Solvency ii Association
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.solvency-ii-association.com

Solvency 2 News, July 2023

Dear members and friends,

The European Insurance and Occupational Pensions Authority published its June 2023 *Financial Stability Report,* which takes stock of the key developments and risks in the European insurance and occupational pensions sectors.

EIOPA notes that the European economy is currently experiencing a new period of high uncertainty and elevated financial stability risk.

Persistent inflation, the fraught geopolitical landscape and rising financing costs – also in the wake of the recent financial turmoil – pose challenges to growth prospects in Europe and the business conditions of financial institutions.

Despite the challenging environment, insurers and pension funds have remained resilient. European (re)insurers entered 2023 with robust solvency positions even in the face of sizeable natural catastrophe losses,

weaker investment returns, higher-than-expected inflation and continued economic uncertainties.

Premiums grew for non-life business but stagnated for life business. Underwriting profitability varied greatly across segments and declined overall.

Despite challenging renewal negotiations at the beginning of 2023, which lasted longer than usual and saw substantial price increases, insurers were able to obtain the reinsurance cover they sought.

Concerning investments, fixed income assets remain the dominant category for insurers, although the share of government and corporate bonds in their investment portfolios declined.

In 2022, insurers notably emerged as net sellers of corporate bonds and government bonds as they moved from more interest rate sensitive assets towards other, sometimes less liquid investment options.

Both insurers and occupational pension funds carry material direct exposures to the banking sector with 13% and 6% of their respective total investments exposed, albeit with a steadily falling trend since Q2 2019.

Occupational pension funds and insurers alike make use of derivatives to hedge against interest rate risk.

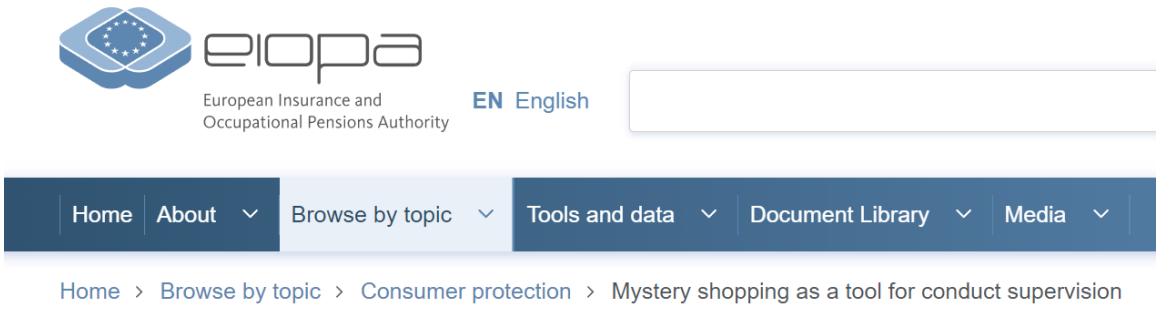
EIOPA's analysis included in this report has shown that insurers have enough liquid assets to cover potential margin calls resulting from a 100bps shift in the yield curve in either direction.

To read more:
https://www.eiopa.europa.eu/system/files/2023-06/EIOPA-BOS-23-209-EIOPA%20Financial%20Stability%20Report%20June%202023.pdf

EIOPA to undertake the first joint mystery shopping exercise across several EU Member States

The Board of Supervisors of the European Insurance and Occupational Pensions Authority (EIOPA) agreed today that EIOPA will coordinate the first joint mystery shopping exercise on sales of insurance.

The exercise will be conducted in 8 Member States and will follow a common methodology and criteria developed by EIOPA and its Members. The results of the exercise will be available in the first half of 2024.



Mystery shopping as a tool for conduct supervision

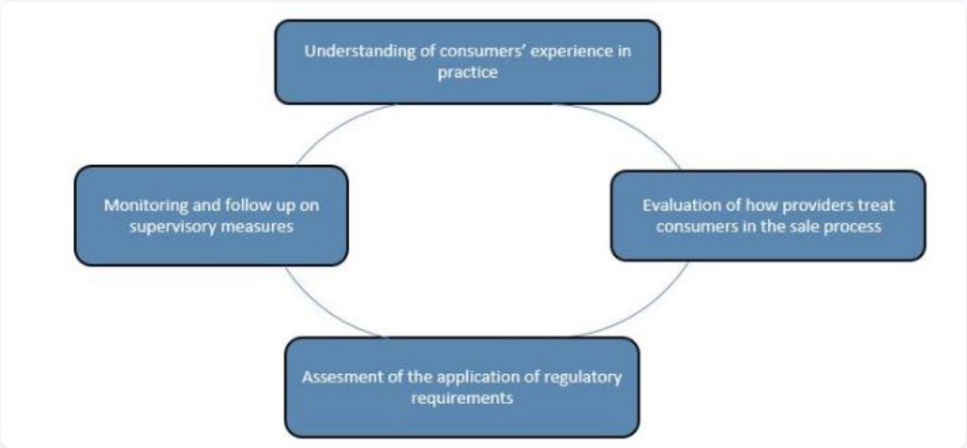
Mystery shopping is a technique that involves the use of trained “mystery shoppers” acting as potential customers. It allows the experience of customers in practice to be assessed.

It would typically involve physical visits to distributors’ premises but also can be done via digital channels, phone calls or similar methods.

The “mystery shoppers” act as any potential customer might (for instance, ask for information about product, request advice, explain their situation).

While doing so, they gather detailed information on how providers or distributors sell the products and provide services to consumers, in order to report back comparable and statistically relevant observations on consumers’ outcomes in a structured, detailed and systematic manner.

The main objectives of mystery shopping are:



Mystery shopping in relation to other matrket monitoring and supervisory tools:

To read more: https://www.eiopa.europa.eu/eiopa-undertake-first-joint-mystery-shopping-exercise-across-several-eu-member-states-2023-06-28_en

ECB welcomes European Commission legislative proposals on digital euro and cash

- Proposed legislation establishes framework facilitating the possible introduction of a digital euro that is widely usable and available throughout the euro area

- ECB also welcomes Commission proposal to protect legal tender status of euro cash

- Governing Council to decide in autumn whether to move to next phase of digital euro project

The European Commission has published today its legislative proposal on a digital euro. Like banknotes and coins are now, a digital euro would be a universal means of payment across the entire euro area.

The proposed legal tender status for the digital euro would ensure it is widely accepted as a means of payment.

The provision that people can get digital euros through their bank on request would make it easily accessible and ensures that nobody would be left behind.

The proposal also foresees that people could use basic digital euro services for free. At the same time, the proposal offers private intermediaries appropriate economic incentives to distribute the digital euro as they do

other digital means of payment, while preventing excessive fees for merchants.

Moreover, the proposed legislation supports a high degree of privacy and data protection for users, while minimising money laundering and terrorist financing risks. It enables offline digital euro payments, to provide cash-like privacy levels.

“The euro is the most tangible symbol of European integration”, said ECB President Christine Lagarde. “It is highly valued and trusted by citizens. We look forward to continuing working together with other EU institutions towards a digital euro to ensure our currency is fit for the digital age.”

The investigation phase of the digital euro project will conclude in October 2023. The Governing Council of the ECB will then decide whether to move to the next phase of the project.

In the next phase, the ECB would further develop and test the technical solutions and business arrangements. A possible decision by the Governing Council to issue a digital euro would be taken only after the legislative act is adopted.

“The legislative proposal is key to ensuring that the digital euro brings value to the people, taking the appreciated features of cash into the digital sphere”, said Executive Board member Fabio Panetta, who chairs the High-Level Task Force on a digital euro.

“The ECB also welcomes the Commission’s proposal on the legal tender status of euro cash, to ensure banknotes remain easily accessible for citizens and businesses and widely accepted throughout the euro area.”

The ECB welcomes the Commission’s proposal aiming to ensure that cash continues to be a vital part of the payments system. It is crucial that cash remains widely accepted in physical transactions in line with its legal tender status.

People and businesses need to be able to efficiently withdraw and deposit their money.

The legislative proposal ensures that both acceptance of and access to euro banknotes and coins is legally guaranteed, so that everyone who wants to pay with cash can do so.

The ECB stands ready to provide technical input to support the work of the EU co-legislators.

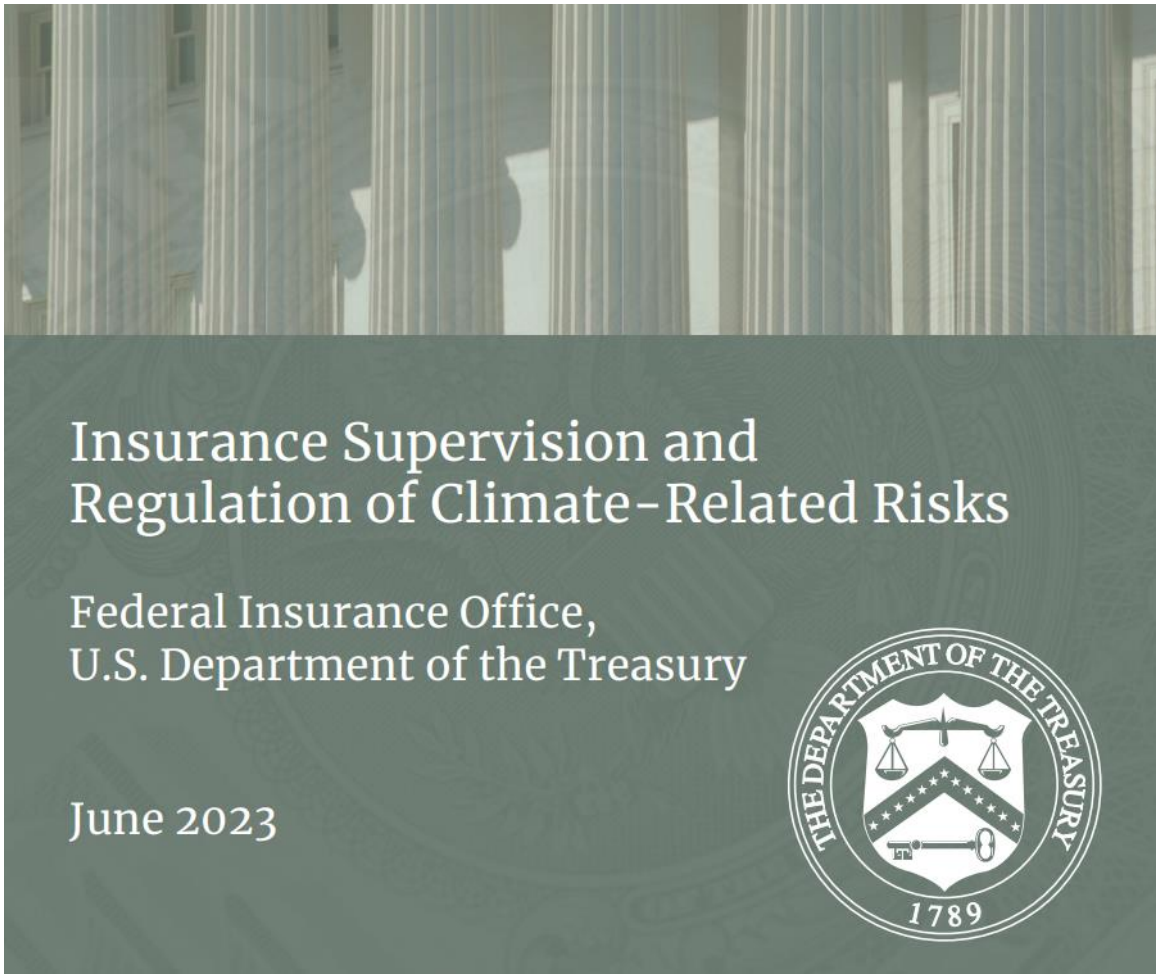
The European Commission has recommended that the European Parliament and the EU Council consult the ECB on the proposed legislative changes. Following requests for consultation, the ECB would deliver its opinion in due course.

To read more:
https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230628~e76738d851.en.html

Insurance Supervision and Regulation of Climate-Related Risks

Federal Insurance Office, U.S. Department of the Treasury

The Federal Insurance Office (FIO) prepared this Report in response to Executive Order 14030 on Climate-Related Financial Risk, which calls on the Secretary of the U.S. Department of the Treasury (Treasury) to direct FIO "to assess climate-related issues or gaps in the supervision and regulation of insurers, including as part of the [Financial Stability Oversight Council's] analysis of financial stability, and to further assess, in consultation with States, the potential for major disruptions of private insurance coverage in regions of the country particularly vulnerable to climate change impacts."



This Report addresses the first task by analyzing climate-related issues and gaps in U.S. insurance supervision and regulation.

After undertaking this analysis, FIO concludes that there are nascent and important efforts to incorporate climate-related risks into state insurance regulation and supervision.

FIO commends these initial efforts from the National Association of Insurance Commissioners (NAIC) and state insurance regulators. However, these efforts are fragmented across states and limited in several critical ways. FIO encourages state insurance regulators to build on their progress.

As highlighted in this Report, FIO will continue to prioritize climate-related work, in collaboration with our state and federal partners, including state insurance regulators, the NAIC, and the Financial Stability Oversight Council (FSOC).

TABLE OF CONTENTS

FIO's key findings and recommendations of this Report include:

• Climate-related risks—including physical, transition, and litigation risks—present new and increasingly significant challenges for the insurance industry. The oversight of climate-related risks is therefore an emerging and increasingly critical topic for state insurance regulators. Climate-related risks also warrant careful monitoring by financial regulators, policymakers, and insurers.

• State insurance regulators and the NAIC are increasingly focused on incorporating climate-related risks into supervision and regulation, but in most cases their efforts remain at a preliminary stage.

• Current regulatory frameworks provide state insurance regulators with tools they can adapt to better consider climate-related risks. The NAIC and some state insurance regulators are beginning to incorporate climate - related considerations into their regulatory tools.

• All state insurance regulators should prioritize efforts to adapt their regulatory and supervisory tools to incorporate climate-related risks. The NAIC and state insurance regulators should also prioritize the creation of new and effective climate-related risk tools and processes for use by state insurance regulators through, for example, the development of scenario analysis and increased use of the NAIC's Catastrophe (CAT) Modeling Center of Excellence.

• More work is needed by state and federal regulators and policymakers, as well as by the private sector and the climate science and research communities, to better understand the nature of climate-related risks for the insurance industry, their implications for insurance regulation and supervision, and for the stability of the financial system—including for real estate markets and the banking sector.

FIO makes 20 recommendations in this Report. The report includes important context for each recommendation, highlighting efforts that are already underway while also explaining how implementation of the recommendation could improve management and supervision of climate related risks.

The Report also proposes areas of focus for future work by state insurance regulators and the NAIC.

In Section II, the Report provides background on the significance of climate-related risks for the insurance industry and discusses the roles of the states, the NAIC, and FIO.

Section II then provides FIO's assessment of U.S. climate-related supervision and regulation of insurance in three categories:

(1) prudential (sometimes referred to as microprudential),

(2) macroprudential, and

(3) market conduct.

Section II concludes by reviewing several climate-related disclosure initiatives.

Section III discusses additional FIO priorities concerning climate-related risks; how insurance-related disaster mitigation efforts may increase the resilience of policyholders to climate-related disasters; and how FIO is engaging with domestic and international stakeholders on climate risk issues.

Finally, Section IV outlines next steps for FIO's work.

To read more: https://home.treasury.gov/system/files/136/FIO-June-2023-Insurance-Supervision-and-Regulation-of-Climate-Related-Risks.pdf

Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows

European Commission

The European Commission adopted its adequacy decision for the EU-U.S. Data Privacy Framework.

The decision concludes that the United States ensures an adequate level of protection – comparable to that of the European Union – for personal data transferred from the EU to US companies under the new framework.

EUROPEAN COMMISSION

Brussels, 10.7.2023
C(2023) 4745 final

COMMISSION IMPLEMENTING DECISION

of 10.7.2023

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework

On the basis of the new adequacy decision, personal data can flow safely from the EU to US companies participating in the Framework, without having to put in place additional data protection safeguards.

The EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by US intelligence services to what is necessary and proportionate, and establishing a Data Protection Review Court (DPRC), to which EU individuals will have access.
The new framework introduces significant improvements compared to the mechanism that existed under the Privacy Shield. For example, if the

DPRC finds that data was collected in violation of the new safeguards, it will be able to order the deletion of the data.

The new safeguards in the area of government access to data will complement the obligations that US companies importing data from EU will have to subscribe to.

President Ursula von der Leyen said:

“The new EU-U.S. Data Privacy Framework will ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the US has implemented unprecedented commitments to establish the new framework.

Today we take an important step to provide trust to citizens that their data is safe, to deepen our economic ties between the EU and the US, and at the same time to reaffirm our shared values. It shows that by working together, we can address the most complex issues.”

US companies will be able to join the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations, for instance the requirement to delete personal data when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties.

EU individuals will benefit from several redress avenues in case their data is wrongly handled by US companies. This includes free of charge independent dispute resolution mechanisms and an arbitration panel.

In addition, the US legal framework provides for a number of safeguards regarding the access to data transferred under the framework by US public authorities, in particular for criminal law enforcement and national security purposes. Access to data is limited to what is necessary and proportionate to protect national security.

EU individuals will have access to an independent and impartial redress mechanism regarding the collection and use of their data by US intelligence agencies, which includes a newly created Data Protection Review Court (DPRC). The Court will independently investigate and resolve complaints, including by adopting binding remedial measures.

The safeguards put in place by the US will also facilitate transatlantic data flows more generally, since they also apply when data is transferred by using other tools, such as standard contractual clauses and binding corporate rules.

Next steps

The functioning of the EU-U.S. Data Privacy Framework will be subject to periodic reviews, to be carried out by the European Commission, together with representatives of European data protection authorities and competent US authorities.

The first review will take place within a year of the entry into force of the adequacy decision, in order to verify that all relevant elements have been fully implemented in the US legal framework and are functioning effectively in practice.

Questions & Answers: EU-US Data Privacy Framework

1. What is an adequacy decision?

An adequacy decision is one of the tools provided under the General Data Protection Regulation (GDPR) to transfer personal data from the EU to third countries which, in the assessment of the Commission, offer a comparable level of protection of personal data to that of the European Union.

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland and Liechtenstein, to a third country, without being subject to any further conditions or authorisations. In other words, transfers to the third country can be handled in the same way as intra-EU transmissions of data.

The adequacy decision on the EU-U.S. Data Privacy Framework covers data transfers from any public or private entity in the EEA to US companies participating in the EU-U.S. Data Privacy Framework.

2. What are the criteria to assess adequacy?

Adequacy does not require the third country's data protection system to be identical to the one of the EU, but is based on the standard of ‘essential equivalence'. It involves a comprehensive assessment of a country's data protection framework, both of the protection applicable to personal data and of the available oversight and redress mechanisms.

The European data protection authorities have developed a list of elements that must be taken into account for this assessment, such as the existence of core data protection principles, individual rights, independent supervision and effective remedies.

3. What is the EU-U.S. Data Privacy Framework?

In its adequacy decision, the Commission has carefully assessed the requirements that follow from the EU-U.S. Data Privacy Framework, as well as the limitations and safeguards that apply when personal data transferred to the US would be accessed by US public authorities, in particular for criminal law enforcement and national security purposes.

On that basis, the adequacy decision concludes that the United States ensures an adequate level of protection for personal data transferred from the EU to companies participating in the EU-U.S. Data Privacy Framework. With the adoption of the adequacy decision, European entities are able to transfer personal data to participating companies in the United States, without having to put in place additional data protection safeguards.

The Framework provides EU individuals whose data would be transferred to participating companies in the US with several new rights (e.g. to obtain access to their data, or obtain correction or deletion of incorrect or unlawfully handled data). In addition, it offers different redress avenues in case their data is wrongly handled, including before free of charge independent dispute resolution mechanisms and an arbitration panel.

US companies can certify their participation in the EU-U.S. Data Privacy Framework by committing to comply with a detailed set of privacy obligations. This could include, for example, privacy principles such as purpose limitation, data minimisation and data retention, as well as specific obligations concerning data security and the sharing of data with third parties.

The Framework will be administered by the US Department of Commerce, which will process applications for certification and monitor whether participating companies continue to meet the certification requirements. Compliance by US companies with their obligations under the EU-U.S. Data Privacy Framework will be enforced by the US Federal Trade Commission.

4. What are the limitations and safeguards regarding access to data by United States intelligence agencies?

An essential element of the US legal framework on which the adequacy decision is based concerns Executive Order on ‘Enhancing Safeguards for United States Signals Intelligence Activities', which was signed by President Biden on 7 October and is accompanied by regulations adopted by the Attorney General. These instruments were adopted to address the issues raised by the Court of Justice in its Schrems II judgment.

For Europeans whose personal data is transferred to the US, the Executive Order provides for:

- Binding safeguards that limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;

- Enhanced oversight of activities by US intelligence services to ensure compliance with limitations on surveillance activities; and

- The establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court to investigate and resolve complaints regarding access to their data by US national security authorities.

5. What is the new redress mechanism in the area of national security and how can individuals make use of it?

The US Government has established a new two-layer redress mechanism, with independent and binding authority, to handle and resolve complaints from any individual whose data has been transferred from the EEA to companies in the US about the collection and use of their data by US intelligence agencies.

For a complaint to be admissible, individuals do not need to demonstrate that their data was in fact collected by US intelligence agencies. Individuals can submit a complaint to their national data protection authority, which will ensure that the complaint will be properly transmitted and that any further information relating to the procedure —including on the outcome— is provided to the individual.

This ensures that individuals can turn to an authority close to home, in their own language. Complaints will be transmitted to the United States by the European Data Protection Board.

First, complaints will be investigated by the so-called 'Civil Liberties Protection Officer' of the US intelligence community. This person is responsible for ensuring compliance by US intelligence agencies with privacy and fundamental rights.

Second, individuals have the possibility to appeal the decision of the Civil Liberties Protection Officer before the newly created Data Protection Review Court (DPRC).

The Court is composed of members from outside the US Government, who are appointed on the basis of specific qualifications, can only be dismissed

for cause (such as a criminal conviction, or being deemed mentally or physically unfit to perform their tasks) and cannot receive instructions from the government.

The DPRC has powers to investigate complaints from EU individuals, including to obtain relevant information from intelligence agencies, and can take binding remedial decisions. For example, if the DPRC would find that data was collected in violation of the safeguards provided in the Executive Order, it can order the deletion of the data.

In each case, the Court will select a special advocate with relevant experience to support the Court, who will ensure that the complainant's interests are represented and that the Court is well informed of the factual and legal aspects of the case. This will ensure that both sides are represented, and introduce important guarantees in terms of fair trial and due process.

Once the Civil Liberties Protection Officer or the DPRC completes the investigation, the complainant will be informed that either no violation of US law was identified, or that a violation was found and remedied. At a later stage, the complainant will also be informed when any information about the procedure before the DPRC—such as the reasoned decision of the Court— is no longer subject to confidentiality requirements and can be obtained.

6. When will the decision apply?

The adequacy decision entered into force with its adoption on 10 July.

There is no time limitation, but the Commission will continuously monitor relevant developments in the United States and regularly review the adequacy decision.

The first review will take place within one year after the entry into force of the adequacy decision, to verify whether all relevant elements of the US legal framework are functioning effectively in practice. Subsequently, and depending on the outcome of that first review, the Commission will decide, in consultation with the EU Member States and data protection authorities, on the periodicity of future reviews, which will take place at least every four years.

Adequacy decisions can be adapted or even withdrawn in case of developments affecting the level of protection in the third country.

7. What is the impact of the decision on the possibility to use other tools for data transfers to the United States?

All the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanism used. These safeguards therefore also facilitate the use of other tools, such as standard contractual clauses and binding corporate rules.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf

Enhancing Third-Party Risk Management and Oversight

A toolkit for financial institutions and financial authorities, consultative document

FSB FINANCIAL STABILITY BOARD

Executive summary

Financial institutions rely on third-party service providers for a range of services, some of which support their critical operations.

These dependencies have grown in recent years as part of the digitalisation of the financial services sector and can bring multiple benefits to financial institutions including flexibility, innovation and improved operational resilience.

However, if not properly managed, disruption to critical services or service providers could pose risks to financial institutions and, in some cases, financial stability.

The FSB has developed a toolkit for financial authorities and financial institutions as well as service providers for their third-party risk management and oversight.

The toolkit also aims to reduce fragmentation in regulatory and supervisory approaches across jurisdictions and different areas of the financial services sector, thereby helping mitigate compliance costs for both financial institutions and third-party service providers, and facilitate coordination among relevant stakeholders.

The toolkit comprises 4 main chapters.

Chapter 1 presents a list of common terms and definitions as a foundation. While complete harmonisation of terms is not always possible or desirable, a common understanding of terms and definitions can help improve clarity and consistency, assisting and enhancing communication among stakeholders under interoperable approaches.

Chapter 2 summarises the toolkit's approach. In particular, the primary emphasis is on critical services given the potential impact of their disruption on financial institutions' critical operations and financial stability.

It also looks holistically on third-party risk management, which is wider than a historical narrower focus on outsourcing, in light of changing

industry practices and recent regulatory and supervisory approaches to operational resilience.

Similar to the terms and definitions, the toolkit aims to promote interoperability of regulatory and supervisory approaches, short of full homogeneity.

Finally, the principle of proportionality is applicable throughout the toolkit, which allows the tools to be adapted to smaller, less complex institutions or intra-group third-party service relationships.

Chapter 3 sets out tools to help financial institutions identify critical services and manage potential risks throughout the lifecycle of a third-party service relationship.

These tools seek to help financial institutions to:

■ Identify critical services consistently yet flexibly;

■ Conduct due diligence, contracting and ongoing monitoring of critical services and service providers;

■ Be informed of incidents affecting critical services in a timely way;

■ Have consistent mapping of financial institutions' third-party service relationships;

■ Manage risks relating to their third-party service providers' use of service supply chain;

■ Implement and test business continuity plans and coordinate with their third-party service providers for their business continuity;

■ Develop effective exit strategies; and

■ Strengthen the identification and management of service provider concentration, and concentration-related risks.

Chapter 4 sets out financial authorities' current and developing approaches and tools for supervising how financial institutions manage third-party risks, and for identifying, monitoring and managing systemic third-party dependencies and potential systemic risks.

Table of Contents

In some jurisdictions or regions, financial authorities have or are in the process of acquiring regulatory powers to formally designate certain service providers as critical for the financial system and oversee these service providers and their services to financial institutions. However, this is not the case in other jurisdictions.

Accordingly, the tools in this toolkit are versatile and can be adopted through either voluntary collaboration between financial authorities, financial institutions and relevant service providers, requirements or expectations on financial institutions, or direct requirements or expectations on service providers.

Box 1: Examples of regimes

US Bank Service Company Act (BSCA)

The BSCA allows for the US Federal Banking Agencies (FBA) to supervise and regulate certain bank services provided by third parties. In particular, the BSCA provides that when an FBA-regulated bank or its affiliate causes to be performed for itself (by contract or otherwise) bank services, then the performance of the bank services is subject to regulation and examination by the FBA to the same extent as if those services were being performed by the bank. Title VIII of the Dodd-Frank Act also allows supervisory agencies of designated financial market utilities (DFMUs) – currently the FRB, SEC, and CFTC – to examine the provision of a service provided by another entity when such a service is "integral" to the operation of the DFMU.

EU Digital Operational Resilience Act (DORA)

DORA provides for the creation of an EU oversight framework for critical Information Communication Technologies (ICT) third-party service providers to EU financial entities. The European Supervisory Authorities (ESAs)[65] will designate critical ICT third-party service providers (there will also be an opt-in process for service providers to apply for voluntary designation even if they are not initially designated by the authorities). The ESAs have powers to request information, conduct investigations and inspections, issue recommendations to critical ICT third party service providers, impose periodic penalties to critical ICT third-party service providers who failed to comply with requests for information or refused to submit to investigations and inspections, and in certain circumstances to request financial entities to suspend or terminate the contracts for the provision of services by ICT critical third-party service providers. The rules in DORA will become applicable starting 17 January 2025. The drafting of accompanying regulatory and implementing technical standards, as well as guidelines is on-going.

Among other areas, the tools cover:

■ Incident reporting to financial authorities, including the possibility of enhancing the existing cyber reporting framework to include reporting by service providers where an incident could give rise to potential risks to financial stability;

■ Non-exhaustive criteria to help financial authorities identify systemic third-party dependencies and assess potential systemic risks; and

■ Tools to identify and manage potential systemic risks, including but not limited to sector wide exercises and incident response coordination frameworks.

Finally, the importance of cross-border supervisory cooperation and information sharing is underscored.

For this objective, the chapter sets out certain ways to explore greater convergence of regulatory and supervisory frameworks around systemic

third-party dependencies, options for greater cross-border information-sharing, and cross-border resilience testing and exercises.

To read more: https://www.fsb.org/wp-content/uploads/P220623.pdf

Financial Stability Institute, FSI Insights on policy implementation No 50

Banks' cyber security – a second generation of regulatory approaches

Juan Carlos Crisanto, Jefferson Umebara Pelegrini and Jermy Prenio

BANK FOR INTERNATIONAL SETTLEMENTS

Executive summary

Cyber resilience continues to be a top priority for the financial services industry and a key area of attention for financial authorities.

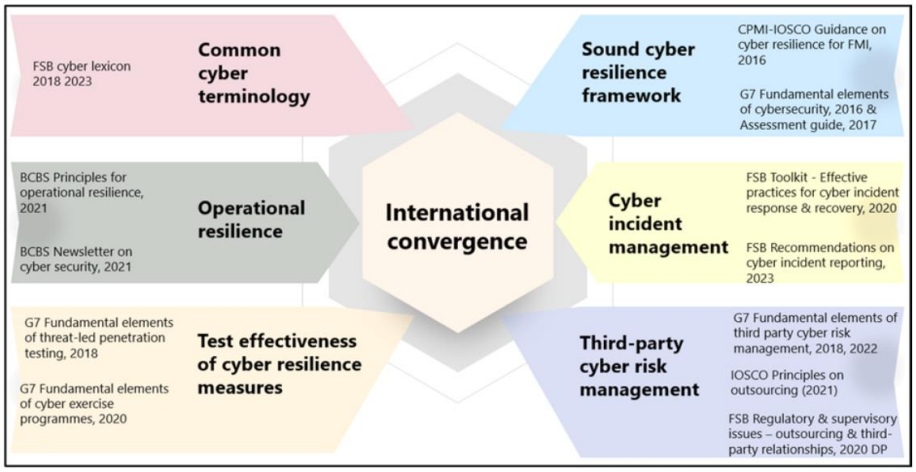
This is not surprising given that cyber incidents pose a significant threat to the stability of the financial system and the global economy.

The financial system performs a number of key activities that support the real economy (eg deposit taking, lending, payments and settlement services).

Cyber incidents can disrupt the information and communication technologies that support these activities and can lead to the misuse and abuse of data that such technologies process or store.

This is complicated by the fact that the cyber threat landscape keeps evolving and becoming more complex amid continuous digitalisation, increased third-party dependencies and geopolitical tensions.

Moreover, the cost of cyber incidents has continuously and significantly increased over the years.



This paper updates Crisanto and Prenio (2017) by revisiting the cyber regulations in the jurisdictions covered in that paper, as well as examining those issued in other jurisdictions.

Aside from cyber regulations in Hong Kong SAR, Singapore, the United Kingdom and the United States, which the 2017 paper covered, this paper examines cyber regulations in Australia, Brazil, the European Union, Israel, Kenya, Mexico, Peru, Philippines, Rwanda, Saudi Arabia and South Africa.

The jurisdictions were chosen to reflect cyber regulations in both advanced economies (AEs) and emerging market and developing economies (EMDEs). This highlights the fact that since 2017 several jurisdictions – including EMDEs – have put cyber regulations in place.

There remain two predominant approaches to the regulation of banks' cyber resilience: the first leverages existing related regulations and the second involves issuing comprehensive regulations.

The first approach takes as a starting point regulations on operational risk, information security etc and add cyber-specific elements to them.

Here, cyber risk is viewed as any other risk and thus the general requirements for risk management, as well as the requirements on information security and operational risks, also apply.

This approach is more commonly observed in jurisdictions that already have these related regulations firmly established.

The second approach seeks to cover all aspects of cybersecurity, from governance arrangements to operational procedures, in one comprehensive regulation.

In both approaches, to counter the risks that might result from having too much prescriptiveness in cyber regulations, some regulations combine broad cyber resilience principles with a set of baseline requirements.

Regardless of the regulatory approach taken, the proportionality principle is given due consideration in the application of cyber resilience frameworks.

Whether as part of related regulations or separate comprehensive ones, recent cyber security policies have evolved and could be described as "second-generation" cyber regulations.

The "first generation" cyber regulations, which were issued mainly in AEs, focused on establishing a cyber risk management approach and controls. Over the last few years, authorities, including those in EMDEs, have issued new or additional cyber regulations.

These second-generation regulations have a more embedded “assume breach” mentality and hence are more aligned with operational resilience concepts.

As such, they focus on improving cyber resilience and providing financial institutions and authorities with specific tools to achieve this.

The “second-generation” regulations leverage existing policy approaches to provide additional specific guidance to improve cyber resilience.

Cyber security strategy, cyber incident reporting, threat intelligence sharing and cyber resilience testing are still the primary focus of the newer regulations.

Managing cyber risks that could arise from connections with third-party service providers has become a key element of the “second generation” cyber security framework.

Moreover, there are now more specific regulatory requirements on cyber incident response and recovery, as well as on incident reporting and cyber resilience testing frameworks.

In addition, regulatory requirements or expectations relating to issues such as cyber resilience metrics and the availability of appropriate cyber security expertise in banks have been introduced in a few jurisdictions.

Authorities in EMDEs tend to be more prescriptive in their cyber regulations.

Cyber security strategy, governance arrangements – including roles and responsibilities – and the nature and frequency of cyber resilience testing are some of the areas where EMDE authorities provide prescriptive requirements.

This is approach seems to be connected to the need to strengthen the cyber resilience culture across the financial sector, resource constraints and/or the lack of sufficient cyber security expertise in these jurisdictions.

Hence, EMDE authorities may see the need to be clearer in their expectations to make sure banks’ boards and senior management invest in cyber security and banks’ staff know exactly what they need to do.

International work has resulted in a convergence in cyber resilience regulations and expectations in the financial sector, but more could be done in some areas.

Work by the G7 Cyber Expert Group (CEG) and the global standard-setting bodies (SSBs) on cyber resilience has facilitated consistency in financial regulatory and supervisory expectations across jurisdictions.

This is necessary given the borderless nature of cyber crime and its potential impact on global financial stability.

Another area where there might be scope for convergence is the way in which authorities assess the cyber resilience of supervised institutions. This could, for example, include aligning the assessment of adequacy of a firm's cyber security governance, workforce and cyber resilience metrics.

Lastly, there might be scope to consider an international framework for critical third-party providers, in particular cloud providers, given the potential cross-border impact of a cyber incident in one of these providers.

Contents

Comparative description of the first and second generation of cyber regulations. Table 1

	1st generation (2017 paper)	2nd generation (2023 paper)
Conceptual underpinning	Focus on building "strong perimeter"	More embedded "assume breach" mentality
Scope	Aligned with IT/ICT and information security framework	In addition, aligned with operational resilience framework
Requirements	Emphasis on enhancing security capabilities	Emphasis on improving resilience capabilities
	Guidance/expectations regarding cyber risk management and (typical) security controls	In addition, guidance/expectations regarding key aspects of cyber resilience framework
	Third-party dependencies largely managed through outsourcing lens	Third-party dependencies increasingly becoming a key part of cyber resilience framework
Types of rules	(i) Leverage existing regulations and (ii) "all-in-one" cybersecurity frameworks	In addition, (iii) principles plus baseline requirements
Tailoring	Apply proportionality approach	
References	In addition to SSB & G7 guidance, well-established technical standards on cyber & information security	

To read more:
https://www.bis.org/fsi/publ/insights50.pdf

Financial stability in the world of geopolitical fragmentation and rapid technological change

Olli Rehn, Governor of the Bank of Finland, at the 2023 RiskLab – BoF - ESRB Conference on Systemic Risk Analytics, organised by the RiskLab (at Arcada), the Bank of Finland and the European Systemic Risk Board.

SUOMEN PANKKI EUROJÄRJESTELMÄ FINLANDS BANK EUROSYSTEMET

Good morning Ladies and Gentlemen, Friends and Colleagues,

Let me welcome you to the Conference on Systemic Risk Analytics, jointly organised by the RiskLab [at Arcada], Bank of Finland and the European Systemic Risk Board. I also welcome you to the Bank of Finland – Suomen Pankki – the fourth oldest central bank in the world, established in 1811.

In my opening remarks, I will focus on financial stability in the world of geopolitical fragmentation and rapid technological change.

Meanwhile, I will not even touch upon monetary policy, as we have just started the ECB's silent period a few hours ago.

Let me begin by noting that the global financial system and banking system have remained remarkably resilient after the global financial crisis, despite recently being hit by waves of unexpected shocks: COVID-19, Russia's brutal and illegal war against Ukraine, and a sharp increase in inflation.

However, the failure of the Silicon Valley Bank and some smaller banks in the US, as well as the forced sale of Credit Suisse to UBS just three months ago – the "March Madness" – reminded us that we can never take financial stability for granted.

With that in mind, I am very much looking forward to hearing Steven Cecchetti's views on how to make banking safer, in his keynote speech right after these opening remarks.

I also appreciate the strong focus of this conference on non-bank financial intermediation and climate risks. The role of non-banks like money market funds and insurance companies in the global financial system has clearly been increasing.

And it goes without saying that climate change, if not properly addressed, may create serious risks also to financial stability.

Dear Colleagues,

In the last few years, we have seen that crises can happen at any time and take unexpected forms. Just after the world had recovered from the pandemic, the war broke out in Europe.

The geopolitical environment is now changing as rapidly as it did in the late 80s and early 90s. At that time, the Berlin Wall crumbled, the Soviet Union collapsed, Eastern Europe broke free, Europe was united and China was integrated into the world economy. The world became a safer and more prosperous place to live – for a while.

Now, sadly, we are moving in the opposite direction, towards a new Cold War and a breakdown in international cooperation. Autocracies like Russia and China are forcibly challenging the rules-based international order.

The security policy environment of Europe is being transformed as fundamentally as it was 30 years ago, only this time in reverse.

The current geopolitical headwinds are detrimental also to the world economy. In the last few years, some have even predicted the end of globalisation.

Fortunately, the rumours on the death of globalisation have thus far proven to be exaggerated. In fact, the volume of world trade has already surpassed its pre-pandemic levels and is now close to its record level.

At the same time, however, protectionism and friend-shoring are increasing and supply chains are being shortened.

In the world of high geopolitical tensions, strengthening and maintaining the resilience of the financial system has become ever more important.

To make the financial system safe and resilient, we need rigorous financial regulation and supervision. We also need high-quality macroprudential analysis and policy – another of the key topics of this conference.

Several sessions and presentations of this event are devoted to the analysis of the impacts of different macroprudential measures – both borrower-based and capital-based measures – on households and banks, housing and labour markets, and even on tackling climate change.

Let me try and complement the forthcoming presentations with some thoughts on how macroprudential policymaking in Europe could potentially be improved.

First, it would be useful if the application of the capital-based macroprudential tools, especially the so-called O-SII buffer requirements, was based on more uniform criteria across the EU.

In highly integrated banking markets, banks with equal or close to equal systemic importance should not have very different capital buffer requirements. Similar application of tools would foster a level playing field and reduce any pockets of vulnerabilities.

Second, in the longer term, the borrower-based tools targeting housing loans and household indebtedness should be based on some minimum and common EU level requirements. At the moment, those tools are solely based on national legislation and are rather diverse across countries.

In addition to credit institutions, these EU level regulations should be applied to all lenders providing housing loans. Such regulations may not be needed right now. But they could be useful next time when the lending cycle starts to rise again.

Third, the EU legislation should explicitly allow the use of the so-called positive neutral countercyclical capital buffer requirement. National macroprudential authorities should be able to set that buffer requirement at a positive level during normal times.

In times of unexpected and sudden crises, the buffer could be flexibly released, if needed, to support bank lending and economic recovery.

Dear Friends,

In addition to Steven Cecchetti's keynote starting in a minute, I believe you are eagerly awaiting the other two keynote speeches of this conference: Alex Jung's presentation on machine learning and Michael Platzer's on AI-generated synthetic data.

Before those, let me tell you about my forgotten history in computer programming. In high school – that is, only few years ago – I was an avid member of our school's automated data programming club.

There we, for example, practised programming languages BASIC and FORTRAN after school.

Unfortunately, the school did not have any computers! So, we wrote our BASIC and FORTRAN codes only on paper. Not surprisingly, the local football club's training matches, taking place at the same time, began to feel more attractive.

So, the world lost one potential coder in me. I'll let you judge whether monetary policy was ultimately a winner or loser in that outcome.

Even more seriously, the potential threats and opportunities of artificial intelligence and machine learning are very hotly debated at the moment.

I think we may assume that in the field of financial services, the developments in AI and machine learning can bring substantial benefits, for example in risk management, loan underwriting and customer behaviour analysis. The developments may also help the work of supervisors.

That said, we should be aware of the potential dangers of the misuse of such powerful tools. Above all, we should improve our understanding of these fascinating technological developments, also in order to make better policy choices. In that, the forthcoming keynote speeches will be most helpful.

With these words, let me wish you a stimulating and productive conference!

To read more: https://www.suomenpankki.fi/en/media-and-publications/speeches-and-interviews/2023/governor-olli-rehn-financial-stability-in-the-world-of-geopolitical-fragmentation-and-rapid-technological-change/

Building together a future-proof banking and payment sector in Europe

François Villeroy de Galhau, Governor of the Banque de France

Ladies and Gentlemen,

I am pleased to be with you for this Global Official Institutions Conference organised by BNPP, and I extend my warmest thanks to Jean Lemierre, Chairman of BNPP's board of directors, for his invitation to give this speech.

Facing the obvious turbulence and challenges of the last 18 months, we come here from different perspectives. Let me focus nevertheless on some common features: I will take the European view, and not only the French one. And I will focus on two delicate interactions between public authorities and private sector financial institutions:

- the first one is about the recent past: why did the euro area escape the banking turmoil born in the US and in Switzerland, and can we be safe enough? (I)

- the second one is about the next future: why should Central banks stand ready to issue a digital currency? (II)

I. Banking turmoil: three blessings and a funeral

I spoke after SVB's failure of 'Three blessings and a funeral'. Let me start with the funeral, at least the one that we can welcome, but which, unfortunately, is not final. It should be the condemnation and the funeral of mismanagement.

Blatant mismanagement of the risks and of the business model in some banks explains first and foremost the recent turmoil. It must be reiterated, SVB's business model was fortunately an outlier, and the rise in interest rates generally benefits European banks, thanks to their diversified deposit base and large loan portfolio.
As president of the French prudential authority, I can attest to French banks' robustness: their net banking income increased by 5.3% in 2022, and their revenues remain on a high track in 2023.

After the (temporary, alas) funeral, let me come to the three blessings. This word is a bit self-centred, I confess, since I am referring to public policies. But the blessings refer first to two reasons why the US banking crises did not affect the euro area this time: our regulation, and our supervision.

As regards regulation, Basel III in its entirety applies to all European banks, but only to 13 banks in the United States.

According to a number of estimates, including our own, SVB's short-term liquidity ratio (LCR), had it been applicable, would have been below the 100% requirement, which would have been an early warning signal – for memory's sake, all liquid assets are booked at fair market value in this ratio.

The priority is therefore not to keep reworking the Basel requirements - and thus delaying their implementation - but to implement them everywhere and quickly, as the Fed Vice Chair's – Michael Barr – report suggested it in April.

In short, more Basel III now, rather than a hypothetical and delayed Basel IV. However, there are two issues to consider: the increased speed of deposit withdrawals - connected with digitalisation and social networks - raises new challenges.

None of the ideas put forward on this subject are clear-cut, but none should be taboo. Moreover, the lack of liquidity and transparency in the single-issuer CDS market must no longer give rise to systemic risks: as a first step, we must ensure a better understanding of the transactions, the participants and the correlation risk with other financial instruments.

Let me now turn to supervision. Why did Credit Suisse fail despite meeting the requirements of Basel III? The answer is clear: good regulation is necessary; but it is never enough.

A Highway Code - regulations -, even the best one in the world, will only be effective if the traffic police - supervisors - are efficient. Risks generated by specific business models should lead to stricter requirements.

This is precisely the spirit of "Pillar 2" of the Basel framework. Supervision can and must be responsive, intrusive - including with on-site inspections - , exercised by highly qualified professionals, and applied forcefully.

This is not wishful thinking: this active supervision is one of the greatest success stories of our European Banking Union. The SSM demonstrates the benefits of bringing all players under one main authority only, rather than regional ones, with clearly defined responsibilities and coordination.

Furthermore, our active supervision demonstrates the strong value of regular stress tests, which are this year typically based on a sharp rise in short and long-term interest rates: this is the way we in Europe already deal actively with IRRBB, including for smaller institutions.

Resolution is the third ‘blessing’, also less operational. The fact that the Swiss authorities opted for a merger in the case of Credit Suisse raised new questions about how to make resolution more reliable.

Let me share just some thoughts at this point. The first concerns the resolution of large or even systemically important banks. The provision of potentially significant amounts of liquidity in times of crisis is a prerequisite for successful resolution.

The framework for the ECB to provide "Eurosystem resolution liquidity" has yet to be built. The other priority, at the other end of the spectrum, is to shift from resolution "for a minority" - a far too small minority of cases: two in the last nine years - to resolution "for the majority" of cases, including small and medium-sized banks.

The European Commission's proposal for a revised crisis management and deposit insurance (CMDI) framework is a step in the right direction.

Yet, level-playing field must be ensured not to give unfair advantage to smaller banks; and greater pooling between the Resolution Fund and deposit guarantee schemes should not lead to large companies potentially benefiting from the same protection as the smaller deposits of individuals or SMEs.

II. The digital currency for a changing world

Let me now turn to my second topic: the technological evolutions underway in the fields of finance and payments, which has led us, the Eurosystem, to have launched an investigation phase on a retail central bank digital currency (CBDC) under the sponsorship of President Christine Lagarde and my friend and colleague Fabio Panetta.

Pending an approval by the Governing Council, a preparation phase will then start at the end of this year, before a potential and gradual launch from 2027 or 2028 onwards. I am aware I am entering here a less consensual ground, listening to banks’ doubts along two arguments

(i) the CBDC would be a ‘solution in search of a problem’, the ‘why?’ question

(ii) and the CBDC would be a competitor to commercial bank money.

The purpose: a digital banknote

About the 'why?', I can imagine that two centuries ago, there were many voices questioning the need for a paper banknote – at that time a huge technical innovation – to be issued along the good old gold and silver coins.

Today, it all boils down to one simple question: as everything is becoming digital, why should central bank money be the only thing to remain in paper?

As many of you know, central banks have also – and fortunately so – innovation in their DNA, keeping pace with technological disruptions. The Eurosystem has made headway on the design of the digital euro, including through regular exchanges with consumer associations, merchants and financial players, and the testing of dedicated prototypes.

To put it in a nutshell, the e-euro will be a digital banknote, or 'Cash+'. Naturally, it will feature the same characteristics as existing cash.

Notably, it will ensure privacy, with the offline functionality ensuring the highest level of confidentiality; it will be the safest of assets; thanks to its likely legal tender status, it will be accepted everywhere across the euro area; and its basic functionalities will be free of charge for individuals.

But 'Cash+', bringing significant advantages compared with banknotes: it will allow each and every one to use central bank money in e-commerce, in remote peer-to-peer payments, as well as for conditional payments.

I think it's our duty to build this capacity for our fellow citizens, but it will be their freedom to use it.

The digital euro will offer European citizens an additional option in the way they make purchases and transactions, and they will determine the pace of its development, and its 'market share'.

A digital euro will not replace physical cash or other forms of money, and this brings me to this alleged 'competition' issue.
Money is and will remain a public-private partnership

For a long time now, money has been a public-private partnership. We need the skills of both sides: the agility, innovations, customer relations of commercial banks; and the trust and stability guaranteed by Central banks.

Yes, digital commercial bank money already exists, and is usually regarded as safe as central bank money; it will remain very significant in payment amounts, and you may possibly develop tokenised deposits.

But the trust commercial bank money inspires is not only due to each bank's private signature; it's anchored by its full equivalence and permanent convertibility, 1:1, to the public money issued by the Central bank.

Loosing this public anchor – in a world of digital payments without CBDC – would sooner or later mean undermining this private trust; think of the 19th century in the United States, before the Fed, where there were regularly confidence crises.

To make it crystal-clear, a digital euro will not lead to disintermediation. It will be distributed through banks: we central banks have absolutely no intention to open private accounts.

In response to some other worries, there will be no financial stability risks, due to possible significant outflows from commercial bank money to central bank money: a holding limit will apply to digital euro accounts, and it will ensure that the digital euro serves as a payment means, more than as a store of value.

So commercial banks can and should get on board with full confidence. We are, in this 21st century as in the two previous ones, complementary and not competitors on money and payments. As said, it's very probably our duty to issue a CBDC, but it's our will to issue it with you, commercial banks, and not against you.

Developing a scheme of shared benefits for all stakeholders

More generally, I would like to insist that there can be benefits for every stakeholder along the chain. The 'economic equation' can be worked out so that each and every one – including banks and merchants – has a direct interest in being part of it, like for cash issuance today.

We are well aware that, to quote the words of our host, payments have gone from being a simple convenience to a central element of banks' relationships with their customers, and we strongly desire that this will continue to be the case.

The European payment ecosystem as a whole will also benefit from the digital euro, rather than giving ground to so called 'stablecoins' probably issued by non-European players.

The scheme we are currently developing will enable the emergence of open acceptance standards on a pan-European scale, fostering convergence and enabling all players to build further innovations on common ground.

In short, a digital euro will act as a 'platform for innovation' – including for solutions in commercial bank money, which will benefit from the acceptance standards of the digital euro.

Let me stress in this regard that for instance the European Payment Initiative (EPI), which we strongly support, successfully tested and integrated the digital euro during the prototyping exercise organised by the Eurosystem over the past few months. This success should urge European banks to join both initiatives and related working groups.

In the same spirit, we – Banque de France and ECB – are actively working with financial institutions on wholesale CBDC. Our shared purpose is twofold: fostering tokenised finance and tokenised securities; facilitating cross-border interoperability. We will publish an update of our wholesale experiments by early July.

The two topics I have touched upon today may seem hardly connected to one another, but they actually have something very strong in common: ensuring the European banking and payment sector is fit for purpose in a rapidly changing technological landscape.

Looking ahead, as Abraham Lincoln once put it, 'the best way to predict the future is to create it'. Let us do it together, as talented and committed Europeans.

I thank you for your attention.

To read more: https://www.banque-france.fr/en/intervention/building-together-future-proof-banking-and-payment-sector-europe

Trust Services & Digital Wallets: Moving to the Cloud and Remote Identity Proofing

In order to address the cybersecurity questions of remote identity proofing, the European Union Agency for Cybersecurity (ENISA) organised a workshop to support the area of Trust Services and Digital Wallets and published a report on moving trust services to the cloud.

Report on Trust Services: Secure Move to the Cloud of the eIDAS ecosystem

For the purpose of the report, ENISA conducted a survey with more than 120 stakeholders from over 29 countries in the EU and globally. The survey allowed to get an insight of practical experiences of Trust Service Providers, Conformity Assessment Bodies, Supervisory Bodies and Cloud Service Providers regarding the transition of trust services to the cloud.

Moving trust services to the cloud must be understood as an ongoing process that has to be followed step by step.

While some services – such as the validation of signatures, registered delivery, time stamp or signature preservation – are moved rather quickly, other services – such as the issuance of certificates and remote control over the signing device – require in-depth analysis and preparation.

The transition of data to the cloud has to be secure at all times and, in the best case, must remain in the data centre of the trust services provider.

This report has given a detailed overview of the issues to be addressed for such a transition, including the related challenges, impediments and opportunities.

Workshop on Remote Video Identification: Attacks and Foresight

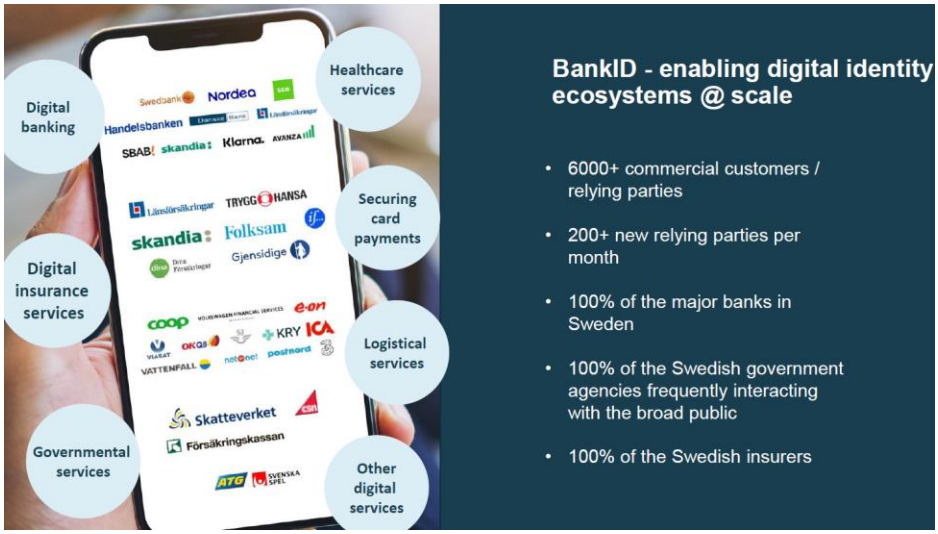
The workshop was the occasion for ENISA to publish its report exploring the secure move to the cloud of the eIDAS ecosystem. In cooperation with the European Competent Authorities for Trust Services (ECATS) expert group, ENISA organised a workshop on 10 May 2023 in Amsterdam, Netherlands.
The purpose of the workshop was to explore and discuss the latest national implementations, existing and emerging attacks, and the security measures envisaged for the protection of remote identity proofing across the EU.

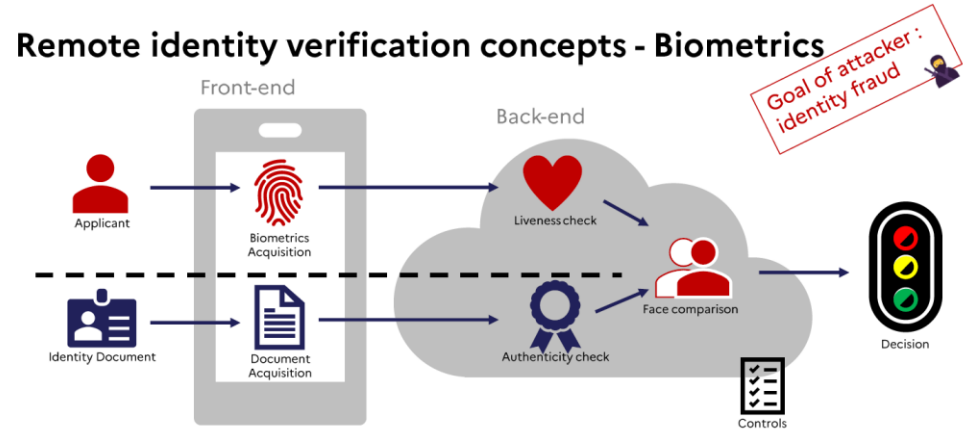
Over 100 participants attended the workshop and included representatives from Supervisory Bodies, Identity and trust service providers, conformity assessment bodies, standardisation bodies and research community.

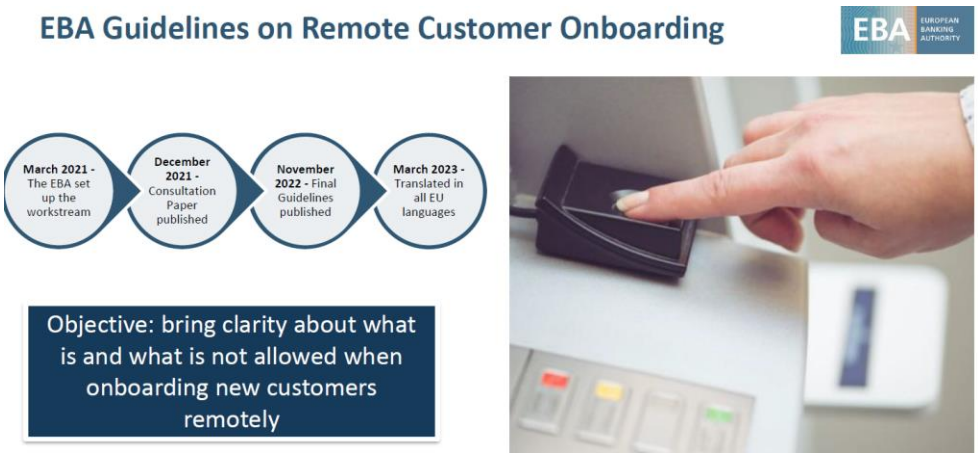
The workshop addressed the following main challenges:

- lack of EU legislation harmonisation;
- how to keep up with technological advancements connected to AI;
- the testing and performance measuring landscape;
- how to continuously follow the supply chain of products and services.

For the presentations you may visit:
https://www.enisa.europa.eu/events/remote-video-identification-attacks-and-foresight







Meeting of the European Competent Authorities for Trust Services (ECATS) Expert Group

The Dutch Supervisory Authority hosted the 21st meeting of the ECATS on 11 and 12 May, back-to-back with the meeting of FESA (Forum of European Supervisory Authorities).

The group discussed latest developments in eIDAS2, the connection between the upcoming implementation of the NIS 2 and eIDAS2, as well as updates on standardisation and certification in relation to trust services.

The ECATS EG is the informal group focusing to facilitates voluntary and informal collaboration between competent authority experts from EU Member States, European Economic Area (EEA) and European Free Trade Association (EFTA) States, EU Candidate countries and other relevant stakeholders to ensure smooth and secure functioning of trust services.

To read more: https://www.enisa.europa.eu/news/trust-services-digital-wallets-moving-to-the-cloud-and-remote-identity-proofing

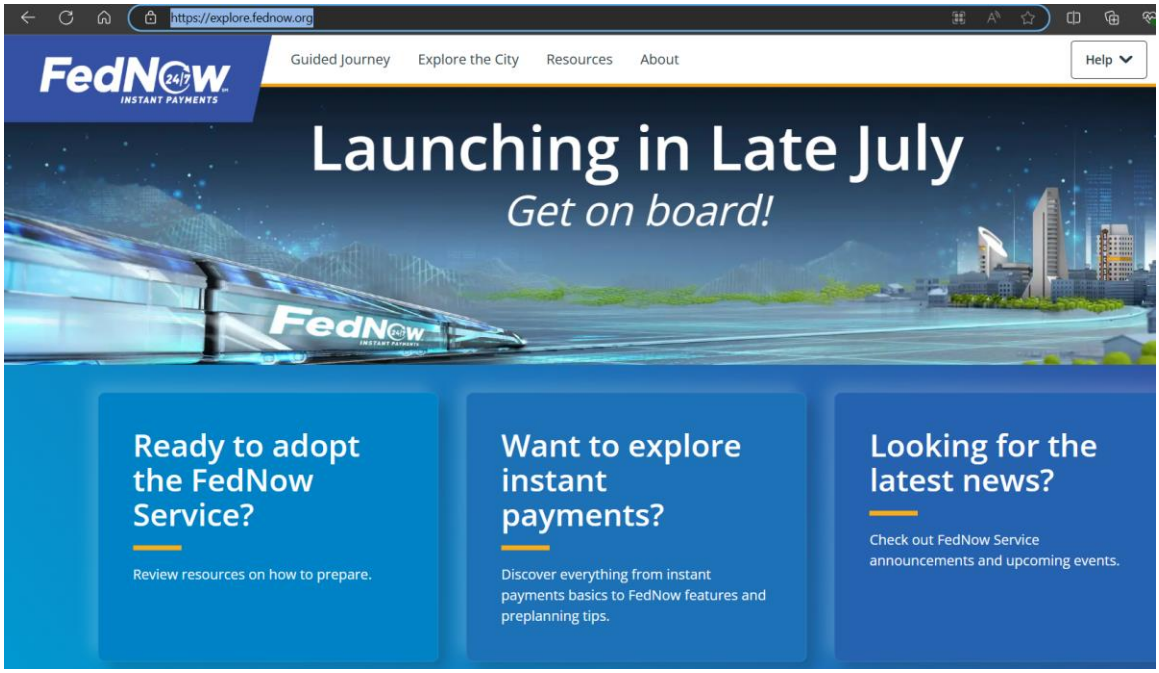
Federal Reserve names organizations certified as ready for FedNow® Service

About the FedNow Service

The Federal Reserve Banks are developing the FedNow Service to facilitate nationwide reach of instant payment services by financial institutions — regardless of size or geographic location — around the clock, every day of the year.

Through financial institutions participating in the FedNow Service, businesses and individuals will be able to send and receive instant payments at any time of day, and recipients will have full access to funds immediately, giving them greater flexibility to manage their money and make time-sensitive payments.

Access will be provided through the Federal Reserve's FedLine® network, which serves more than 10,000 financial institutions directly or through their agents.



For more information: https://explore.fednow.org

57 early adopter organizations

The Federal Reserve announced that 57 early adopter organizations, including financial institutions and service providers, have completed formal testing and certification in advance of the FedNow Service's launch planned for late July.

Organizations that have completed certification in the FedNow Service

Participants

- 1st Bank Yuma
- 1st Source Bank
- Adyen
- Alloya Corporate Federal Credit Union
- Atlantic Community Bankers Bank
- Avidia Bank
- Bankers' Bank of the West
- BNY Mellon
- Bridge Community Bank
- Bryant Bank
- Buffalo Federal Bank
- Catalyst Corporate Federal Credit Union
- Community Bankers' Bank
- Consumers Cooperative Credit Union
- Corporate America Credit Union
- Corporate One Federal Credit Union
- Eastern Corporate Federal Credit Union
- First Internet Bank of Indiana
- Global Innovations Bank
- HawaiiUSA Federal Credit Union
- JPMorgan Chase
- Malaga Bank
- Mediapolis Savings Bank
- Michigan Schools & Government Credit Union
- Millennium Corporate Credit Union
- Nicolet National Bank
- North American Banking Company
- PCBB
- Peoples Bank
- Pima Federal Credit Union
- Quad City Bank & Trust
- Salem Five Bank
- Star One Credit Union
- The Bankers Bank
- United Bankers' Bank

- U.S. Bank
- U.S. Century Bank
- U.S. Department of the Treasury's Bureau of the Fiscal Service
- Veridian Credit Union
- Vizo Financial Corporate Credit Union
- Wells Fargo Bank, N.A.

Service Providers

- ACI Worldwide Corp.
- Alacriti
- Aptys Solutions
- ECS Fin Inc.
- Finastra
- Finzly
- FIS
- Fiserv Solutions, LLC
- FPS GOLD
- Jack Henry
- Juniper Payments, a PSCU Company
- Open Payment Network
- Pidgin, Inc.
- Temenos
- Vertifi Software, LLC

Many of these organizations will be live when the FedNow Service launches or shortly after, with financial institutions ready to send and receive transactions and service providers ready to support transaction activity.

This group of early adopters is now performing final trial runs on the service to confirm their readiness to support live transactions over the new instant payments infrastructure. The early adopters include 41 financial institutions participating as senders, receivers and/or correspondents supporting settlement, 15 service providers processing on behalf of participants, and the U.S. Department of the Treasury.

"We are on track for the FedNow Service launch, with a strong cohort of financial institutions and service providers of all sizes in the process of completing the final round of readiness testing," said Ken Montgomery, first vice president of the Federal Reserve Bank of Boston and FedNow program executive. "With go-live nearing, financial institutions and their industry partners should be confident in moving forward with plans to join the network of organizations participating in the FedNow Service."

Over time, financial institutions are expected to adopt and build on the FedNow Service with the goal of offering new instant payments services to their customers. Montgomery noted that as a platform for innovation, the FedNow Service is intended to support multiple use cases, such as account to account transfer, request for payment, bill pay, and many others.

In addition to working with early adopters, the Federal Reserve continues to work with and onboard financial institutions planning to join later in 2023 and beyond, as the initial step to growing a robust network aiming to reach all 10,000 U.S. financial institutions.

FedNow 24/7 INSTANT PAYMENTS

THE FEDERAL RESERVE Financial Services

RISK MANAGEMENT AND ERROR RESOLUTION

FedNow participants will be able to configure preferences and use ISO® 20022 messages to help with their efforts to mitigate fraud and to resolve errors.

Participation type

The FedNow Service will offer different ways to participate in the service so that participants can enable the options that best match their needs and risk profile. For example, financial institutions may choose to support customer credit transfers, but elect not to support liquidity management transfers.

Accept without posting

Participants may submit an "accept without posting" status back to the originating financial institution indicating that further information is required with respect to compliance considerations before accepting the payment.

Request for information

Financial institutions may request another FedNow participant provide additional information on a transaction or request for payment message – for example, if the receiver financial institution would like to request further details about a sender.

Return request

Financial institutions may submit a "return request" message to request another FedNow participant return the amount of a transaction identified as fraudulent.

FedNow Is Coming in July. What Is It, and What Does It Do?

Michael Lee and Antoine Martin

FEDERAL RESERVE BANK *of* NEW YORK

On March 15, the Federal Reserve announced that the FedNow Service will launch in July 2023. FedNow will "facilitate nationwide reach of instant payment services by financial institutions—regardless of size or geographic location—around the clock, every day of the year."

But what exactly is the FedNow Service, and what does it do? In this article, we describe FedNow at a high level, offer answers to common and anticipated questions about the service, and explain how it will support the provision of instant payment services in the United States.

A New and Different Payment "Rail"

At its core, FedNow is an interbank instant payment infrastructure. Banks, credit unions, and other eligible institutions have accounts at the Federal Reserve. These Fed accounts allow institutions to hold reserves.

Banks pay each other by transferring reserves from the paying bank's Fed account to the receiving bank's Fed account using several interbank payment options. FedNow is a new addition to the suite of options to make such transfers.

What differentiates FedNow from other payment rails is that it is specifically designed to support instant retail payments. With such payments in mind, FedNow's most important feature is that it will operate 24 hours a day, seven days a week, year-round.

With FedNow, financial institutions will be able to clear and settle retail payments instantly at any time, including nights and weekends.

Still, FedNow shares some characteristics with existing payment systems. It is an interbank system, like ACH and Fedwire. In addition, FedNow, like Fedwire but in contrast to ACH, will be a real-time gross settlement (RTGS) system.

This means that every transaction of FedNow will be processed in real time, whenever the paying bank chooses to send the payment, and settled on a gross basis, payment by payment, rather than periodically settling several payments in batch.

Will retail customers get to use FedNow directly? The short answer is no, at least not directly. Instead, FedNow will support instant payment services,

to which individuals will have access through their financial institutions, if these institutions adopt FedNow.

Banks and credit unions that offer retail payment services will be able to use FedNow to clear and settle retail transactions and instantly make funds available to both merchant and customer.

Supporting Instant Retail Payments

If banks can already use an effective RTGS system like Fedwire to settle their payments, why is it necessary to build a new system? The answer is that existing interbank payment systems in the United States are not well suited to support instant retail payments.

The goal of an instant retail payment system is to allow consumers and businesses to transfer funds at any time, from anywhere, and for these funds to be available to the recipient immediately.

Imagine that Alice has lost her wallet and needs cash to take a taxi back home, late on a Saturday night. With a phone and an instant payment service app available, Bob would be able to send Alice or the taxi driver funds immediately, from across the country, and these funds would be available to pay for the taxi ride right away.

The connection between an interbank payment system and an instant retail payment system (the FedNow Service) may not be immediately obvious. So, let's break down what happens in the example above.

For Bob to send Alice cash with an interbank payment system, Bob needs to instruct his bank to debit his account, Bob's bank needs to send cash to Alice's bank, and Alice's bank must credit her account. If Alice and Bob don't have the same bank, any fund transfer between them requires an interbank transfer.

In principle, Alice's bank could agree to extend an advance to Bob's bank. This would allow the transfer between Bob and Alice to occur even if the transfer between their banks is delayed. However, doing so creates an interbank exposure that would need to be settled later.

If instant payment usage grows enough, such interbank exposures could become large, and managing the risk they create could be complex and costly. This risk is eliminated if Bob's bank can settle its obligation to Alice's bank in real time, when Alice's bank credits her account.
Since individuals may have the need to send each other funds at any time, including late on weekend nights, as in our example, eliminating the risk that could arise from the resulting interbank exposures requires banks to

have the ability to clear and settle transactions, and also make funds available—all within seconds, at any time. FedNow will do that.

Where Does Fedwire Stand?

Couldn't Fedwire Funds Service's hours of operations have been extended to allow it to support instant retail payments?

There are several reasons why this would not have been practical; let us focus on one.

Systems that operate 24 hours a day, seven days a week, 365 days a year need to be updated from time to time, without service interruption.

The technology that supports Fedwire is not designed to do that effectively. Fedwire's technology updates typically happen on weekends, when the service is not operating.

FedNow, by contrast, is built to make the service upgradable without needing to shut it down.

FedNow will not replace Fedwire. FedNow is meant to support instant retail payments with a maximum value of $500,000; in most cases, financial institutions needing to make large, dollar-denominated RTGS transfers will continue to use the Fedwire Funds Service.

To Sum Up

FedNow is a new interbank RTGS payment system that will support instant clearing and settling of retail transactions.

Individuals will not have access to FedNow directly, but instead will have access to the instant payment services offered by their financial institutions.

FedNow will allow participating institutions to transfer funds between their customers and provide immediate availability without incurring credit exposures.

Because of their speed and convenience, instant payments, whether between individuals or between a business and a customer, are expected to grow in the United States, as they have grown abroad.
With FedNow, the Federal Reserve is supporting the growth of this segment of the payment industry.

To read more: https://tellerwindow.newyorkfed.org/2023/06/26/fednow-is-coming-in-july-what-is-it-and-what-does-it-do/

Modernising payment services and opening financial services data: new opportunities for consumers and businesses

The European Commission has put forward proposals to bring payments and the wider financial sector into the digital age.

Today's new rules will further improve consumer protection and competition in electronic payments, and will empower consumers to share their data in a secure way so that they can get a wider range of better and cheaper financial products and services.

These proposals place consumers' interests, competition, security and trust at their centre.

The payment services market has changed significantly in recent years. Electronic payments in the EU have been constantly growing, reaching €240 trillion in value in 2021 (compared with €184.2 trillion in 2017).

This trend was accelerated by the COVID-19 pandemic. New providers, enabled by digital technologies, have entered the market, in particular providing 'open banking' services – i.e. securely sharing financial data between banks and financial technology firms ('fintechs').

More sophisticated types of fraud have also emerged, putting consumers at risk and affecting trust.

In response to these developments, today's package seeks to ensure the EU's financial sector is fit for purpose and capable of adapting to the ongoing digital transformation, and the risks and opportunities it presents – in particular for consumers.

Today's proposal fulfils a key commitment in the Commission's 2020 Retail Payments Strategy, by ensuring the rules applicable to the EU retail payments industry remain fit for purpose, taking in account market developments, as well as promoting the development of instant payments in the EU.

For the Retail Payments Strategy, you may visit: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:592:FIN

EUROPEAN COMMISSION

Brussels, 24.9.2020
COM(2020) 592 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

on a Retail Payments Strategy for the EU

On that front, it complements the Commission's proposal from 2022 for a Regulation to make instant payments in euro available to all citizens and businesses holding a bank account in the EU and in EEA countries.

EUROPEAN
COMMISSION

Brussels, 26.10.2022
COM(2022) 546 final

2022/0341 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro

In parallel, the Financial Data Access proposal contributes to the commitment set out in the 2020 Digital Finance Strategy to put in place a European financial data space.

Overall, this financial sector initiative fits into the broader European data strategy and builds upon the key principles for data access and processing set out in its accompanying initiatives, such as the Data Governance Act, the Digital Markets Act and the Data Act proposal.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

Why Europe needs a digital euro

Contribution by Fabio Panetta and Valdis Dombrovskis

Fabio Panetta
Member of the ECB's Executive Board

Valdis Dombrovskis
Executive Vice-President of the European Commission

Our world is changing. Digitalisation has transformed society in ways that would have been difficult to imagine only ten years ago. It is also changing how we make payments: people increasingly want to pay digitally. The COVID-19 pandemic has accelerated this shift.

Central banks around the world are now working on complementing the public money they currently make available – cash – with a digital version of it: a central bank digital currency. In the euro area, the digital euro would offer a digital payment solution that is available to everyone, everywhere, for free.

Cash remains important: it is still the preferred means of making small in-store payments and person-to-person transactions. Most people in the euro area want to keep the option to pay with banknotes and coins.

This is why the European Commission and the European Central Bank (ECB) are fully committed to making sure that cash remains fully accepted and available across all 20 countries in the euro area.

But the fact is, using cash for payments is declining in many parts of the world, including Europe. As we move towards a true digital economy, adapting cash to reflect the digital age is the logical next step.

Having both options – a cash euro and a digital euro – would mean that everyone can choose how to pay and no one is left behind in the digitalisation of payments.

Crucially, it would offer Europeans the option to pay digitally throughout the euro area, from Dublin to Nicosia and from Lisbon to Helsinki.

For consumers, the digital euro would bring many practical advantages. It would be simple to use and cost-free.

No matter where they were in the euro area, people could pay anyone for free with their digital euro, for instance using a digital wallet on their phones. They would not even have to make payments online: they could also pay offline.

Protecting privacy is a vital feature of the digital euro. The ECB would not see users' personal details or their payment patterns. The offline

functionality would also bring a higher degree of data privacy than any other digital payment methods currently available.

A digital euro would also reduce payment-related fees for consumers by spurring competition in Europe. At present, two-thirds of Europe's digital retail payments are processed by a handful of global companies. Thanks to greater competition, customers and merchants would benefit from cheaper services.

For banks and other payment service providers, the digital euro would act as a springboard for the development of new pan-European payment and financial services, stimulating innovation and making it easier to compete with large, non-European financial and technology firms.

It would include safeguards, such as limits on the amount that people could hold, to avoid any substantial outflow of deposits from banks. But users wishing to pay more than the set limit would be able to do so by linking their digital wallet to their bank account.

There are also major strategic advantages to having a digital euro. As the world's largest single market, Europe cannot afford to remain passive while other jurisdictions move ahead.

If other central bank digital currencies were allowed to be used more widely for cross-border payments, we would risk diminishing the attractiveness of the euro – currently the world's second most-important currency after the US dollar.

And the euro could become more exposed to competition from alternatives such as global stablecoins. Ultimately, this could endanger our monetary sovereignty and the stability of the European financial sector.

A digital euro would also enhance the integrity and safety of the European payment system at a time when growing geopolitical tensions make us more vulnerable to attacks to our critical infrastructure.

By relying on European infrastructure, the system would be better equipped to withstand disruptions, including cyberattacks and power outages.

We are still only at the start of this exciting new project. The European Commission presents its legal proposal today. This autumn, the ECB will complete its investigation phase on the digital euro's design and distribution. It will then decide whether to initiate a preparation phase to look at developing and testing the new digital currency.

Central bank money underpins our trust in all forms of money as well as the stability and resilience of our payment system. It is the anchor for Europe's financial system and monetary union.

A digital euro would preserve the role of central bank money, because whatever form it takes – cash or digital – a euro will remain a euro.

Our monetary system, with our common currency at its core, needs to keep up with digital advances. We are committed to ensuring that it does.

To read more:
https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230628~140c43d2f3.en.html

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Solvency II Association

At every stage of your career, our association provides networking, training, certification, information, updates, alerts, and services you can use. Join us. Stay current. Take advantage of the new opportunities. Read our monthly newsletter. Get certified.

You can explore what we offer to our members:

1. Membership – Become a standard, premium or lifetime member. You may visit: https://www.solvency-ii-association.com/How_to_become_member.htm

2. Monthly Updates – Visit the Reading Room of the association at: https://www.solvency-ii-association.com/Reading_Room.htm

3. Training and Certification – You may visit: https://www.solvency-ii-association.com/CSiiP_Distance_Learning_Online_Certification_Program.htm

For instructor-led training, you may contact us. We tailor Solvency II presentations, awareness and training programs for supervisors, boards of directors, employees, service providers and consultants.