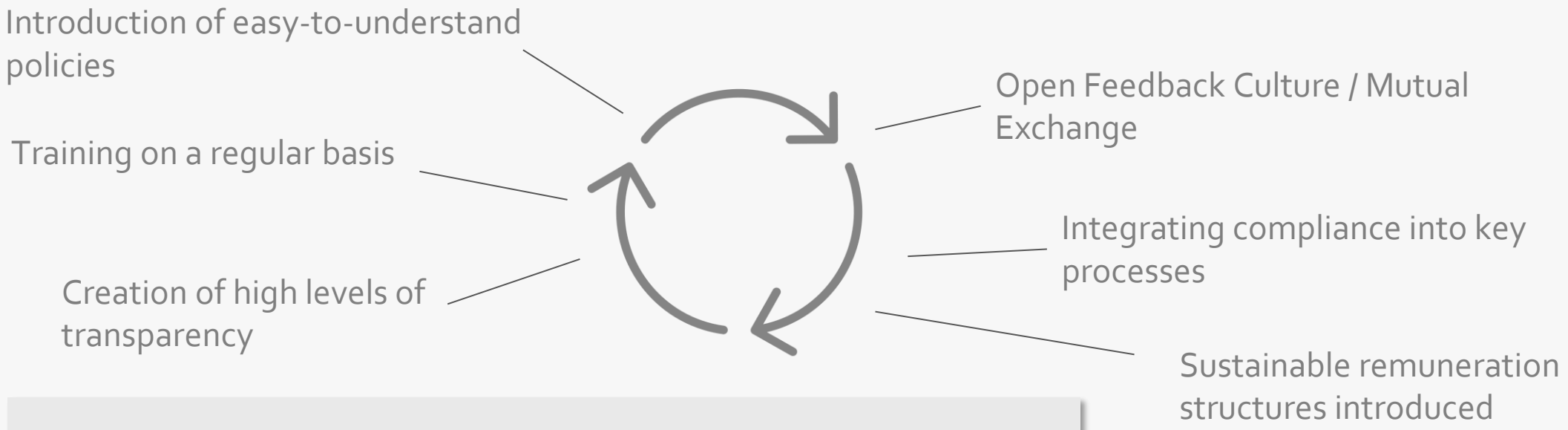
Giving contracts to family and friends without any consequences

No team spirit

- → Little growth
- → Money laundering incidents
- → High staff turnover, difficult to attract top talent
- → Bad press, serious damage to reputation

Client #2: Real Estate Fund Manager

Ahead of the curve



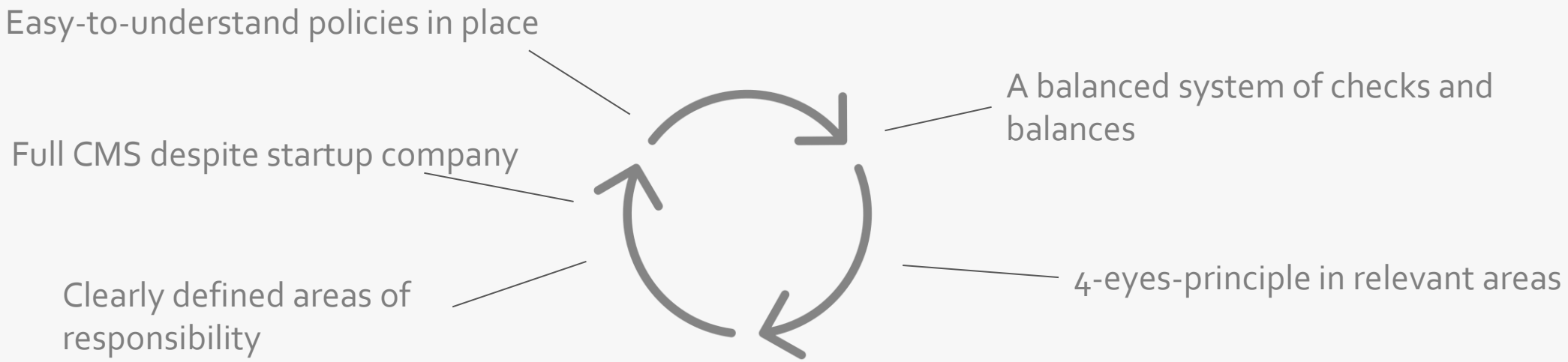
- → 600% increase in high-caliber staff in 2 ½ years
- → Salary increases of >40%.
- → "Black sheep" voluntarily resigned → High employee satisfaction
- → Risks significantly reduced
- → Product portfolio and new businesses significantly expanded

Reverse Case Study

From being ahead of the curve to being behind of the curve

Client #3: Hedge Fund-Manager

Ahead of the curve



- → Clear and simple processes
- → Easy onboarding of large institutional investors
- → Very successful launch with > EUR 1 billion AuM after first year
- → Very high client satisfaction due to transparent reporting

Client #3: Hedge Fund-Manager

Behind the curve

Failure to adopt ESG strategy despite game changing mindset

ESG compliance ignored

No ESG disclosures

Not trained or counseled regarding ESG

- → Major customers have envisaged to reduce their commitments by up to 50%.
- → Potential client not acquired. Reason: no ESG strategy
- → Loss of two high-caliber employees
- → Numerous justifications from existing clients
- → Costly retrospective implementation of ESG strategy and compliance

Takeaways & Conclusion

Takeaways & Conclusion

behind the curve

- Difficulty attracting new customers while retaining less desirable customers
- Difficulty in attracting and retaining staff with high staff turnover
- High risk of reputational damage and direct economic damage
- Very high implementation cost to remedy lack of regulatory compliance

ahead of the curve

- Desirable AAA-Customers
- Clear and simple processes
- Easy onboarding of large institutional investors
- Very high client satisfaction due to transparent reporting

Remuneration

Special Part 8 (BT 8) 1/2

Overview

Basis: ESMA's guidelines on some aspects of MiFID II remuneration requirements

Increase in salary & promotion

Remuneration policies and procedures

- The new ESMA guidelines extend the previous requirements for compensation systems to all types of salary increases and promotions.
- Personnel development measures must not only be based on purely quantitative criteria, but must also take sufficient account of qualitative criteria.

Qualitative components of the remuneration

Importance of qualitative criteria in determining compensation

- The design of quantitative criteria must not give rise to conflicts of interest.
- Any remaining conflicts of interest must be "mitigated" by the use of other criteria, such as compliance with suitability requirements or client satisfaction.
- ESMA guidelines now explicitly refers to "equally weighted" qualitative and quantitative criteria.

Special Part 8 (BT 8) 2/2

Overview

Basis: ESMA's guidelines on some aspects of MiFID II remuneration requirements

Deferred Payment

Criteria for retrospective adjustments and claw backs

- For reasons of prevention, it should also be possible to adjust variable remuneration components if the institution only becomes aware of an employee's misconduct after it has already granted or even paid out bonuses for the relevant period.
- Rules comparable to those in the Remuneration Ordinance for Institutions for Risk Takers
- The introduction of retrospective adjustment criteria is not mandatory ("should ... consider").

BUT: A decision against implementation requires sound justification.

NEW: Governance-Rule

Possible new areas for auditors to focus on

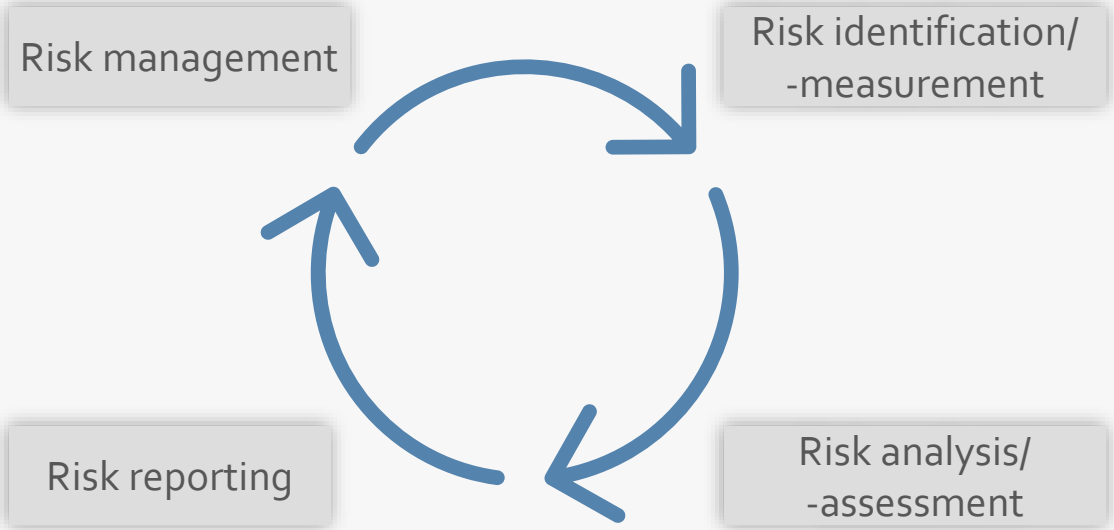
- Ultimate responsibility for the appropriate design and implementation of the remuneration system lies with the board.
- Remuneration policies, their approval and changes must be properly documented.
- The compliance function must review the remuneration policies and procedures.

Credit & ESG Risks

EBA guidelines for lending and credit monitoring

Further development

- **ESG risks in processes, risk measurement and reporting**
- Real estate business
- Model requirements
- Business model analysis
- Large development banks



ESG-Requirements

ESG requirements are fully integrated throughout the risk framework:

1. Integration of ESG factors into business and risk strategy and risk appetite
2. Consideration of ESG factors in risk identification, risk measurement/assessment, risk management, risk monitoring and risk reporting, up to and including risk-bearing capacity (normative and economic).
3. In terms of risk measurement/assessment, also quantitative measurement of ESG risks where appropriate and possible (e.g. through ESG scenario calculations or separate ESG sensitivity analyses).
4. Clearly define ESG responsibilities within boards and allocate resources appropriately
5. The integration of ESG factors into the organisation's policies and processes, including investment decisions and risk management.

Compliance Risk Analysis

Considering quantitative and qualitative risk

05

Contact

Ihr Ansprechpartner: Marcus Columbu

@ marcus.columbu@actlegal-germany.com

☎ +49 69 24 70 97 35

+49 151 230 666 77

Practice Areas

Banking-/Financial Services Regulatory
Compliance-Projects
Compliance Officer
Supervisory Board

CV

Marcus Columbu is a partner at ACT since 2015. Previously, he worked for several years at a major law firm in the area of Banking Regulatory, including the interface to M&A. He is external chief compliance officer, anti-money laundering and ESG officer of numerous regulated and non-regulated companies. He is also member of the Supervisory Board of Varengold Bank AG. His particular expertise includes the design and implementation of compliance management systems (CMS), the optimization of existing processes and the implementation of new, efficient and sustainable processes. He specializes in efficient and pragmatic solutions to ad-hoc compliance and regulatory issues and the sustainable further development of CMS.

Marcus Columbu is a member of the Bankrechtliche Vereinigung-Wissenschaftliche Gesellschaft für Bankrecht e.V. and of the Frankfurt Working Group Compliance & Governance with a focus on MaRisk compliance, compliance management systems and money laundering.

Marcus Columbu is consistently recognized in the relevant rankings:

- Legal500, recommended lawyer Compliance and Regulatory (2024)
- WirtschaftsWoche, Top Lawyer Regulatory (2022, 2023, 2024)
- Handelsblatt / Best Lawyers Finance (2022)

Roderick Kroon

Senior Consultant
Projective Group

ABE EBA
EURO BANKING ASSOCIATION

The new Instant Payments Regulation

What we know and what is still in the grey zone… Reading between the lines!

Draft version 0.9

Instant? …… It is the new normal in many situations

Instant is already the new normal

Instant Payments – everywhere now

Faster and Secure Transfers
Singapore

Swiss Instant Payments

New Payments Platform
Australia

Faster Payment System
Hong Kong

Projective GROUP

Instant Payments in the SEPA zone

The first formal version of the SCT Inst Scheme Rulebook was approved by the EPC Board on **November 2016**!

European Payments Council

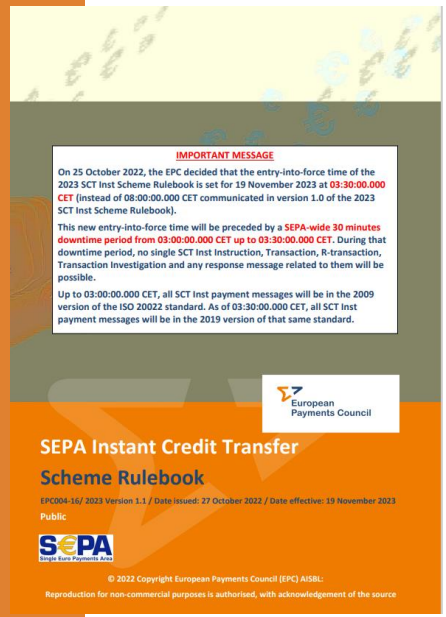
SEPA Instant Credit Transfer

Scheme Rulebook

EPC004-16/ 2021 Version 1.1 / Date issued: 13 December 2021 / Date effective: 11 January 2022

Public

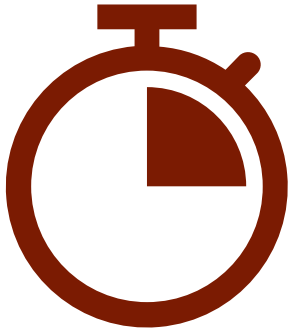
SEPA Single Euro Payments Area



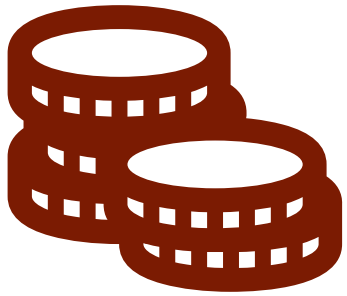
Projective GROUP

SEPA Instant Payments

How are they different?



Within seconds, irrevocable



Potential amount limits

24x7x365

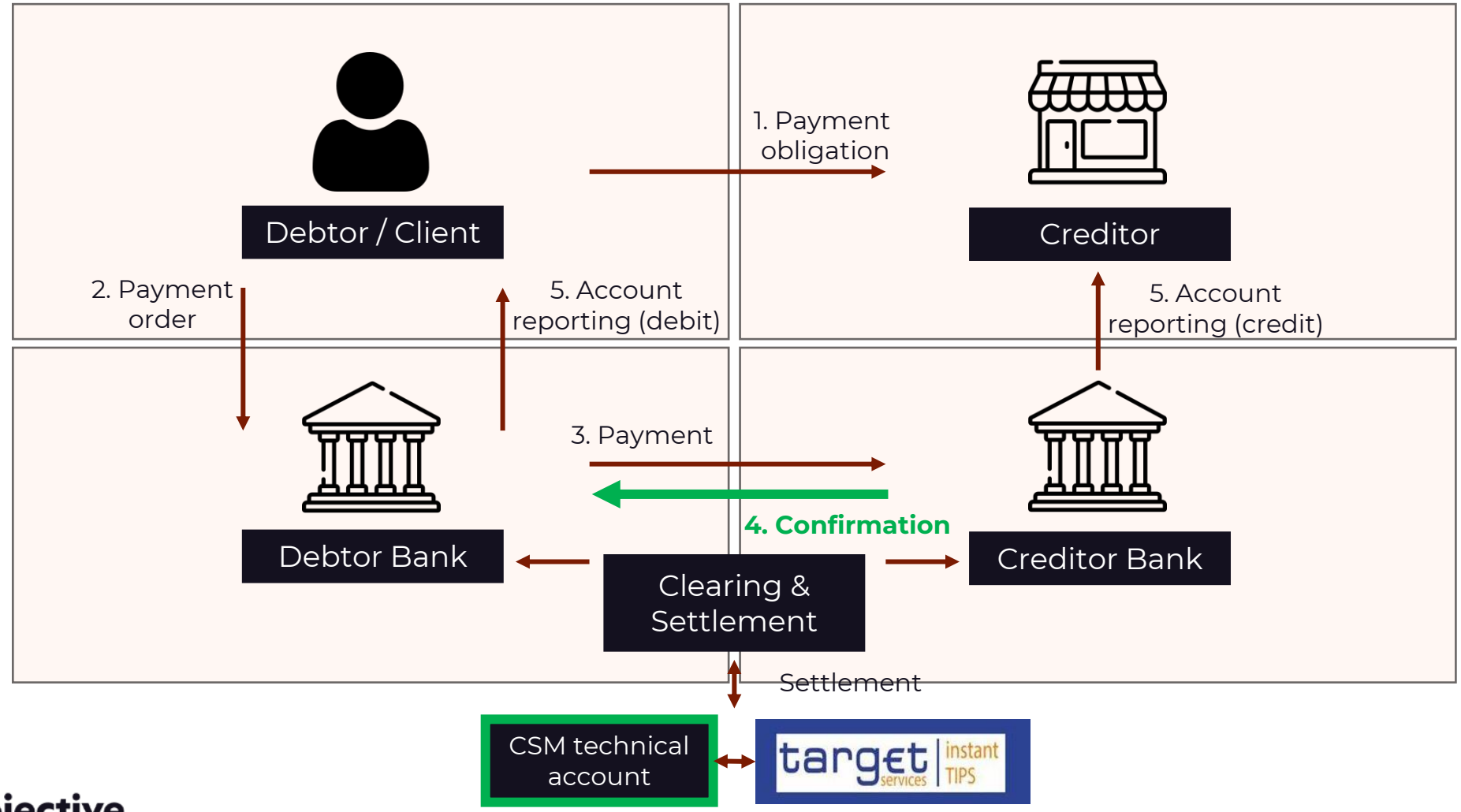
Confirmation receipt
(pos/neg - TIME-OUTs)

Consumer vs. business

Head of Payments, SWIFT : "The major challenges in this domain are not the latency and speed, as many would expect, but the 24/7 guaranteed availability: the network as well as the endpoints at -and CSM- side have to foresee full 24/7 operations, even during upgrades, releases, unforeseen outages of any hardware component "

Projective GROUP

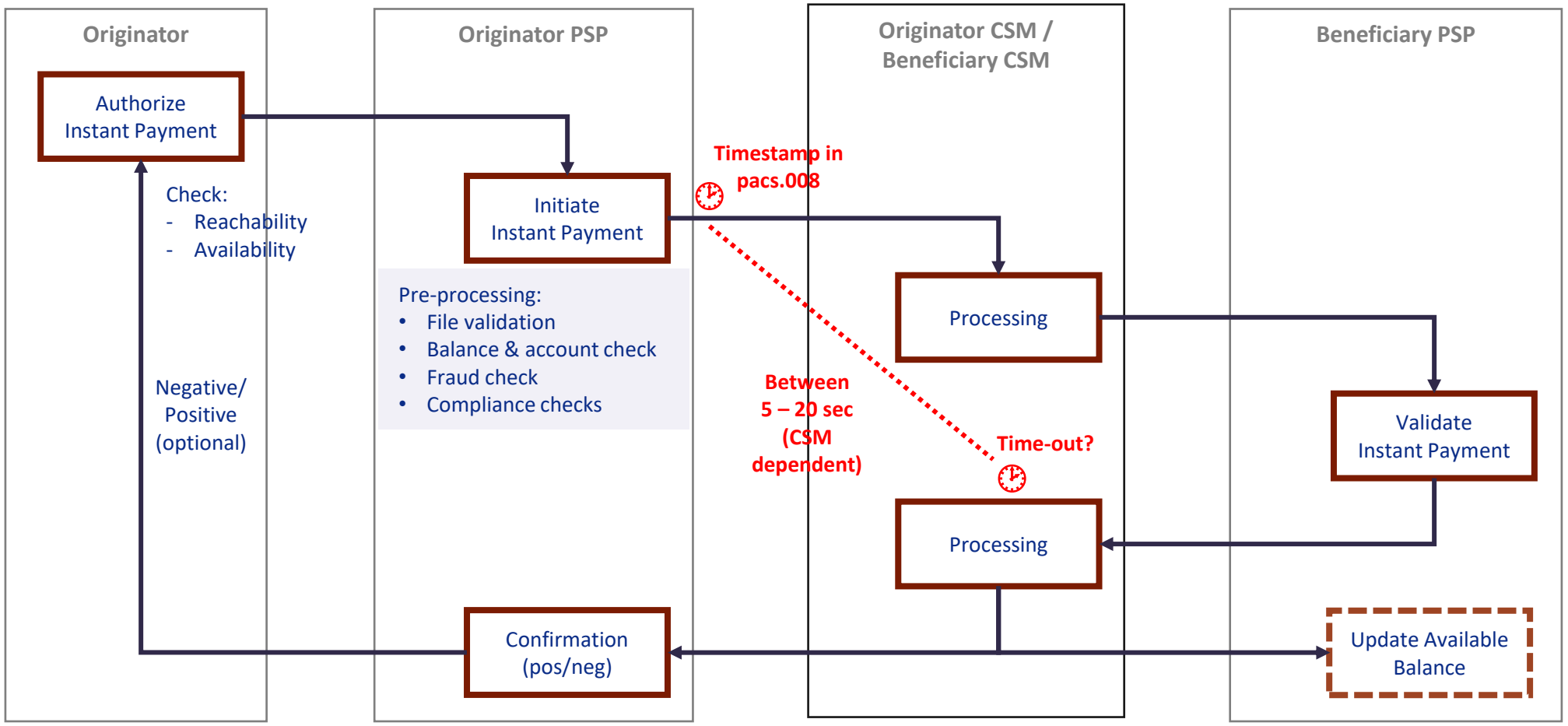
4 corner model – SCT INSTANT



Projective GROUP

Current SCT Instant rulebook version

The current SCT Instant rulebook determines how the value chain is organised



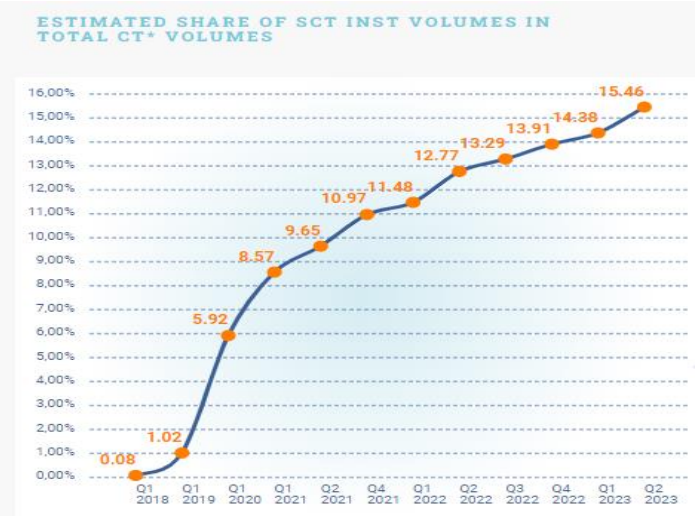
Currently (CSM) VAS:
- **Non-time critical**
- **Transaction limit**

No CSM interoperability
- But CSM's offer to forward a transaction to/from TIPS if needed (TIPS routing services)

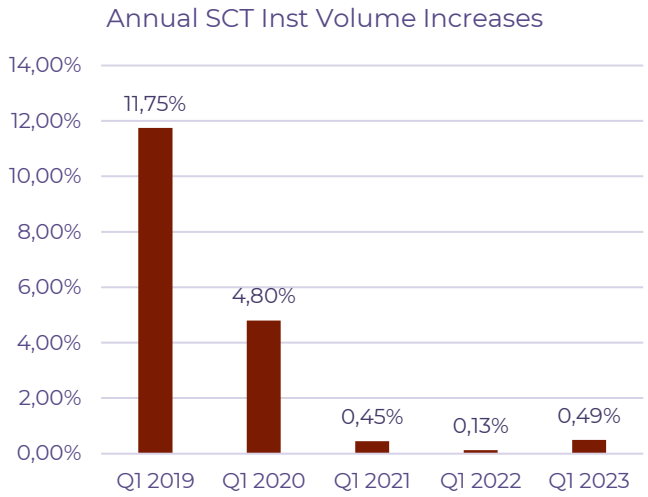
Projective GROUP

Instant Payments Regulation – Why?

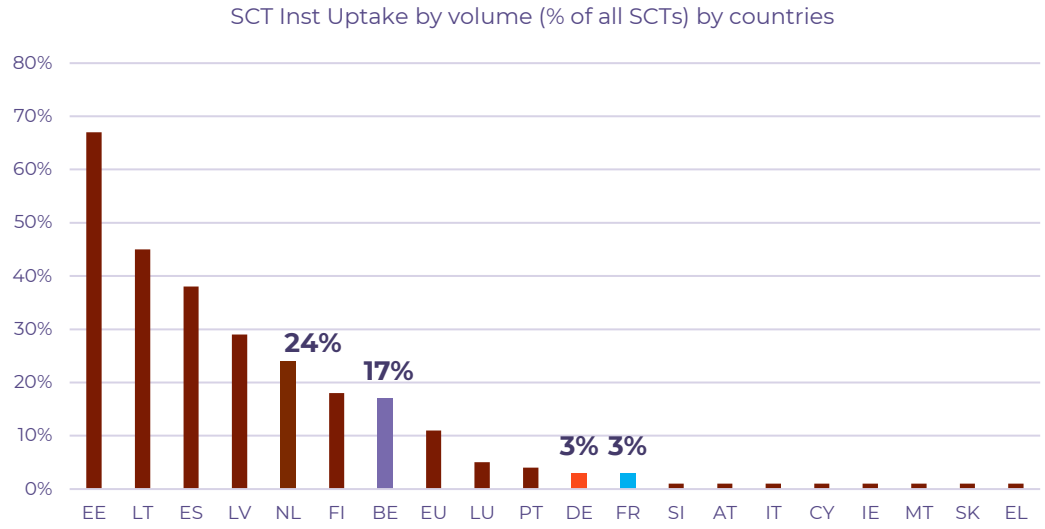
- EPC does not like the slow uptake and differences in approach between the EU countries (premium instrument vs the new normal)



SCT Inst usage within SEPA has steadily risen since its introduction in 2017, now accounting for 15% of all SCT transactions



After rapid acceleration in 2019 and 2020, annual growth of SCT Inst transactions is currently slowing



There is a big difference between countries

Projective GROUP

Instant Payments Regulation – What will change?

Ambition of the new IPR:

1. Making Euro Instant payments universally available
2. Making Euro Instant payments accessible at no extra cost
3. Increasing trust in Euro Instant payments (VoP)
4. Making sanctions screening of Euro Instant payments more efficient

*"All payment services providers (with very **targeted exceptions**) that offer credit transfers in euro must offer instant payments in euro to all their customers".*

- Will all banks move> **=> NO**
- Will the 'classic' SCT disappear**? => NO**

Projective GROUP

Instant Payments Regulation – What happened?

Political process

Implementation process

European Commission IPR proposal

Position European Council

Position European Parliament

Provisional Agreement

Publication Official Journal EU

Entry into Force

Requirement to offer Instant Payments (receiving)

Requirement that charges for Instant Payments shall not be higher than charges for traditional credit transfers

Harmonised sanctions screening procedure

Requirement to offer Instant Payments (sending)

Requirement to offer **Verification of Payee** for SCT and SCT Inst

Note: Indicated requirement time-lines are for credit institution within the Eurozone. Other institutions (non-EUR, EMI) have different time-lines.

Projective GROUP

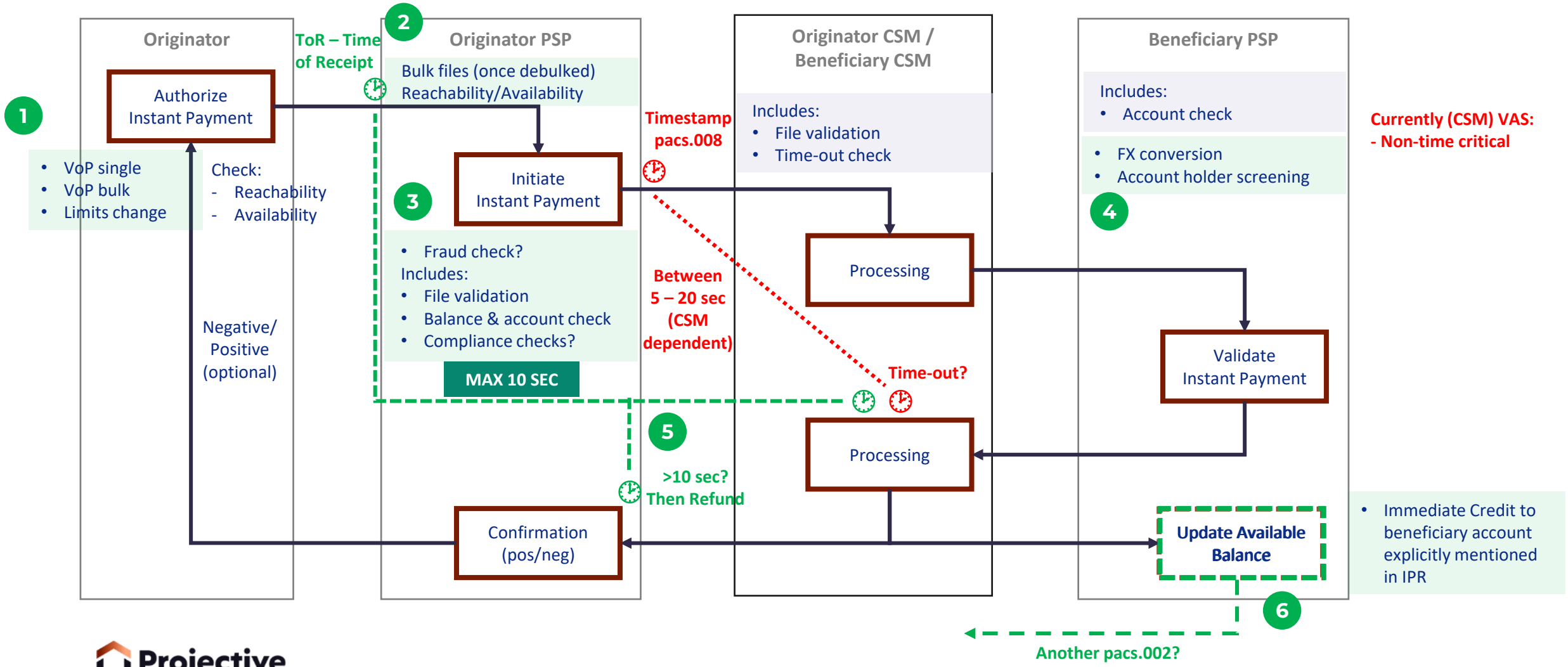
Instant Payments Regulation – New rules??

- The recently published IPR does introduce **new processing rules** and **mandatory features**
- The IPR and current SCT Inst rulebooks are **not (yet) aligned**
- Interoperability of VoP schemes a challenge. Final rulebook in Sept., **will local flavours be allowed?**

Projective GROUP

Instant Payments Regulation – Processing rules

There is a key difference between the IPR and the existing SEPA Instant rulebook



Projective GROUP

Relation IPR & Fraud? (1 of 3)

Experiences show that there are **no new forms of fraud** emerging from instant payments, still the new scheme features provide **numerous opportunities for fraudsters** to exploit:

Posting speed

- Time out if processing (E2E) if > 10 seconds
- Funds available immediately
- Funds sent to Bank account directly instead of prefunded account

- Risk of 'time-out' makes that required checks might be done with less accuracy/quality because a PSP is 'running out of time'
- Time to respond to fraud is limited with beneficiary able to move funds i.e.: money mules

24/7/365 availability

- Continuous availability
- Increased utility for sending/receiving party

- Fraudsters can work off-peak hours i.e.: when PSP staff inactive – victims may not be able to report fraud timely

Projective GROUP

Relation IPR & Fraud? (2 of 3)

Payment finality

- Payment cannot be reversed
- Improved cash flow
- Lack of chargeback increases attractiveness compared to cards

- SCT Inst payment cannot be easily reversed, unlike card payment with chargeback
- Funds hard to recover due to speed to identify fraudulent payment and fraudster reactiveness

PSU limits adjustments

- IPR states that if a PSU wants to change their transaction or daily limit this needs to be executed IMMEDIATELY
- Maximum (scheme) limits (now 100.000 EUR for TIPS) are likely to be removed
- Higher limits means more use cases supported

- High transaction limits makes SCT Inst attractive to fraudsters
- The obligation for immediate change is fully against current fraud prevention practices to have **a 'cool off' period of (average) 4 hours** to make this limit change effective

Projective GROUP

Relation IPR & Fraud – all bad news then? (3 of 3)

Fortunately, it is not all bad news

Verification of Payee

- VoP checks are mandatory in the channels
- For both SCT Inst as well as Classic SEPA
- Even 'Opt in' for VoP on bulk payment files

- From countries that have implemented VoP the fraud rates have been reduced significantly
- Still, the need to support VoP for bulk files is seen by many parties, including corporates, as introducing unnecessary complexity (unhappy flows ….)
  => is a default opt-out or 'two-step' approach (legally) allowed?

'Switching'

- Best practice is to build a 'switch' between Classic SEPA and SEPA Instant
  - With amount thresholds (all > 50 EUR)
  - For all SCT out

- The regulation is not very clear if a PSP has to offer SCT Inst as 'default' and when the classic SCT still can be used (Standing order?)
- In case of Fraud alerts/suspicion a best practice is to be able to switch (temporary) to SEPA Classic. Here you have more time to check what is happening, hold a 'batch' a little longer before sending it to the CSM

Value added services

- To combat payment fraud new services are introduced
- Making use of advanced technology for fraud pattern and anomaly detection (FPAD)

- Plug-ins on top of PSP's fraud prevention and transaction processing capabilities
- These services are being introduced by VoP solution providers but as well by CSM's and for example SWIFT

Projective GROUP

Instant Payments Regulation – What's next?

- Make sure you are prepared
- Look at solutions in the market that may help you ….
- Study final response of ECB to FAQ's and keep contact with local associations
- Await the publication of the new rulebooks for VoP (Sept) and SCT Inst (Nov)

Projective GROUP

Thank you

Do you want to talk about Instant Payments (Regulation)?
Feel free to reach out

Roderick Kroon
+31 6 51 22 06 31
Roderick.kroon@projectivegroup.com

ABE EBA
EURO BANKING ASSOCIATION

Coffee Break
14:35 – 14:50 CET

During coffee break, do not “leave the meeting”
(i.e., stay connected while muting your sound and turning off your camera)

David Renault

Team Leader SEPA
EBA CLEARING

Ronny Wolf

Vice President
Commerzbank AG

ABE EBA
EURO BANKING ASSOCIATION

Dr. Matthias Terlau

Partner
Görg

ABE EBA
EURO BANKING ASSOCIATION

GÖRG

YOUR BUSINESS LAW FIRM

Regulating the fraud chain in payments – What's to be expected (PSR/PSD3)?

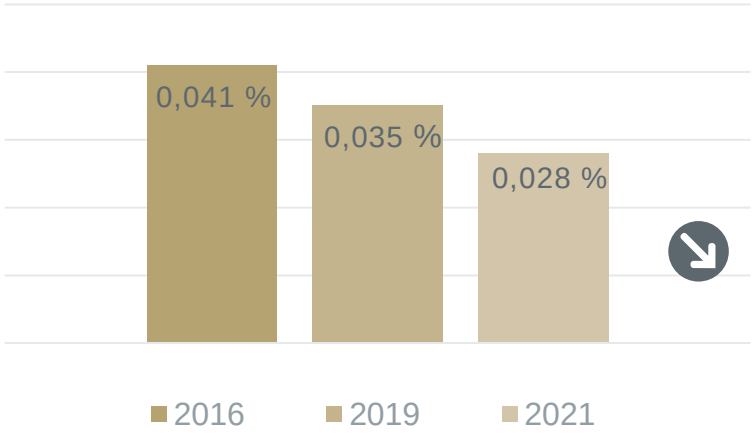
EBA Open Forum on Digital Transformation

Dr Matthias Terlau | 11 July 2024

Card fraud in Europe - ECB statistics

GÖRG
YOUR BUSINESS LAW FIRM

- **Fraudulent card transactions** measured by the total value of card payments made with cards issued in the euro payments area (SEPA):



2021:

- 0.028 % corresponds to a value of € 1.53 billion with a total value of all card payments of € 5.40 trillion
- lowest level since data collection began

- Card not present (**CNP)** fraud measured by the total value of card fraud

  2021: 84 %

  - Decrease of 12 % following implementation of strong customer authentication in accordance with PSD2

Source: report on card fraud in 2020 and 2021, ECB, https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305%7E5d832d6515.en.html

Card fraud in Europe - ECB statistics

GÖRG
YOUR BUSINESS LAW FIRM

Nevertheless, industry, regulators and consumers need to remain vigilant. 2020 and 2021 were exceptional years, with the COVID-19 pandemic and the related measures (e.g. lockdowns) having a notable impact on both card payments and fraud; among other factors, both international travel and the cross-border use of cards were limited by the pandemic. Furthermore, the aforementioned success of both industry and regulatory measures in reducing card fraud may shift the attention of fraudsters towards card holders, potentially further increasing fraud through social engineering (e.g. by manipulation of the payer) or the theft of physical cards.

Source: report on card fraud in 2020 and 2021, ECB, https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305%7E5d832d6515.en.html

GÖRG
YOUR BUSINESS LAW FIRM

Legislative procedure

- **28 June 2023:** Proposals of the EU Commission
- **End of 2023:** EU Council: Progress report of the Spanish Presidency
- **14 February 2024:** Vote on proposed amendments in the ECON Committee

- **And now? A break for now ... Election to the EU Parliament**
  (discontinuity principle, inaugural meeting on 16/7/24)

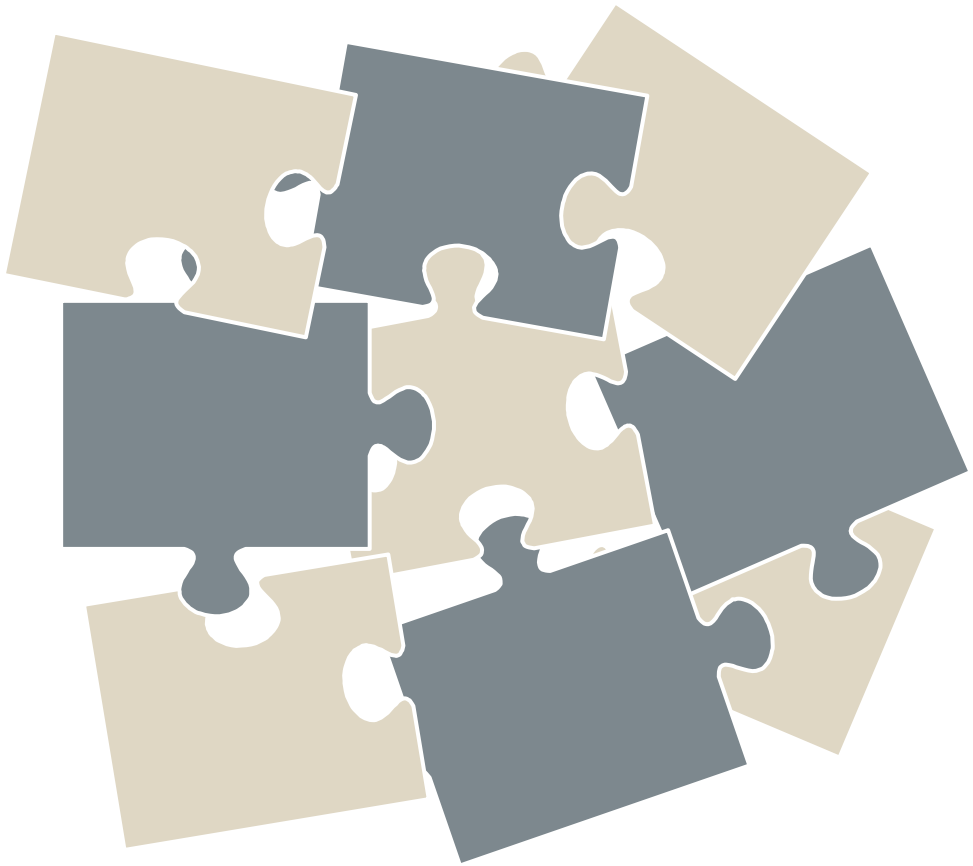
Adoption expected between Q3/24 – Q1/25

Application* expected between Q1/26 – Q3/26

* Application PSR after 18 months, implementation PSD3 within 18 months,

Implementation of the Retail Payment Strategy

GÖRG
YOUR BUSINESS LAW FIRM



PSD3/PSR

- Strengthening the internal payments market
- Improvement XS2A
- Improve fraud prevention
- Strengthening payment institutions

Instant Payment-VO / d€-VO

- European payment sovereignty
- Global payment security and convenience

Digital Markets Act / FIDA

- Opening up infrastructures to competition
- Opening up the financial market to competition

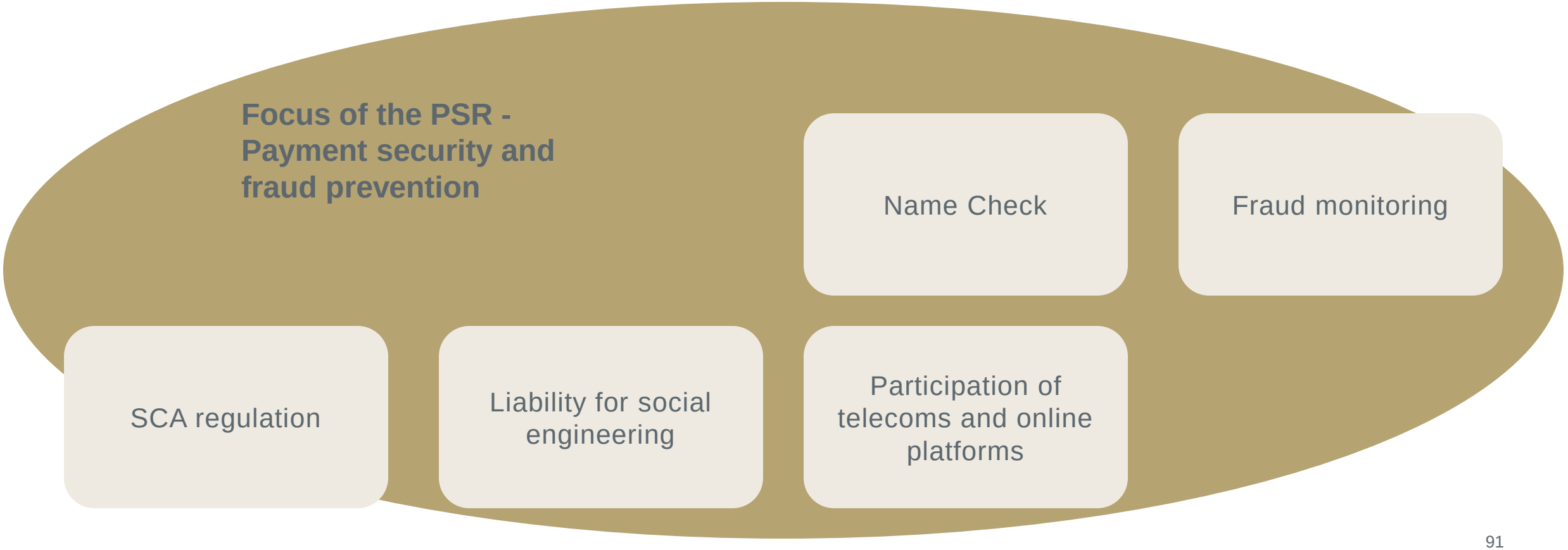
Reform through PSR and PSD3

GÖRG
YOUR BUSINESS LAW FIRM

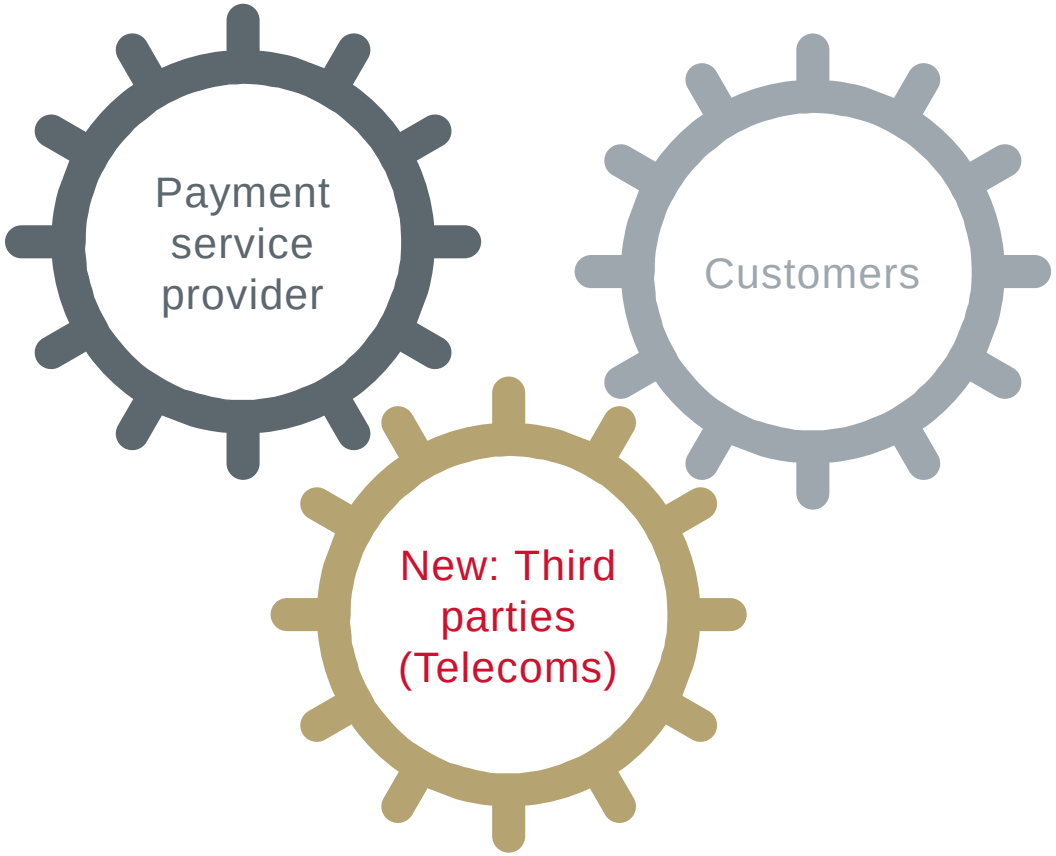
Cash supply	Group exemption	Fee regulation	XS2A fees
No standardised APIs	XS2A-Dash Board	Name Check	Fraud monitoring
SCA regulation	Liability for social engineering	Participation of telecoms and online platforms	Payment institutions

Reform through PSR and PSD3

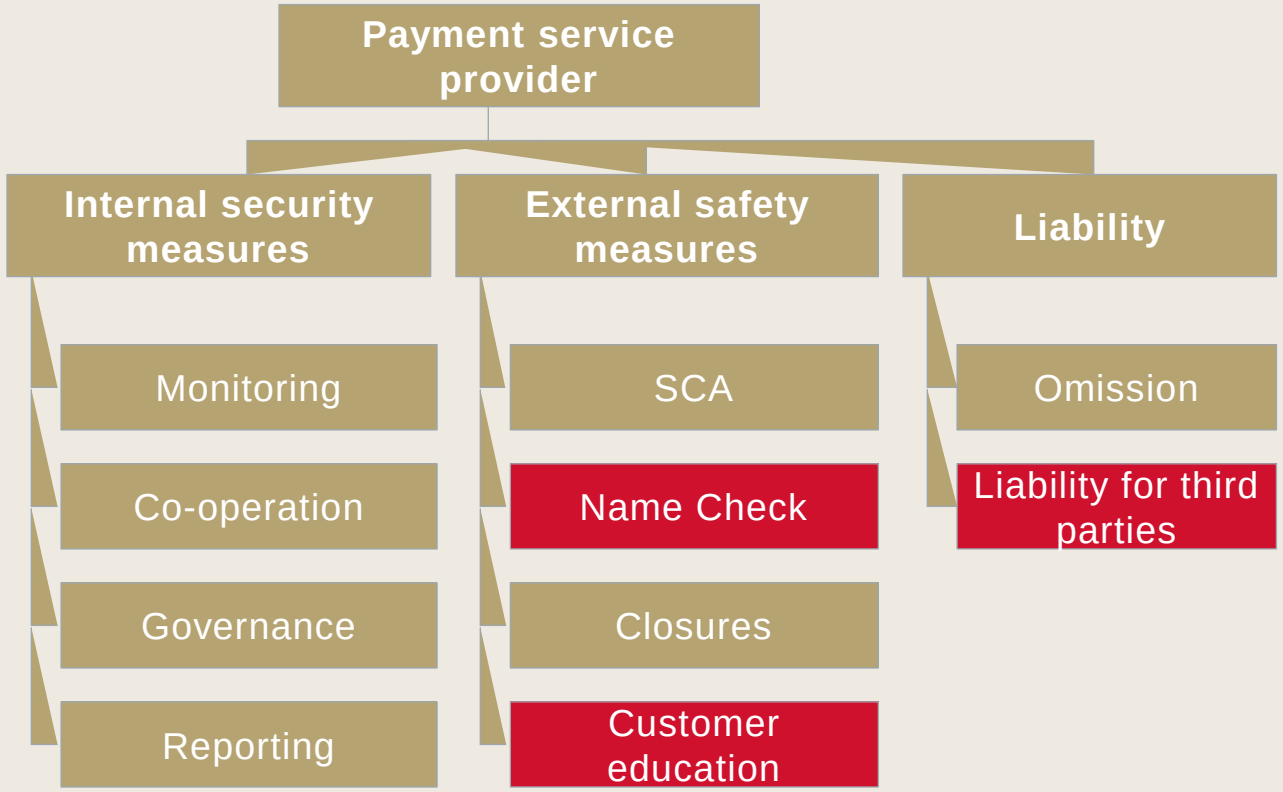
GÖRG
YOUR BUSINESS LAW FIRM

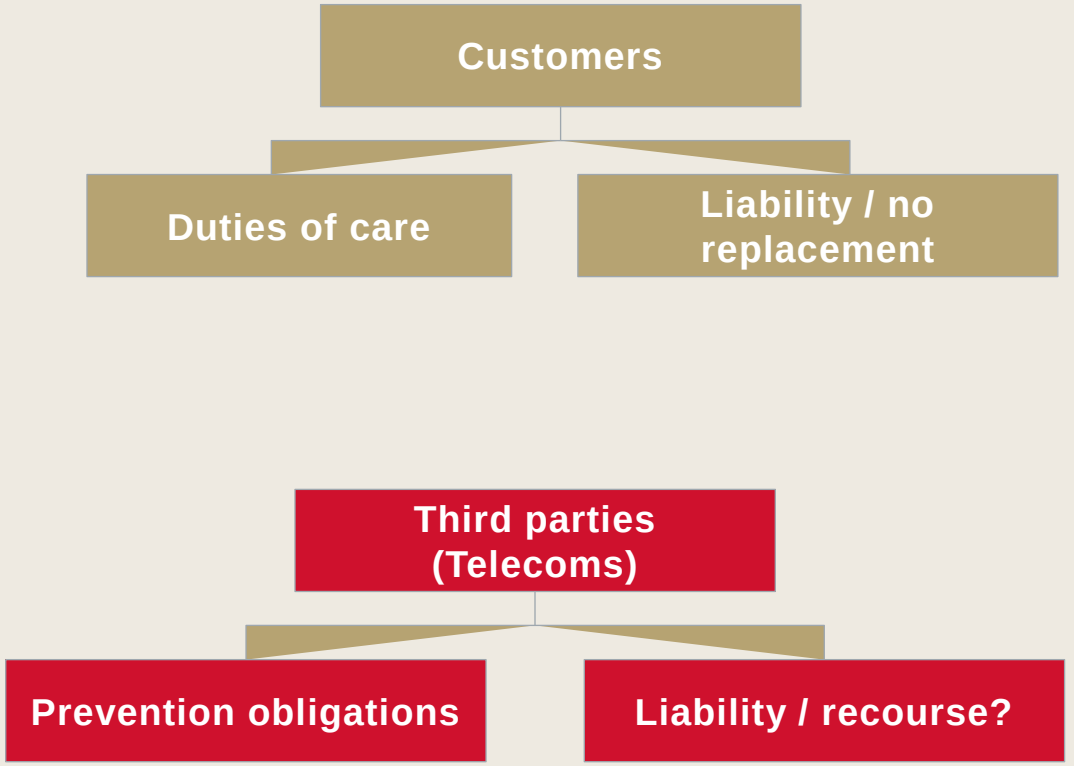


Regulation of payment security: parties involved



Payment security regulation system





GÖRG

YOUR BUSINESS LAW FIRM

Innovations in internal security measures

Monitoring

GÖRG
YOUR BUSINESS LAW FIRM

- **Risk minimisation measures and control mechanisms for risks**

Art. 81-83 PSR-E

- Monitoring, incident management, also inclusion of behavioural data
- Econ Committee: **e-wallet providers** as obligated parties
- Liability of the PSP if IBAN or other of a payee is **not blocked** although reported as fraudulent or involved in fraud
- Information sharing arrangements on fraudulent payees between PSPs & liability

New features for external security measures

Name check and liability

GÖRG
YOUR BUSINESS LAW FIRM

Art. 50 PSR-E

- **Name check for all transfers (for SEPA already in IP-Reg; PSR extends this to other schemes, Target2)**
- **In case of discrepancy - payer may still authorise**
- **In real time for all payment releases**
- **Liability: payer's PSP liable, recourse**

Art. 57 PSR-E

Call centre equipment and communication

- Discussion in the Econ Committee:
  - CC employees Language skills
  - Sufficient qualification of the CC employee
  - (Ltd.) Access without prior identification of the user

Art. 53 (1) (c) PSR-E

- **Communication:** Discussion in the Econ Committee
  - Use of secure communication channels
  - "in principle" no sending of links or documents by e-mail

Art. 53 (1) (a) PSR-E

SCA for direct debit & MIT

- **Direct debit excluded**, but not entirely clear ("without interaction or involvement of the payer"?) Art. 85 (2) PSR-E

- **MIT still excluded**, Art. 85 (2) PSR-E;
  New right to reimbursement for MIT (no questions asked) within 8 weeks (Art. 62 (1) (UAbs. 3) PSR-E)

Facilitated implementation of SCA

Art. 85 (12) PSR-E

GÖRG
YOUR BUSINESS LAW FIRM

- New: **two factors from the same group allowed**
  (2x knowledge, 2x possession, 2x inherence)

- **Econ Committee**: not 2x knowledge, but inherence may also include behavioural characteristics

- **Discussion in the Econ Committee: SCA free of charge in any case**

SCA at MoTo

Art. 85 (7) PSR-E

- **MOTO** (Mail Order, Telephone Order)
  - **No SCA**
  - but **another form of** authentication

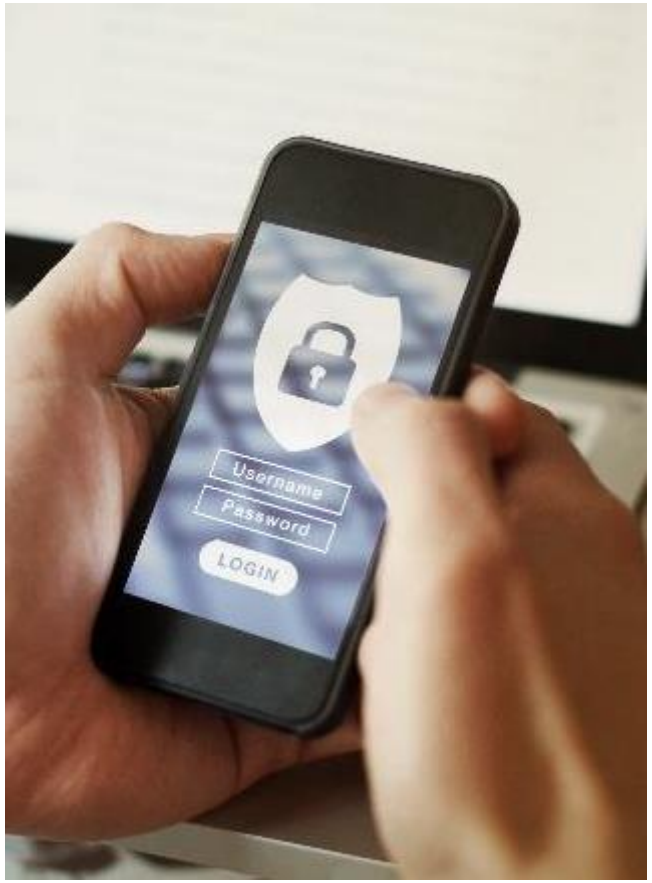
SCA for vulnerable groups

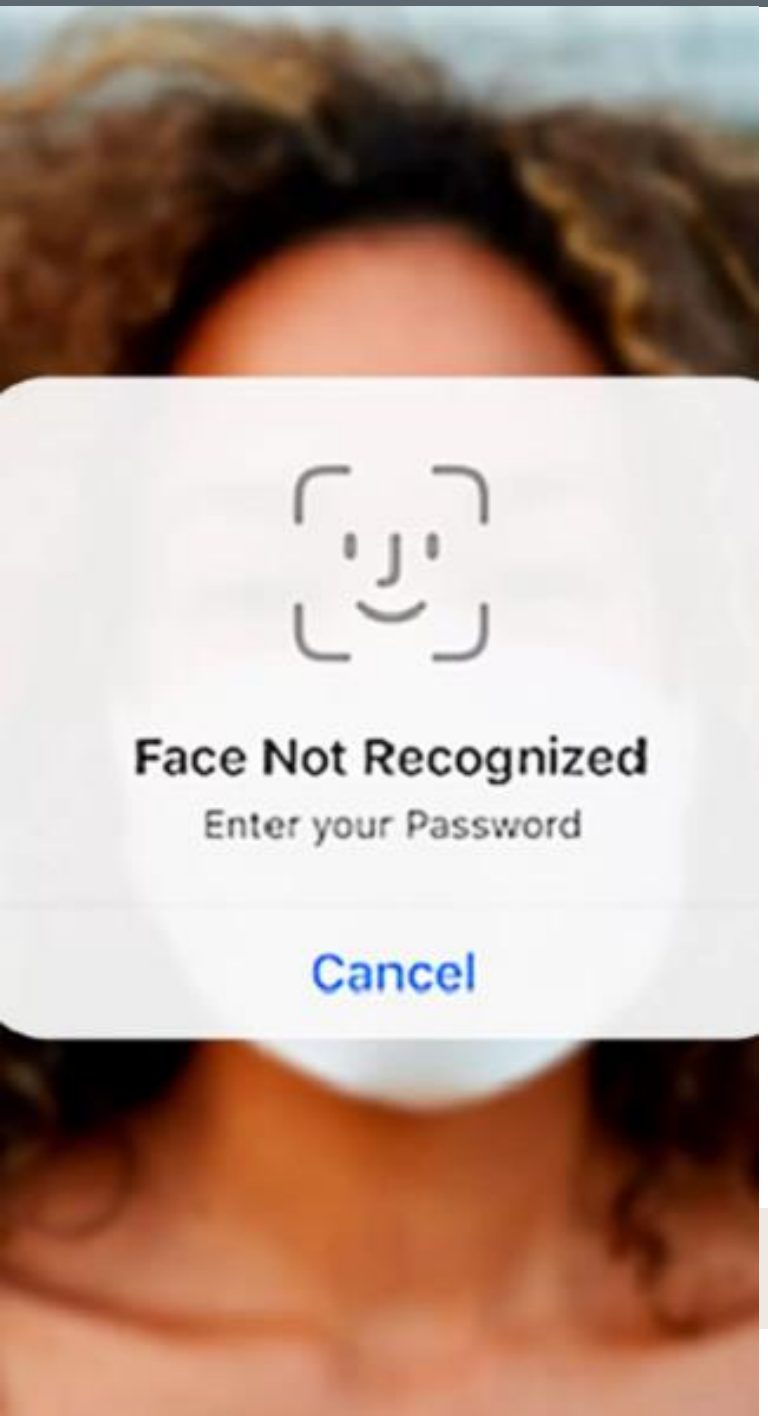
Art. 88
PSR-E

GÖRG
YOUR BUSINESS LAW FIRM

- Persons who **do not have access to digital channels or payment instruments** (persons with disabilities, low digital skills, elderly people)

- SCA **not just a single means of authentication**
  - Not limited by possession of a smartphone





ApplePay etc & strong customer authentication (SCA)

GÖRG
YOUR BUSINESS LAW FIRM

- **Apple Pay / Google Pay as outsourcing**?
- **significant outsourcing**? / **ICT-services DORA**

Art. 87 PSR-E

- Consequences (among others):
  - **Written outsourcing agreement,**
  - **Review and monitoring obligations of the institutions**

GÖRG

YOUR BUSINESS LAW FIRM

Liability of payment service providers

Liability for failure to carry out strong customer authentication

GÖRG
YOUR BUSINESS LAW FIRM

- **So far:**
  - **PSD2: increased liability for non-application of SCA**
  - **Not where exemptions apply (some German courts)**

- **Commission proposal:**
  - In future: **Stricter liability regulations even when using an exemption**
  - **Criticism:**
    - Exemptions user-friendly; banks should not bear risk
    - Particularly clear for the exemption of white listing

GÖRG

YOUR BUSINESS LAW FIRM

Small revolution: Strict liability of banks for social engineering

The Proposal by the EU Commission

- **Impersonisation Fraud:**

Art. 59 (1) PSR-E

  - Third party pretends to be a "bank employee",
  - ECON Committee: or as a police officer or as a technical service provider
  - with name, telephone number or e-mail address of the bank (the police etc.)
  - Manipulation of PSU to initiate a payment transaction

- **Full refund to PSU**
  - unless fraud or gross negligence on part of the PSU

Legislative justification of strict liability for social engineering

GÖRG
YOUR BUSINESS LAW FIRM

- **Justification** of the new strict liability?
  - **economic consideration** (Cooter/Ulen, Law and Economics, 2016)**:** Liability is allocated where it can best be **insured**
  - **Central preventive measures** (e.g. customer education, process design) can take place
  - Double-sided incentive to avoid damage through negligence exemption

GÖRG

IHRE WIRTSCHAFTSKANZLEI

Involvement of third parties (telecoms, online platforms)

Discussion since June 2023

- **Proposals ECON Committee 14 February 2024:**

  - **Security measures by providers of electronic communications services,**
    - ✓ Removal of illegal or fraudulent content
    - ✓ Information / education of users, including alerts
    - ✓ Provide ways for users to report

  - **Obligation of all service providers in the fraud chain (PSP, telco, online platforms)**
    - ✓ to take technical and organisational measures

GÖRG

IHRE WIRTSCHAFTSKANZLEI

Conclusion

Small revolution and otherwise Fine Tuning

GÖRG
YOUR BUSINESS LAW FIRM

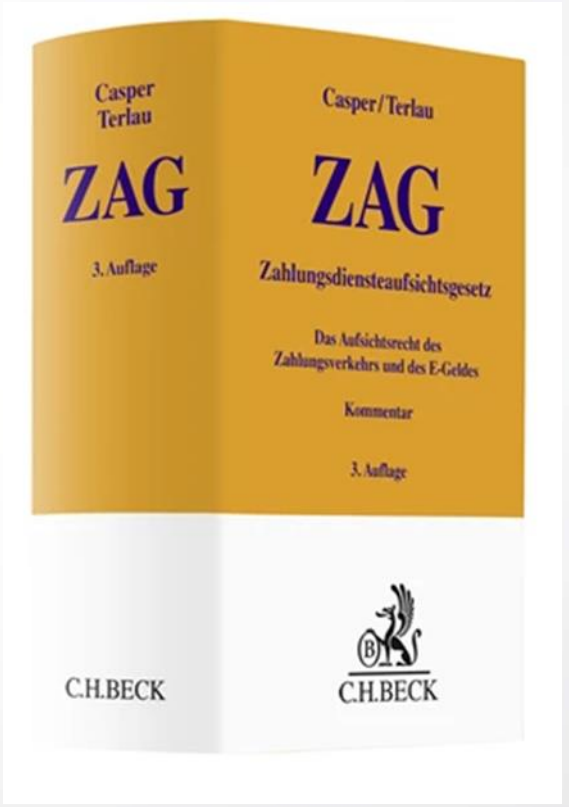
- through PSD3/PSR
  - Fraud prevention system intensively sharpened
  - PSR tries to close gaps in the payment security system
  - Significant additional liability obligations
  - SCA refined
  - Involvement of third parties in the fraud chain

- **Other challenges in the coming months**
  - Implementation of the Instant Payment Regulation
  - DORA

GÖRG
IHRE WIRTSCHAFTSKANZLEI

Thank you very much for your attention!

Further information at
payment-law.eu



Dr Matthias Terlau
Partner

Kennedyplatz 2
50679 Cologne
T: +49 221 33660-470
F: +49 221 33660-960
M: mterlau@goerg.de

Wrap-up

ABE EBA
EURO BANKING ASSOCIATION

ABE EBA
EURO BANKING ASSOCIATION

Thank you!

ABE EBA

EURO BANKING ASSOCIATION

Participants in the forum are reminded of their responsibility to observe anti-trust laws.

The EBA Anti-Trust Policy is available on the EBA website.

https://www.abe-eba.eu/media/azure/production/1352/eba_antitrust_policy_20170602_final_clean.pdf

ABE EBA

EURO BANKING ASSOCIATION

The forum is an open group, where interested stakeholders can discuss and exchange information on industry-wide topics.

The content of the slides presented and the views expressed in the context of the activities of the forum are those of the respective participants in the forum, and do not represent the views of the Euro Banking Association (EBA).