International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.iambd.org

News for the Board of Directors, October 2023

Dear members and friends,

We will start with a proposal that updates a nearly 20-year-old rule, that allows the PCAOB to hold associated persons accountable when they negligently, directly, and substantially contribute to firms' violations.

The Public Company Accounting Oversight Board (PCAOB) issued for public comment a proposal to amend PCAOB Rule 3502, Responsibility Not to Knowingly or Recklessly Contribute to Violations.

The rule, originally enacted in 2005, governs the liability of associated persons who contribute to registered public accounting firms' violations of the laws, rules, and standards that the PCAOB enforces.

The deadline for public comment on the proposal is November 3, 2023.

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

1666 K Street NW
Washington, DC 20006

Office: 202-207-9100
Fax: 202-862-8430

www.pcaobus.org

PROPOSED AMENDMENTS TO PCAOB RULE 3502 GOVERNING CONTRIBUTORY LIABILITY

PCAOB Release No. 2023-007
September 19, 2023

PCAOB Rulemaking
Docket Matter No. 053

The proposal: https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/053/pcaob-release-no.-2023-007-rule-3502-proposal.pdf?sfvrsn=7d49cc51_9

Through the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley" or the "Act"), Congress established the Board in the wake of a series of high-profile corporate collapses that laid bare auditor misconduct and the need for a new type of oversight of the public accounting industry.[1] As part of its comprehensive, multipronged approach to such oversight, Congress authorized the Board to investigate, bring charges against, and sanction (when appropriate) registered public accounting firms and associated persons[2] thereof for violations of the laws, rules, and standards that Congress charged the Board with enforcing.[3] That enforcement authority covers a wide array of auditor conduct, including negligent conduct.

"This proposal is simply updating PCAOB rules to match what investors already expect: that auditors act with reasonable care whenever they are performing their duties – and when an auditor's negligence results in firm violations that can put investors at risk, the PCAOB has tools to hold them accountable," said PCAOB Chair Erica Y. Williams.

Rule 3502's purpose is to enable the Board to hold accountable associated persons of PCAOB-registered firms who directly and substantially contribute to violations committed by registered firms.

Today's proposal better protects investors with two key updates:

1. It strengthens accountability for those who put investors at risk by updating the threshold for liability:

Auditors are already required to exercise reasonable care anytime they perform an audit – and failure to do so constitutes "negligence."

The current Rule 3502, however, only allows auditors to be held liable for firms' violations when they "recklessly" contribute to those violations – which represents a greater departure from the standard of care than negligence.

This means even when a firm commits a violation negligently, an associated person who directly and substantially contributed to the firm's violation can be sanctioned only if the PCAOB shows that the associated person acted recklessly.

The proposal, if adopted, would update Rule 3502's liability standard from recklessness to negligence, aligning it with the same standard of reasonable care auditors are already required to exercise anytime they are executing their professional duties.

Similarly, the U.S. Securities and Exchange Commission already has the ability to bring enforcement actions against associated persons when they negligently cause firm violations. The proposal maintains the requirement under the current version of Rule 3502 that an associated person must have contributed to the firm's violation both "directly and substantially" in order to be held liable.

2. It clarifies the relationship between the contributory actor and the primary violator:

To be held liable under the current Rule 3502, an associated person who contributes to a firm's violation must be an associated person of that particular firm. Given the increasing complexity of arrangements among firms and the constantly evolving nature of technology, the proposal clarifies that associated persons of any firm can be held liable as long as their conduct at least negligently, and directly and substantially, contributes to any firm's violation, not just violations by a firm with which they are associated.

Throughout the proposal, the Board requests comments on specific aspects of the proposed amendments. Readers are encouraged to answer the Board's questions, to comment on any aspect of the proposal, and to provide reasoning and relevant data supporting their views.

The public can learn more about submitting comments on PCAOB proposals at the Open for Public Comment page. Learn more about the PCAOB's rulemaking agenda on the PCAOB website.

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-issues-proposal-to-strengthen-accountability-for-contributing-to-firm-violations

SEC Approves Revised Privacy Act Rule

The Securities and Exchange Commission approved a rule to revise the Commission's regulations under the Privacy Act, which is the principal law governing the handling of personal information in the federal government.

The rule: https://www.sec.gov/files/rules/final/2023/34-98437.pdf

AGENCY: Securities and Exchange Commission.

ACTION: Final rule.

SUMMARY: The Securities and Exchange Commission ("Commission" or "SEC") is adopting amendments to the Commission's regulations under the Privacy Act of 1974, as amended ("Privacy Act"). The amendments revise the Commission's regulations under the Privacy Act to clarify, update, and streamline the language of several procedural provisions.

The final rule clarifies, updates, and streamlines the Commission's Privacy Act regulations. In addition, the final rule revises procedural and fee provisions and eliminates unnecessary provisions. The final rule also allows for electronic methods to verify one's identity and submit Privacy Act requests.

"I was pleased to support this adoption because it will update the Commission's rules with respect to this important law," said SEC Chair Gary Gensler. "These amendments will provide more clarity on how the public can access their records maintained by the Commission and request amendments."

The Commission last updated its Privacy Act rules in 2011. The revisions approved today will codify current practices for processing requests made by the public under the Privacy Act. This provides greater clarity regarding the Commission's process for how individuals can access information pertaining to themselves.

Due to the scope of the revisions, the final rule replaces the Commission's current Privacy Act regulations in their entirety. The final rule is published on SEC.gov and will be published in the Federal Register. The final rule becomes effective 30 days after publication in the Federal Register.

To read more: https://www.sec.gov/news/press-release/2023-189

Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation

RICHARD BLUMENTHAL
U.S. SENATOR FOR CONNECTICUT

U.S. Senators Richard Blumenthal (D-CT) and Josh Hawley (R-MO), Chair and Ranking Member of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, announced a bipartisan legislative framework to establish guardrails for artificial intelligence.

The framework lays out specific principles for upcoming legislative efforts, including the establishment of an independent oversight body, ensuring legal accountability for harms, defending national security, promoting transparency, and protecting consumers and kids.

The announcement follows multiple hearings in the Subcommittee featuring witness testimony from industry and academic leaders, including OpenAI CEO Sam Altman, Anthropic CEO Dario Amodei, and Microsoft President and Vice Chair Brad Smith who will testify before the Subcommittee on Tuesday.

“This bipartisan framework is a milestone—the first tough, comprehensive legislative blueprint for real, enforceable AI protections. It should put us on a path to addressing the promise and peril AI portends,” said Blumenthal.

“We’ll continue hearings with industry leaders and experts, as well as other conversations and fact finding to build a coalition of support for legislation. License requirements, clear AI identification, accountability, transparency, and strong protections for consumers and kids—such common sense principles are a solid starting point.”

“Congress must act on AI regulation, and these principles should form the backbone,” said Hawley. “Our American families, workers, and national security are on the line. We know what needs to be done—the only question is whether Congress has the willingness to see it through.”

Specifically, the framework would:

Establish a Licensing Regime Administered by an Independent Oversight Body. Companies developing sophisticated general purpose AI models (e.g.,GPT-4) or models used in high risk situations (e.g., facial recognition) should be required to register with an independent oversight body, which would have the authority to audit companies seeking licenses and cooperating with other enforcers such as state Attorneys General. The entity should also monitor and report on technological developments and economic impacts of AI.

Ensure Legal Accountability for Harms. Congress should require AI companies to be held liable through entity enforcement and private rights of action when their models and systems breach privacy, violate civil rights, or cause other harms such as non-consensual explicit deepfake imagery of real people, production of child sexual abuse material from generative AI, and election interference. Congress should clarify that Section 230 does not apply to AI and ensure enforcers and victims can take companies and perpetrators to court.

Defend National Security and International Competition. Congress should utilize export controls, sanctions, and other legal restrictions to limit the transfer of advanced AI models, hardware, and other equipment to China Russia, other adversary nations, and countries engaged in gross human rights violations.

Promote Transparency. Congress should promote responsibility, due diligence, and consumer redress by requiring transparency from companies. Developers should be required to disclose essential information about training data, limitations, accuracy, and safety of AI models to users and other companies. Users should also have a right to an affirmative notice when they are interacting with an AI model or system, and the new agency should establish a public database to report when significant adverse incidents occur or failures cause harms.

Protect Consumers and Kids. Consumers should have control over how their personal data is used in AI systems and strict limits should be imposed on generating AI involving kids. Companies deploying AI in high-risk or consequential situations should be required to implement safety brakes and give notice when AI is being used to make adverse decisions.

A copy of the bipartisan framework can be found at:
https://www.blumenthal.senate.gov/imo/media/doc/09072023bipartisanaiframework.pdf

To read more:
https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation

Basel III Monitoring Report, September 2023

BIS

Highlights of the Basel III monitoring exercise as of 31 December 2022

After their downturn at end-June 2022, initial Basel III capital ratios increase and rise above pre-pandemic levels.

Liquidity Coverage Ratio declines but remains above pre-pandemic levels

To assess the impact of the Basel III framework on banks, the Basel Committee on Banking Supervision monitors the effects and dynamics of the reforms.

For this purpose, a semiannual monitoring framework has been set up on the risk-based capital ratio, the leverage ratio and the liquidity metrics using data collected by national supervisors on a representative sample of institutions in each country.

Since the end2017 reporting date, the report also captures the effects of the Committee's finalisation of the Basel III reforms.

This report summarises the aggregate results using data as of 31 December 2022. The Committee believes that the information contained in the report will provide relevant stakeholders with a useful benchmark for analysis.

Information considered for this report was obtained by voluntary and confidential data submissions from individual banks and their national supervisors.

At the jurisdictional level, there may be mandatory data collections ongoing, which also feed into this report.

Data were included for 178 banks, including 111 large internationally active ("Group 1") banks, among them 29 G-SIBs, and 67 other ("Group 2") banks.

Members' coverage of their banking sector is very high for Group 1 banks, reaching 100% coverage for some countries, while coverage is lower for Group 2 banks and varies by country.

In general, this report does not consider any transitional arrangements such as grandfathering arrangements. Rather, the estimates presented generally assume full implementation of the Basel III requirements based on data as of 31 December 2022.

No assumptions have been made about banks' profitability or behavioural responses, such as changes in bank capital or balance sheet composition, either since this date or in the future.

Furthermore, the report does not reflect any additional capital requirements under Pillar 2 of the Basel III framework or any higher loss absorbency requirements for domestic systemically important banks, nor does it reflect any countercyclical capital buffer requirements.

Overview of results (unbalanced data set) Table 1

	30 June 2022[1]			31 December 2022		
	Group 1	Of which: G-SIBs	Group 2	Group 1	Of which: G-SIBs	Group 2
Initial Basel III framework						
CET1 ratio (%)	12.7	12.6	16.8	13.1	13.1	16.8
Target total capital shortfalls (€ bn)[2]	0.0	0.0	0.0	0.0	0.0	0.0
TLAC shortfall 2022 minimum (€ bn)	35.1	35.1		34.4	34.4	
Total accounting assets (€ bn)	81,839.4	59,481.9	2,417.9	80,915.3	55,405.3	4,193.2
Leverage ratio (%)[3]	5.8	5.7	5.8	6.1	5.9	6.3
LCR (%)	138.2	137.5	220.0	132.0	134.2	188.4
NSFR (%)	123.5	125.2	132.3	124.4	126.7	132.2
Fully phased-in final Basel III framework (2028)						
Change in Tier 1 MRC at the target level (%)	2.8	3.2	-2.0	3.0	2.9	6.6
CET1 ratio (%)	12.5	12.5	14.3	12.7	12.8	14.7
Target capital shortfalls (€ bn); of which:	7.8	7.8	0.0	3.2	3.2	1.1
CET1	3.5	3.5	0.0	0.0	0.0	0.1
Additional Tier 1	1.9	1.9	0.0	0.0	0.0	0.4
Tier 2	2.4	2.4	0.0	3.2	3.2	0.6
TLAC shortfall 2022 minimum (€ bn)	29.8	29.8		37.4	37.4	
Leverage ratio (%)[3]	6.0	5.9	5.8	6.1	6.0	6.3

See Table A.4 for the target level capital requirements. [1] The values for the previous period may differ slightly from those published in the end-December 2021 report at the time of its release. This is caused by data resubmissions for previous periods to improve the underlying data quality and enlarge the time series sample. [2] Uses the 2017 definition of the leverage ratio exposure measure. [3] The leverage ratios reflect temporary exclusions from leverage exposures introduced in some jurisdictions.

To read more: https://www.bis.org/bcbs/publ/d554.pdf

PCAOB Adopts New Standard, Modernizing Requirements for Auditors' Use of Confirmation to Better Protect Investors in Today's World

New standard replaces outdated interim standard, enhances procedures including strengthening an auditor's approach to identify fraud

The Public Company Accounting Oversight Board (PCAOB) adopted a new standard to strengthen and modernize the requirements for the auditor's use of confirmation – *the process that involves verifying information about one or more financial statement assertions with a third party*.

The new standard reflects changes in technology, communications, and business practices since the interim standard was first adopted by the PCAOB in 2003 after being issued by the AICPA in 1991.

The updated standard will better protect investors by strengthening procedures that enhance an auditor's ability to identify fraud in certain circumstances and improving overall audit quality.

"The new standard will help auditors detect fraud and better protect investors. By replacing a confirmation standard that had not changed significantly since faxes were a regular form of communication, the Board has taken an important step in modernizing our standards to effectively protect investors in today's world," said PCAOB Chair Erica Y. Williams.

"The Board thanks the many commenters whose thoughtful input helped to shape this new standard on the auditor's use of confirmation, and we look forward to monitoring the new standard's implementation and impact."

Key Provisions of the New Standard

Touching nearly every audit, the confirmation process involves an auditor selecting one or more items to be confirmed, sending a confirmation request directly to a confirming party (e.g., a financial institution), evaluating the information received, and addressing nonresponses and incomplete responses to obtain audit evidence about one or more financial statement assertions.

The new standard establishes principles-based requirements designed to stay relevant as technology evolves by applying to all methods of confirmation, including electronic and paper-based communications. In

addition, the new standard better integrates with the PCAOB's risk assessment standards. Among its key provisions, the new standard:

- Includes a new requirement regarding confirming cash and cash equivalents held by third parties or otherwise obtaining relevant and reliable audit evidence by directly accessing information maintained by a knowledgeable external source;

- Carries forward the existing requirement regarding confirming accounts receivable, while addressing situations where it is not feasible for the auditor to perform confirmation procedures or otherwise obtain relevant and reliable audit evidence for accounts receivable by directly accessing information maintained by a knowledgeable external source;

- States that the use of negative confirmation requests alone does not provide sufficient appropriate audit evidence;

- Emphasizes the auditor's responsibility to maintain control over the confirmation process and provides that the auditor is responsible for selecting the items to be confirmed, sending confirmation requests, and receiving confirmation responses; and

- Identifies situations in which alternative procedures should be performed by the auditor.

The adoption of the new confirmation standard was informed by input from an extensive notice-and-comment process, including issuance of a concept release and two proposing releases.

Information on the history of this project, including historical documents and comments received, can be found in Rulemaking Docket 028 and the related Standard-Setting Project page at:

https://pcaobus.org/oversight/standards/standard-setting-research-projects/confirmations

The new standard will apply to all audits conducted under PCAOB standards.

Subject to approval by the Securities and Exchange Commission, the new standard will take effect for audits of financial statements for fiscal years ending on or after **June 15, 2025.**

To read more: https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/docket_028/2023-008_confirmation-adopting-release.pdf?sfvrsn=e18cef74_2

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

The Auditor's Use of Confirmation, and Other Amendments to PCAOB Standards

PCAOB Release No. 2023-008
September 28, 2023

PCAOB Rulemaking
Docket Matter No. 028

Project Mariana: BIS and central banks of France, Singapore and Switzerland successfully test cross-border wholesale CBDCs

BIS Innovation Hub

Foreign exchange (FX) is the largest financial market in the world, trading about $7.5 trillion a day (BIS (2022b)).

It operates 24 hours a day, five and a half days a week.

Project Mariana looks to the future and envisions a world in which central banks have issued central bank digital currencies (CBDCs) and explores how foreign exchange (FX) trading and settlement might look.

Mariana borrows ideas and concepts from decentralised finance (DeFi) and studies whether so-called automated market-makers (AMMs) can simplify FX trading and settlement with a view to enhancing market efficiency and reducing settlement risk.

Project Mariana is a proof of concept (PoC) for a global interbank market for spot FX featuring both an AMM and wholesale CBDCs (wCBDCs).

In the PoC, wCBDCs circulate on domestic platforms and so-called bridges allow them to be moved on to a transnational network that hosts the AMM.

Project Mariana extends previous experimentation on cross-border settlement using wCBDC arrangements and distributed ledger technology.

It successfully demonstrates the technical feasibility of the proposed architecture and adds novel insights on the potential of tokenisation in three dimensions.

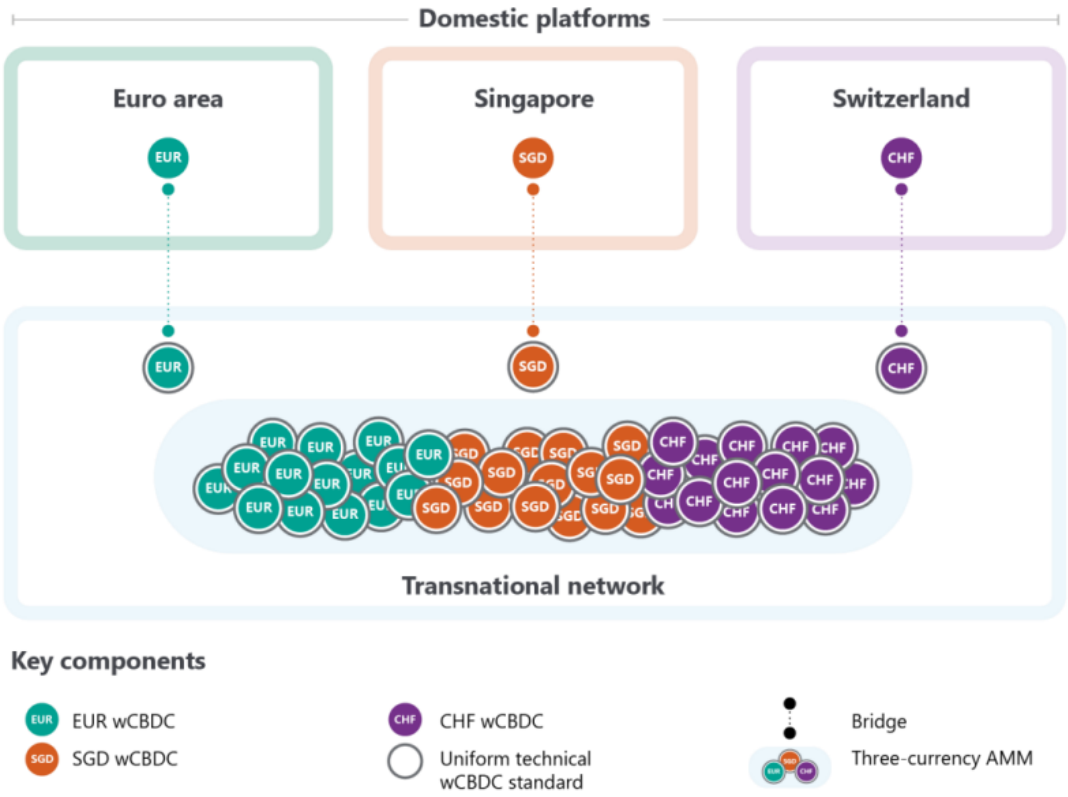
First, wCBDCs are implemented as smart contracts, enabling central banks to manage their wCBDC without the need to directly operate or control the underlying platform.

Their design followed best practices from the public blockchain space, building on a widely used standard (ie ERC-20), as well as enabling upgradeability.

Second, bridges may serve as a mechanism to enable broader interoperability in an emerging tokenised ecosystem.

As implemented in the PoC, they may enable the seamless and safe transfer of wCBDC between domestic platforms and the transnational network without manual intervention.

Mariana high-level architecture Graph 1



The bridge design features controls and safeguards and ensures resilience through on-chain (ie bridge smart contracts) and off-chain (ie communication between bridge smart contracts) infrastructure managed by central banks.

Third, the AMM, as tested and calibrated in Mariana, fulfilled requirements based on selected FX Global Code (FXGC) principles. It delivers the contours of a possible future tokenised FX market that has a number of potential benefits.

These include supporting simple and automated execution of FX transactions, providing options to broaden the range of currencies, eliminating settlement risk and enabling transparency.

However, the use of AMMs requires the pre-funding of liquidity and their adoption would therefore entail a significant departure from the ex post funding (deferred net settlement) in use in today's FX markets.

To learn more: https://www.bis.org/publ/othp75.pdf

Project Mariana

Cross-border exchange of wholesale CBDCs using automated market-makers

Final report

September 2023

Project Atlas, Mapping the world of decentralised finance

October 2023

Project Atlas creates a data platform that sheds light on the macroeconomic relevance of cryptoasset markets and decentralised finance (DeFi).

Together with the project partners within the Eurosystem – the Deutsche Bundesbank and De Nederlandsche Bank – a first proof of concept of Project Atlas was developed focusing on international flows of cryptoassets.

Cryptoassets and DeFi applications are part of an emerging financial ecosystem that spans the globe.

While introducing new technologies, these markets often lack transparency and potentially present risks to financial stability.

The collapse of some stablecoins and DeFi platforms has highlighted the difficulty of making such risk assessments today.

Although blockchain transactions are theoretically transparent, reliable information on macro-financial implications is hard to obtain.

Project Atlas provides data tailored to the needs of central banks and financial regulators.

It fuses data gathered from crypto exchanges (off-chain data) with data from public blockchains (on-chain data) gathered from nodes.

By connecting various sources, Atlas allows for data vetting, giving users tools to evaluate these markets' economic significance more accurately.

As part of a first proof of concept, Project Atlas derives cryptoasset flows across geographical locations.

The approach uses transactions attributed to crypto exchanges in the Bitcoin network, along with the location of those exchanges, as a proxy for cross-border capital flows.

The country location is not always discernible for crypto exchanges, and attribution data are naturally incomplete and possibly not perfectly accurate.

Therefore, the flows should be regarded as a lower-bound estimate of the actual size.

The initial findings indicate that, although relatively small compared with total onchain network traffic, identified flows between crypto exchanges are significant and substantial economically.

Attributing geographical areas to exchanges (where possible) lays out the structure of cross-border flows. Thus, Project Atlas provides a starting point for structural analysis across jurisdictions.

More broadly, there is a need for central banks and financial regulators to gain firsthand knowledge of cryptoasset and DeFi markets, and there is a dearth of reliable and tailored data for such purposes.

Policymakers must understand the underlying data that feed into aggregate indicators to make well informed decisions. Available aggregate statistics provided by market actors or data providers often leave open how data are generated and what the underlying assumptions are.

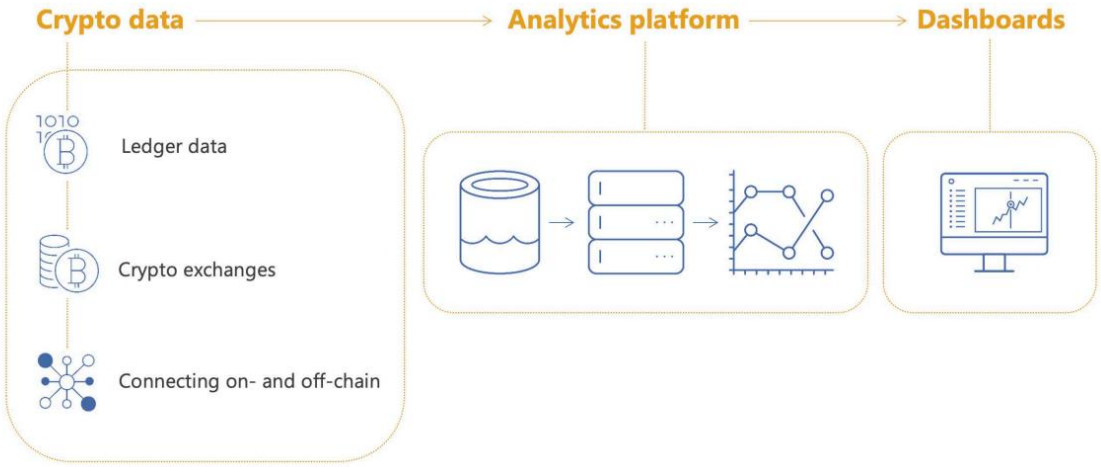
Access to granular data supports assessment of data reliability and enables solid analysis.

Because Project Atlas relies on in-house development of the platform and broader infrastructure, the knowledge and developed code can be openly shared with the central banking community.

At the same time, Atlas enhances technical and analytical capabilities.

Atlas can evolve into an insightful public good as the data platform and outputs will be openly available to central banks.

To read more: https://www.bis.org/publ/othp76.pdf



Source: Project Atlas.

2023 FSB Annual Report

FSB FINANCIAL STABILITY BOARD

Executive summary

The banking turmoil in March 2023 highlighted issues for financial stability.

1. Swift and decisive actions by the US and Swiss authorities were taken to deal with the failures of US regional banks and of Credit Suisse respectively earlier this year.

2. The already implemented Basel III reforms helped shield the global banking sector and real economy from a more severe banking crisis. The events underscored the importance of completing the implementation of the outstanding Basel III standards.

3. A striking feature of the bank failures was the unprecedented speed and scale of deposit runs. The FSB is assessing vulnerabilities from asset-liability and liquidity mismatches and exploring whether technology and social media have changed deposit stickiness.

4. Banks' risk management and governance arrangements remain the first and most important source of resilience.

   The Basel Committee on Banking Supervision (BCBS) is prioritising work to strengthen supervisory effectiveness and is pursuing follow-up work to assess the performance of specific features of the Basel Framework, such as liquidity risk and interest rate risk in the banking book.

5. The FSB's review of the lessons to be learnt for the operation of the international resolution framework concludes that recent events demonstrate the soundness of the framework.

   While the review identifies several areas for further analysis and improvements in the operationalisation and implementation of the framework, the review upholds the appropriateness and feasibility of the framework, rather than presenting issues that would question the substance of the Key Attributes themselves.

Vulnerabilities in the global financial system continue to be elevated…

1. The effects of the post-pandemic rise in interest rates are increasingly being felt. The cost of financing has risen substantially, at a time when debt is at very high levels across the government, corporate and household sectors. This is likely to lead to credit quality challenges that may affect both banks and non-bank investors.

2. High interest rates and an uncertain growth outlook also create the potential for higher volatility in asset prices. This could generate significant spikes in collateral and margin calls, inducing fire sales of assets. Liquidity mismatches in non-bank financial entities could also amplify shocks if they lead to simultaneous asset sales across markets.

… while vulnerabilities from structural change continue to emerge.

1. Exposure to climate-related vulnerabilities is becoming more evident. A manifestation of physical risks, as well as a disorderly transition to a low carbon economy, could have destabilising effects from increases in risk premia and falling asset prices.

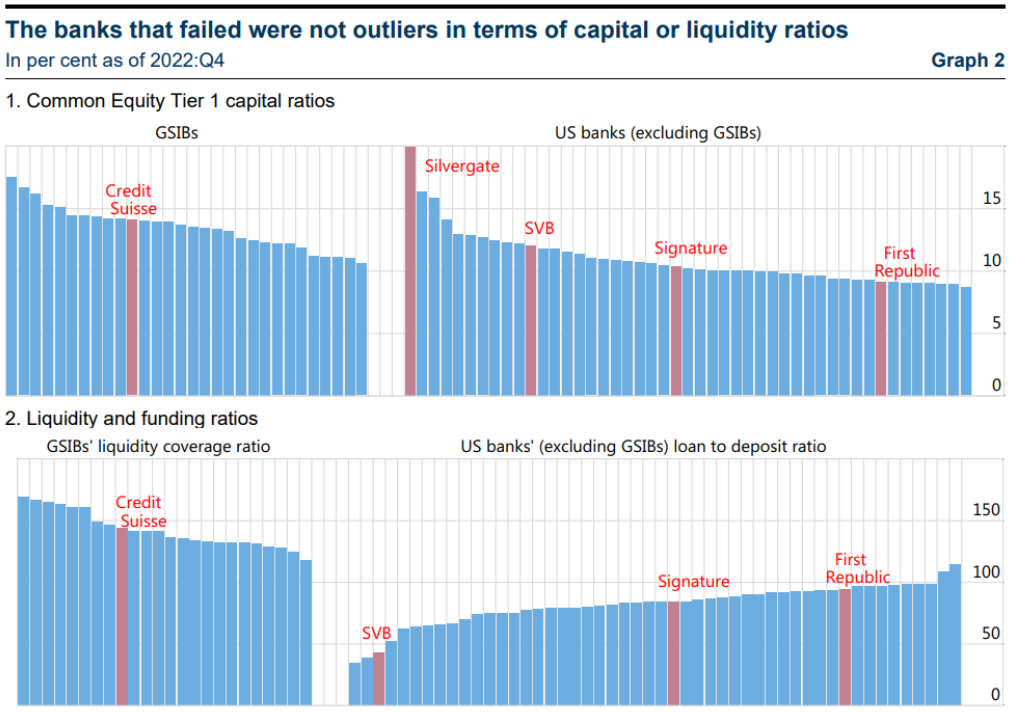
2. Cyber incidents continue to grow in frequency and sophistication. A successful cyberattack on parts of the financial system, including third-party service providers, could interrupt the supply of financial services and damage confidence.

3. Crypto-asset markets are rapidly evolving and, while financial stability risks appear contained at present, recent incidents underscore the need for vigilance and oversight.

   If these markets were to grow and become more interconnected with the traditional financial system, they could reach a point where they represent a threat to global financial stability.

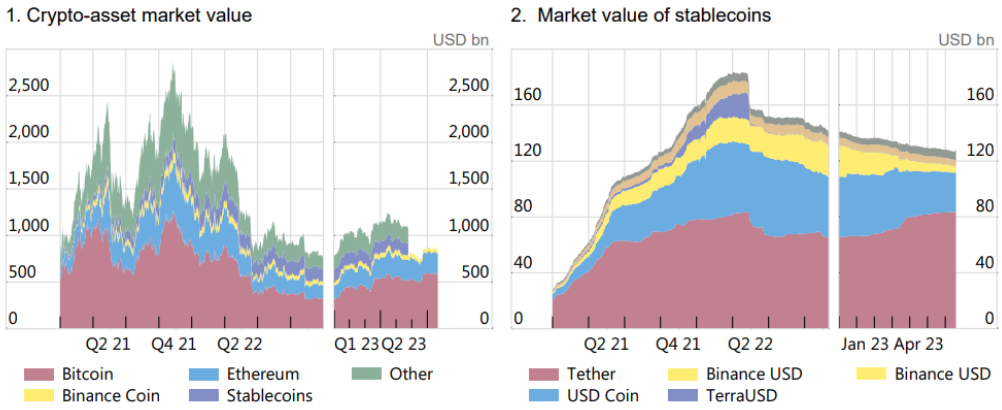
The banks that failed were not outliers in terms of capital or liquidity ratios

In per cent as of 2022:Q4 — **Graph 2**



Sources: S&P Capital IQ; FSB calculations.

Crypto-asset market capitalisation remains well below its peak — **Graph 5**



Sources: CoinGecko; CCData; FSB calculations.

To read more: https://www.fsb.org/wp-content/uploads/P111023.pdf

FSB FINANCIAL STABILITY BOARD

Promoting Global Financial Stability

2023 FSB Annual Report

Crypto-assets regulation: from patchwork to framework

DeNederlandscheBank
EUROSYSTEEM

Hello everyone – offline, and also, hello everyone online.

It is a pleasure to be back in London. Back at the Bank of England. Back at the 'Old Lady of Threadneedle Street'. The Old Lady that battles inflation, safeguards financial stability and firmly protects… the gold in her vaults. Gold that lies right here, under our feet. 400 000 bars of gold, to be precise.

Now, I am not here to take a peek at that small fraction of gold that is ours. No, today, I was invited to talk about a new type of gold – or, at least, to some it is. I am referring to crypto-assets. Something the Financial Stability Board has consistently been monitoring since 2018.

For a long time, crypto-assets were an experiment on the fringes of the financial system. No shop owner would accept bits and bytes instead of cash or card.

But soon, certain illicit online marketplaces got wind of this new digital asset: selling illegal services or products online had never been this easy. So, regulators and law enforcement agencies sprang into action and took coordinated action to combat money laundering.

Nonetheless, in those early days, chances were very slim that someone had heard of bitcoin or ether, let alone owned them.

And then suddenly – seemingly overnight – crypto-assets became the talk of the town, and everybody seemed to wonder: is this the new gold?

As a result, the total market capitalization of crypto-assets exploded. At the same time, ties with traditional financial parties grew. As did the interest in the underlying technologies.

When the 'crypto winter' hit us last year, it became crystal clear however, that not all that glitters is gold. A sudden change in investor sentiment caused a sharp decrease in crypto-asset prices. That, in turn, led to the spectacular failure of several crypto-intermediaries.

Total crypto-asset market capitalization was never really able to recover after that.

But even as crypto-asset prices are in a rut presently, crypto-asset market structures continue to develop at a rapid pace. And at the same time, we see a growing involvement of traditional finance with the crypto-ecosystem – which means that the financial interlinkages between these two worlds are growing as well.

So we cannot exclude that, sooner rather than later, vulnerabilities in crypto-asset markets become big enough to form an actual, transmissible risk to global financial stability. And this risk looms larger if we don't implement comprehensive regulation.

All over the world, national regulators have not been waiting on me to say this. A lot of decisive action has been taken already.

The FSB welcomes these initiatives because they show much-needed willingness to act.

But at the same time, we see a challenge due to crypto's inherent global reach. And that is: how do we ensure consistency between all these regulations?

And how do we deal with crypto parties that choose to operate exactly from those jurisdictions that don't really prioritise the effective regulation and supervision of crypto-asset activities?

To overcome these challenges, the FSB developed a Global Regulatory Framework. This framework, published last July, aims to promote the consistency of regulatory and supervisory practices to address the financial stability risks of crypto-asset activities.

Developing this framework on the basis of consensus among the FSB member authorities has required a careful threading of the needle. And so, I think it is fitting that we find ourselves on Threadneedle Street, today. The perfect place to discuss the FSB's finalized policy work on broader crypto-asset markets and global stablecoin arrangements.

The latter is a specific type of crypto-asset – one that aims to maintain a stable value relative to a pool of assets, usually fiat money. One that carries heightened risks to global financial stability because of its potential systemic relevance in multiple jurisdictions. And so, one that requires special attention.

Because the FSB recommendations are high-level, national authorities can apply these recommendations flexibly, whilst also ensuring a baseline – a baseline that provides for a consistent application of comprehensive regulation across the globe. A baseline that embraces both already existing rules in some countries, and to be drafted regulations in others. A baseline

with a clear thread of gold – and that is the principle of "same activity, same risk, same regulation".

Many crypto-asset activities perform functions and, hence, carry risks, that strongly resemble those of traditional financial activities. Think, for example, of the similarities between staking and deposit-taking, or between crypto-lending and securities financing transactions. And so, we believe they should be regulated as such.

A number of our recommendations have to do with the vulnerabilities of centralized crypto-asset intermediaries. And I stress 'centralized' because, however 'de-centralized' the crypto-asset ecosystem claims to be, economic reality tells a different story. In fact, some of these intermediaries already seem to play a systemic role within the crypto-ecosystem.

That is why we recommend that authorities require a number of things from these entities. For instance to have in place robust governance frameworks and to set up risk management practices.

Of course, I know that implementation takes time. But I also know it's high time – as I have often heard my British colleagues say – to 'crack on'. So, let's prioritise the full and consistent implementation of our high-level recommendations.

Because in the meantime, people investing in crypto-assets continue to run serious risks. In the meantime, linkages between the crypto-ecosystem and traditional finance may very well continue to grow. So, in the meantime, risks to financial stability can still escalate.

There are several ways through which we can prevent crypto-asset volatility from spilling over to the traditional financial system. One important way to do this, is with the full and consistent implementation of the BCBS prudential framework for the treatment of banks' crypto-asset exposures.

Putting this global framework into practice limits the chance that crypto-volatility reaches banks and hence becomes a threat to financial stability.

To keep a close eye on the progress made, the FSB will start monitoring implementation. Our first review should be finalized by the end of 2025.

And the FSB will not only monitor progress. If we are serious about regulating what is essentially a cross-border phenomenon, we also need to be serious about cross-border cooperation. About information sharing. About working together.

This also means that we need to venture outside of the FSB jurisdictions. Because several jurisdictions with material crypto-asset activities are not members of the FSB.

Nevertheless, global financial stability ties all of us together. And to safeguard that stability, the FSB members need to engage with these jurisdictions. We need to ensure the needle of their regulatory compass points in the same direction as ours.

To do so, we want to start with positive incentives like outreach, technical workshops, and capacity building to get them prepared. We'll work closely with the IMF, the World Bank and other international organizations on this.

However, chances are we may still see regulatory competition. And so, we cannot exclude that a toughening of regulation in one part of the world pushes crypto-asset parties to relocate to other parts of the world. Parts of the world with weaker regulatory standards.

What we can do, though, is require that traditional financial institutions take additional measures to manage the risks of interacting with crypto intermediaries operating in such jurisdictions. Measures necessary to protect global financial stability. We are not there yet, but if you ask me, we should be heading in that direction.

Just like crypto-asset threats don't stop at national borders, the thread of crypto-asset risks doesn't only weave through financial stability. There are also macroeconomic risks. Specifically for emerging markets and developing countries.

In EMDEs, crypto-assets are relatively popular. The more popular they are, the more they could erode the effectiveness of domestic monetary policy. Because people may start preferring crypto-assets or stablecoins over domestic currencies.

This risk of currency substitution, or so-called 'crypto-ization', means EMDE's might face even greater risks from crypto-assets than advanced economies. A potentially dangerous cocktail of financial stability and macroeconomic risks.

For this reason, the Indian G20 Presidency asked the FSB and the IMF to combine their work on this subject in a synthesis paper. This was published in September. A key conclusion is that crypto-assets do indeed have implications for macroeconomic and financial stability, but even more, that these implications are mutually interactive and reinforcing.

In our view, this underlines, once more, the need for a global regulatory and supervisory baseline to oversee crypto-asset activities.

A baseline that addresses both financial stability and macroeconomic risks. A baseline that all national regulators can adhere to, but at the same time allows them to take targeted and time-bound measures to address jurisdiction-specific circumstances.

To help EMDEs address these serious risks to financial stability, the FSB will investigate how cross-border cooperation between advanced and developing economies can practically be enhanced.

Dear colleagues, today, I've talked about crypto-assets – a concept that is not even 20 years old. The Bank of England's nickname, the 'Old Lady of Threadneedle Street', dates back more than two hundred years. To 1797.

When crypto-assets were still the distant future. Banknotes could still be converted to gold. And France declared war on Britain, and landed on its shores.

Within hours, people rushed to the Bank of England. Asking for gold. The very gold that lies under our feet. And the famous vaults were rapidly emptying out.

Then-prime minister, William Pitt the Younger, tried to put a halt to that. Not because he wanted to preserve gold for financial stability reasons, but to use it to defend Britain.

In a famous cartoon, probably familiar to many of you, you can see William Pitt the Younger trying to 'woo' an old lady (more information(Refers to an external site)).

But in fact, all he wants, is the gold in her pockets and in the chest she sits on. Of course, she is not inclined to give in. Ever since, the Bank of England has been known as the 'Old Lady of Threadneedle Street'.

Today, the 'Old Ladies' many of us work for, will no longer exchange banknotes for gold. But still people look for stable assets – assets that maintain their value over time and allow them to transact with people from around the globe.

Today, these 'Old Ladies', can still not easily be 'woo-ed'. And remain firmly seated on their chests of gold – or, rather, vaults. And today, once more, these 'Old Ladies' are willing to defend what knits us all together and helps to bring global prosperity – and that's financial stability.

Thank you.

To read more: https://www.dnb.nl/en/general-news/speech-2023/crypto-assets-regulation-from-patchwork-to-framework/

PCAOB 2023 Conference on Auditing and Capital Markets Attracts 359 Participants From Across Academia

The Public Company Accounting Oversight Board (PCAOB) has concluded its two-day 2023 Conference on Auditing and Capital Markets, held in Washington, DC. Open to academics and Ph.D. students, the research conference attracted 359 participants this year.

"Whether it's workers saving for retirement, parents saving to put their kids through college, or anyone who depends on the soundness of our capital markets to invest and build their own version of the American dream, quality audits protect people – and that's why we are here," PCAOB Chair Erica Y. Williams told the conference.

"Our work to protect investors relies on high-quality economic analysis, and we depend on the academic community to expand our knowledge and understanding of the economic impact of auditing and audit regulation on our capital markets."

Established by the PCAOB in 2014, the Conference on Auditing and Capital Markets is designed to foster rigorous economic research on audit-related topics (including the economic impact of auditing and audit regulation on capital markets), inform the academic community about PCAOB activities and developments, and obtain input from the academic community on topics of interest to the PCAOB.

At the 2023 conference, academics presented research during panels focused on the following topics:

- Audit Partner Accountability, Reputation, and Repercussions
- Auditor Expertise and Team Dynamics
- Diversity, Equity, and Inclusion in the Auditing Profession
- Modeling Assisted Decision Making in Auditing and Audit Regulation
- Critical Audit Matters

In addition to these panels and sessions featuring PCAOB speakers, participants heard keynote remarks from Jennifer R. Joe, the John E. Peterson Professor in the Accounting and Information Systems Department of the Pamplin College of Business at Virginia Tech and the President of the Auditing Section of the American Accounting Association; and Karthik Ramanna, Professor of Business and Public Policy at the University of Oxford's Blavatnik School of Government and a fellow at St. John's College.

"We thank all the participants in this year's Conference on Auditing and Capital Markets," said Dr. Martin C. Schmalz, the PCAOB's Chief Economist and the Director of its Office of Economic and Risk Analysis.

"Their insights and perspectives build understanding of opportunities and challenges facing not just the auditing world, but also the broader economy."

Learn more about the PCAOB's work related to economic analysis at: https://pcaobus.org/oversight/standards/economic-analysis

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-2023-conference-on-auditing-and-capital-markets-attracts-359-participants-from-across-academia

The European cyber crisis liaison organisation network (EU-CyCLONe)

The European cyber crisis liaison organisation network (EU-CyCLONe) is a cooperation network for Member States national authorities in charge of cyber crisis management.

The network was launched in 2020 and formalized on 16th of January 2023 with entrance into force of NIS 2 Article 16.

Article 16

European cyber crisis liaison organisation network (EU-CyCLONe)

1. EU-CyCLONe is established to support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies.

2. EU-CyCLONe shall be composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer.

ENISA shall provide the secretariat of EU-CyCLONe and support the secure exchange of information as well as provide necessary tools to support cooperation between Member States ensuring secure exchange of information.

Where appropriate, EU-CyCLONe may invite representatives of relevant stakeholders to participate in its work as observers.

3. EU-CyCLONe shall have the following tasks:

(a) to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;

(b) to develop a shared situational awareness for large-scale cybersecurity incidents and crises;

(c) to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;

(d) to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;

(e) to discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4).

The aim is to collaborate and develop timely information sharing and situational awareness based on tools and support provided by the EU Agency for Cybersecurity, which serves as the CyCLONe Secretariat.

The Chair is a representative of the MS holding the Presidency of the Council of the EU.
EU-CyCLONe is composed of the representatives of Member States' cyber crisis management authorities as well as, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a

significant impact on services and activities falling within the scope of this Directive, the Commission. In other cases, the Commission shall participate in the activities of EU-CyCLONe as an observer.

The main tasks of EU CyCLONe are to:

- Support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies, offices and agencies;

- Increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;

- Develop a shared situational awareness for large-scale cybersecurity incidents and crises;

- Assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;

- Coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;

- Discuss, upon the request of a Member State concerned, national large-scale cybersecurity incident and crisis response plans.

ENISA provides the Secretariat, infrastructures and tools to enable effective cooperation to respond to large scale and cross-border cyber incidents, attacks and crisis.

ENISA also supports the organisation of exercises for CyCLONe members, such as CySOPex (played by officers) and BlueOLEx (played by executives).

These exercises aim to identify improvements and potential gaps in the standardised way of responding to incidents and crises (i.e. Standard Operating Procedures), train on situational awareness and information sharing processes.

To read more: https://www.enisa.europa.eu/topics/incident-response/cyclone

SEC Enhances Rule to Prevent Misleading or Deceptive Fund Names

The Securities and Exchange Commission has adopted amendments to the Investment Company Act "Names Rule," which addresses fund names that are likely to mislead investors about a fund's investments and risks.

The amendments modernize and enhance the Names Rule and other names-related regulatory requirements to further the Commission's investor protection goals and to address developments in the fund industry in the approximately 20 years since the rule was adopted.

"As the fund industry has developed over the last two decades, gaps in the current Names Rule may undermine investor protection," said SEC Chair Gary Gensler. "Today's final rules will help ensure that a fund's portfolio aligns with a fund's name. Such truth in advertising promotes fund integrity on behalf of fund investors."

Typically, a fund's name is the first piece of information that investors receive about a fund, and fund names offer important signaling for investors in assessing their investment options.

The Names Rule currently requires registered investment companies whose names suggest a focus in a particular type of investment to adopt a policy to invest at least 80 percent of the value of their assets in those investments (an "80 percent investment policy").

The amendments to the Names Rule will enhance the rule's protections by requiring more funds to adopt an 80 percent investment policy, including funds with names suggesting a focus in investments with particular characteristics, for example, terms such as "growth" or "value," or certain terms that reference a thematic investment focus, such as the incorporation of one or more Environmental, Social, or Governance factors.

The amendments will also include a new requirement that a fund review its portfolio assets' treatment under its 80 percent investment policy at least quarterly and will include specific time frames – generally 90 days – for getting back into compliance if a fund departs from its 80 percent investment policy.

FACT SHEET

Final Rules: Amendments to the Fund "Names Rule"

The Securities and Exchange Commission adopted amendments to rule 35d-1 under the Investment Company Act of 1940, the fund "Names Rule." The amendments will better serve the Commission's mission of investor protection by:

- Improving and broadening the scope of funds that must comply with the current requirement to adopt a policy to invest at least 80 percent of their assets in accordance with the investment focus the fund's name suggests;
- Providing enhanced disclosure and reporting requirements related to terms used in fund names; and
- Establishing additional recordkeeping requirements.

Why This Matters

The name of a registered investment company or business development company ("BDC") communicates information about the fund to investors and is an important marketing tool for the fund. The purpose of the Names Rule is to prevent fund names from misrepresenting the fund's investments and risks. Typically, a fund's name is the first piece of information that investors receive about a fund and fund names offer important signaling for investors in assessing their investment options. However, because of developments in the fund industry since the adoption of the Names Rule in 2001 – including the increase in fund assets under management and the proliferation of diverse fund strategies, such as those with thematic and environmental, social, or governance ("ESG")-related objectives – the Commission is modernizing and enhancing the Names Rule and other names-related regulatory requirements to further its investor protections goals.

What's Next

The rule amendments will become effective 60 days after publication in the Federal Register. Fund groups with net assets of $1 billion or more will have 24 months to comply with the amendments, and fund groups with net assets of less than $1 billion will have 30 months to comply.

The amendments will include enhanced prospectus disclosure requirements for terminology used in fund names, including a requirement that any terms used in the fund's name that suggest an investment focus must be consistent with those terms' plain English meaning or established industry use.

The amendments will also include additional reporting and recordkeeping requirements for funds regarding compliance with the names-related regulatory requirements.

The rule amendments, adopted at a Commission open meeting on Sept. 20, 2023, will become effective 60 days after publication in the Federal Register.

Fund groups with net assets of $1 billion or more will have 24 months to comply with the amendments, and fund groups with net assets of less than $1 billion will have 30 months to comply.

To read more: https://www.sec.gov/sec-enhances-rule-prevent-misleading-or-deceptive-fund-names

https://www.sec.gov/news/press-release/2023-188

The Commission sends request for information to X under the Digital Services Act

The European Commission services has formally sent X a request for information under the Digital Services Act (DSA).

This request follows indications received by the Commission services of the alleged spreading of illegal content and disinformation, in particular the spreading of terrorist and violent content and hate speech.

The request addresses compliance with other provisions of the DSA as well.

Following its designation as Very Large Online Platform, X is required to comply with the full set of provisions introduced by the DSA since late August 2023, including the assessment and mitigation of risks related to the dissemination of illegal content, disinformation, gender-based violence, and any negative effects on the exercise of fundamental rights, rights of the child, public security and mental well-being.

In this particular case, the Commission services are investigating X's compliance with the DSA, including with regard to its policies and actions regarding notices on illegal content, complaint handling, risk assessment and measures to mitigate the risks identified.

The Commission services are empowered to request further information to X in order to verify the correct implementation of the law.

Next Steps

X needs to provide the requested information to the Commission services. Based on the assessment of X replies, the Commission will assess next steps. This could entail the formal opening of proceedings pursuant to Article 66 of the DSA.

Pursuant to Article 74 (2) of the DSA, the Commission can impose fines for incorrect, incomplete or misleading information in response to a request for information. In case of failure to reply by X, the Commission may decide to request the information by decision. In this case, failure to reply by the deadline could lead to the imposition of periodic penalty payments.

Background

The DSA is a cornerstone of the EU's digital strategy and sets out an unprecedented new standard for the accountability of online platforms

regarding disinformation, illegal content, such as illegal hate speech, and other societal risks. It includes overarching principles and robust guarantees for freedom of expression and other users' rights.

On 25 April 2023, the Commission had designated 19 Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) on the ground of their number of users being above 45 million, or 10% of EU population. These services need to comply with the full set of provisions introduced by the DSA since the end of August 2023.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953

CFPB Issues Guidance on Credit Denials by Lenders Using Artificial Intelligence

Consumers must receive accurate and specific reasons for credit denials

The Consumer Financial Protection Bureau (CFPB) issued guidance about certain legal requirements that lenders must adhere to when using artificial intelligence and other complex models.

The guidance describes how lenders must use specific and accurate reasons when taking adverse actions against consumers.

This means that creditors cannot simply use CFPB sample adverse action forms and checklists if they do not reflect the actual reason for the denial of credit or a change of credit conditions.

This requirement is especially important with the growth of advanced algorithms and personal consumer data in credit underwriting.

Explaining the reasons for adverse actions help improve consumers' chances for future credit, and protect consumers from illegal discrimination.

"Technology marketed as artificial intelligence is expanding the data used for lending decisions, and also growing the list of potential reasons for why credit is denied," said CFPB Director Rohit Chopra. "Creditors must be able to specifically explain their reasons for denial. There is no special exemption for artificial intelligence."

In today's marketplace, creditors are increasingly using complex algorithms, marketed as artificial intelligence, and other predictive decision-making technologies in their underwriting models.

Creditors often feed these complex algorithms with large datasets, sometimes including data that may be harvested from consumer surveillance.

As a result, a consumer may be denied credit for reasons they may not consider particularly relevant to their finances.

Despite the potentially expansive list of reasons for adverse credit actions, some creditors may inappropriately rely on a checklist of reasons provided in CFPB sample forms. However, the Equal Credit Opportunity Act does not allow creditors to simply conduct check-the-box exercises when

delivering notices of adverse action if doing so fails to accurately inform consumers why adverse actions were taken.

In fact, the CFPB has confirmed in a circular from last year, that the Equal Credit Opportunity Act requires creditors to explain the specific reasons for taking adverse actions.

CFPB Acts to Protect the Public from Black-Box Credit Models Using Complex Algorithms

Companies relying on complex algorithms must provide specific and accurate explanations for denying applications

MAY 26, 2022

You may visit: https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/

This requirement remains even if those companies use complex algorithms and black-box credit models that make it difficult to identify those reasons. Today's guidance expands on last year's circular by explaining that sample adverse action checklists should not be considered exhaustive, nor do they automatically cover a creditor's legal requirements.

Specifically, today's guidance explains that even for adverse decisions made by complex algorithms, creditors must provide accurate and specific reasons. Generally, creditors cannot state the reasons for adverse actions by pointing to a broad bucket.

For instance, if a creditor decides to lower the limit on a consumer's credit line based on behavioral spending data, the explanation would likely need to provide more details about the specific negative behaviors that led to the reduction beyond a general reason like "purchasing history."

Creditors that simply select the closest factors from the checklist of sample reasons are not in compliance with the law if those reasons do not sufficiently reflect the actual reason for the action taken.
Creditors must disclose the specific reasons, even if consumers may be surprised, upset, or angered to learn their credit applications were being graded on data that may not intuitively relate to their finances.

In addition to today's and last year's circulars, the CFPB has issued an advisory opinion that consumer financial protection law requires lenders to

provide adverse action notices to borrowers when changes are made to their existing credit.

CFPB Issues Advisory Opinion on Coverage of Fair Lending Laws

Equal Credit Opportunity Act continues to protect borrowers after they have applied for and received credit

MAY 09, 2022

You may visit: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-advisory-opinion-on-coverage-of-fair-lending-laws/

The CFPB has made the intersection of fair lending and technology a priority.

For instance, as the demand for digital, algorithmic scoring of prospective tenants has increased among corporate landlords, the CFPB reminded landlords that prospective tenants must receive adverse action notices when denied housing.

The CFPB also has joined with other federal agencies to issue a proposed rule on automated valuation models, and is actively working to ensure that black-box models do not lead to acts of digital redlining in the mortgage market.

To read more: https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-on-credit-denials-by-lenders-using-artificial-intelligence/

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.

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements.