Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, March 2023

Dear members and friends,

We will stert with the interesting “Investor Advisory: Exercise Caution With Third-Party Verification/Proof of Reserve Reports” from the PCAOB. We read:

“Proof of reserve reports are inherently limited, and customers should exercise extreme caution when relying on them to conclude that there are sufficient assets to meet customer liabilities.

This document represents the views of the Public Company Accounting Oversight Board’s (PCAOB or “Board”) Office of the Investor Advocate staff and not necessarily those of the Board or other PCAOB staff. It is not a rule, policy, or statement of the Board.

The Office of the Investor Advocate is aware of some service providers, including PCAOB-registered audit firms, issuing proof of reserve reports (“PoR Reports”) to certain crypto entities (e.g., crypto exchanges, stablecoin issuers).

Crypto entities may engage a service provider to issue a PoR Report in an attempt to reassure customers in response to widespread concerns about, for example, the type of reserve holdings, or, the safety and availability of customers' digital assets in the event that some or all of the customers decide to withdraw their assets (e.g., if there is a run on a crypto exchange or stablecoin issuer).

The Office of the Investor Advocate is issuing this Investor Advisory because of concerns that investors and others may place undue reliance on PoR Reports, which are not within the PCAOB's oversight authority.

Importantly, investors should note that PoR engagements are not audits and, consequently, the related reports do not provide any meaningful assurance to investors or the public.

As a general matter, these PoR Reports purport to provide an asset verification for an asset type at a particular moment in time, subject to significant limitations based on the procedures performed.

For example, the procedures undertaken likely do not address the crypto entity's liabilities, the rights and obligations of the digital asset holders, or whether the assets have been borrowed by the crypto entity to make it appear they have sufficient collateral or "reserves" in excess of customer demands.

For this reason, if the assets were borrowed by the crypto entity at the time of the PoR engagement, investors would not know based on the PoR Report.

Also, because PoR Reports concern digital assets at one point in time they do not provide any assurance about whether the assets were used, lent, or otherwise became unavailable to customers following issuance of the PoR Report.

Moreover, PoR Reports also provide no assurance regarding the effectiveness of internal controls or of governance of the crypto entity.

Despite any representations to the contrary, PoR Reports are not equivalent or more rigorous than an audit, and they are not conducted in accordance with PCAOB auditing standards.

In addition, there is a lack of uniformity regarding service providers that perform PoR engagements.

For example, some PoR engagements are performed by accounting firms, whereas others are performed by non-accountant assurance providers.

Management of the crypto entities also have discretion on whether the results of PoR reports are made public, including the extent and format of the information provided.

PoR engagements, whether intended to provide reasonable assurance, limited assurance, or no assurance (agreed-upon procedures), are not subject to PCAOB auditing standards and the engagements are not subject to PCAOB inspection.

Importantly, such reports do not provide assurance that such reserves will be adequate as of the date of the PoR Report, in the future, or that customer assets will be protected.

For "agreed-upon procedures," the management of the crypto entity, not the provider of the PoR Report, determines the procedures to be performed by the third party when conducting the engagement.

Under these circumstances, the PoR Report provides only factual findings of the outcome of the procedures performed, and there is no representation as to the sufficiency of such procedures. These types of PoR reports do not express an opinion on the adequacy of the "reserves" or the financial stability of the crypto entity or the validity of management's assertion(s).

Similarly, PoR engagements that purport to provide limited or reasonable assurance are not subject to uniform standards. Therefore, the manner in which the engagements are performed yield different results based on the different standards selected by management and PoR service providers.

Proof of reserve reports are inherently limited, and customers should exercise extreme caution when relying on them to conclude that there are sufficient assets to meet customer liabilities."

To read more: https://pcaobus.org/resources/information-for-investors/investor-advisories/investor-advisory-exercise-caution-with-third-party-verification-proof-of-reserve-reports

Agencies issue joint statement on liquidity risks resulting from crypto-asset market vulnerabilities

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing this statement on the liquidity risks presented by certain sources of funding from crypto-asset-related entities, and some effective practices to manage such risks.

The statement reminds banking organizations to apply existing risk management principles; it does not create new risk management principles.

Banking organizations are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

Liquidity Risks Related to Certain Sources of Funding from Crypto-Asset-Related Entities

This statement highlights key liquidity risks associated with crypto-assets and cryptoasset sector participants that banking organizations should be aware of.

In particular, certain sources of funding from crypto-asset-related entities may pose heightened liquidity risks to banking organizations due to the unpredictability of the scale and timing of deposit inflows and outflows, including, for example:

1. *Deposits placed by a crypto-asset-related entity that are for the benefit of the crypto-asset-related entity's customers (end customers).* The stability of such deposits may be driven by the behavior of the end customer or crypto-asset sector dynamics, and not solely by the crypto-asset-related entity itself, which is the banking organization's direct counterparty.

The stability of the deposits may be influenced by, for example,

periods of stress, market volatility, and related vulnerabilities in the crypto-asset sector, which may or may not be specific to the crypto-asset-related entity.

Such deposits can be susceptible to large and rapid inflows as well as outflows, when end customers react to crypto-asset-sector-related market events, media reports, and uncertainty.

This uncertainty and resulting deposit volatility can be exacerbated by end customer confusion related to inaccurate or misleading representations of deposit insurance by a crypto-asset related entity.

2. *Deposits that constitute stablecoin-related reserves*. The stability of such deposits may be linked to demand for stablecoins, the confidence of stablecoin holders in the stablecoin arrangement, and the stablecoin issuer's reserve management practices.

Such deposits can be susceptible to large and rapid outflows stemming from, for example, unanticipated stablecoin redemptions or dislocations in crypto-asset markets.

More broadly, when a banking organization's deposit funding base is concentrated in crypto-asset-related entities that are highly interconnected or share similar risk profiles, deposit fluctuations may also be correlated, and liquidity risk therefore may be further heightened.

Effective Risk Management Practices

In light of these heightened risks, it is important for banking organizations that use certain sources of funding from crypto-asset-related entities, such as those described above, to actively monitor the liquidity risks inherent in such funding sources and establish and maintain effective risk management and controls commensurate with the level of liquidity risks from such funding sources.

Effective practices for these banking organizations could include, for example:

• Understanding the direct and indirect drivers of potential behavior of deposits from crypto-asset-related entities and the extent to which those deposits are susceptible to unpredictable volatility.

• Assessing potential concentration or interconnectedness across deposits from cryptoasset-related entities and the associated liquidity risks.

• Incorporating the liquidity risks or funding volatility associated with crypto-asset related deposits into contingency funding planning, including

liquidity stress testing and, as appropriate, other asset-liability governance and risk management processes.

• Performing robust due diligence and ongoing monitoring of crypto-asset-related entities that establish deposit accounts, including assessing the representations made by those crypto-asset-related entities to their end customers about such deposit accounts that, if inaccurate, could lead to rapid outflows of such deposits.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20230223a.htm

CISA Director Easterly Remarks at Carnegie Mellon University

Good morning. Thank you to President Jahanian for that warm introduction and to everyone for joining me today on this Monday morning. It's wonderful to start the week off with this incredible community.

I can't think of a more fitting location for this discussion than Pittsburgh, a city built on innovation, imagination, and technological transformation; and Carnegie Mellon University, one of the world's most renowned educational institutions, home to one of our nation's top undergraduate computer science programs and top engineering programs, but also, to so much more. Let me share a few of my own favorites:

- The first smile in an email was created by research Professor Scott Fahlman, which launched the emoticon craze

- CAPTCHAs—or completely automated public Turing tests to tell computers and humans apart— (how many of you knew what that stood for?) were developed here by Professor Luis von Ahn and his colleagues, used to help prevent cybercrime

- Wireless research conducted at CMU laid the foundation for now ubiquitous wi-fi

- CMU is home to the nation's first robotics lab; and of course, home to the Software Engineering Institute, the first Federal Lab dedicated to software engineering. SEI established the first Computer Emergency Response Team, or CERT, in response to the Morris worm—that became the model for CERTs around the globe, and of course was a key partner in the creation of US-CERT in 2003, the precursor to CISA's Cybersecurity Division.

But the partnership between CMU and CISA goes well beyond technical capability – to what I consider the most important aspect of technology – People.

The CISA team is full of amazing CMU alumni like Karen Miller who leads our vulnerability evaluation work and Dr. Jono Spring, who is on the front lines of our vulnerability management work – both are here with me today.

Finally, I wanted to come here because CISA and CMU share a common set of values—collaboration, innovation, inclusion, empathy, impact, and service. And of course, a shared passion for our work.

So, now that you know why I am here, I want to start with a story.

At 2:39 pm on a chilly but sunny Saturday, just six miles off the coast of South Carolina, an F-22 fighter jet from Langley Air Force Base fired a Sidewinder air-to-air missile to take down a balloon—the size of three school buses—that had drifted across the United States.

The deliberate action came after a tense public standoff with Beijing and intense media scrutiny about the Chinese "spy balloon."

The response and surrounding attention to the issue, reinforced for me a major challenge we face in the field of cybersecurity—raising national attention to issues much less visible but in many ways far more dangerous.

Our country is subject to cyber intrusions every day from the Chinese government, but these intrusions rarely make it into national news.

Yet these intrusions can do real damage to our nation—leading to theft of our intellectual property and personal information; and even more nefariously: establishing a foothold for disrupting or destroying the cyber and physical infrastructure that Americans rely upon every hour of every day—for our power, our water, our transportation, our communication, our healthcare, and so much more.

China's massive and sophisticated hacking program is larger than that of every other major nation – combined. This is hacking on an enormous scale, but unlike the spy balloon, which was identified and dealt with, these threats more often than not go unidentified and undeterred.

The Speech: https://www.cisa.gov/cisa-director-easterly-remarks-carnegie-mellon-university

Watch the Speech:
https://www.kaltura.com/index.php/extwidget/preview/partner_id/2612992/uiconf_id/49325582/entry_id/1_s80j6080/embed/dynamic

Financial Stability Institute, FSI Insights on policy implementation No 48

When the music stops – holding bank executives accountable for misconduct

By Rita Oliveira, Ruth Walters and Raihan Zamil

Two lasting imprints of the Great Financial Crisis (GFC) were widespread failures in corporate governance and systemic breakdowns in corporate accountability and ethics.

The result was a toxic mix of bank failures or near failures that triggered financial instability and a global recession, causing widespread job losses and public bailouts of large financial firms.

Amid the economic downturn, a cascade of misconduct scandals emerged, eroding public confidence in banks and fuelling societal anger.

As misconduct cases proliferated, supervisory authorities encountered obstacles in determining the culpability of senior executives, particularly in large banks.

The dispersion of responsibility of senior executives in large firms, where decisions are taken at various levels of the firm, made it difficult to determine accountability where the wrongdoing may have occurred “under their watch”.

In addition, many prudential authorities viewed the board of directors and senior management as collective bodies and senior executives could take cover under collective decision-making.

Following the GFC, international bodies began work to strengthen the accountability of senior executives.

In 2015, the Basel Committee on Banking Supervision (BCBS) updated its corporate governance guidelines for banks (BCBS (2015)), which included a provision for supervisors to issue guidance on the clear allocation of responsibilities, accountability and transparency of a bank’s senior executives.

Subsequently, the Financial Stability Board (FSB) published a toolkit to enhance oversight of misconduct risk, including the advent of bespoke regimes that tackle individual accountability (FSB (2018)).

This paper outlines the contours of regulatory frameworks that govern the oversight of individual accountability in six jurisdictions and explores their implementation challenges. Aside from one jurisdiction, the findings draw

from an FSI survey combined with follow-up interviews. This was supplemented by a review of relevant publications in all six jurisdictions.

To date, only three authorities have introduced specific, standalone frameworks that tackle individual accountability in banks. Most authorities use general prudential frameworks to address personal accountability, with one authority using a hybrid approach that combines aspects of both standalone and prudential frameworks.

For analytical purposes, we identify two broad approaches: the introduction of free-standing, consolidated "individual accountability regimes" (referred to as "IAR jurisdictions") and reliance on broader regulatory frameworks, including hybrid approaches, to hold individuals to account ("other approaches to accountability").

The three IAR jurisdictions share core features that distinguish them from other approaches to accountability, providing a solid foundation for supervisory review.

First, IARs focus on senior executives ("covered individuals").

Second, firms are required to define and allocate certain responsibilities to covered individuals, produce "accountability statements" for each of them and develop firm-wide "responsibility maps".

Third, covered individuals can be held accountable for failings in their areas of responsibility unless they have taken "reasonable steps" to prevent breach(es) from occurring.

These provisions heighten the focus on individual accountability at the highest levels of a bank, while enabling supervisors to promptly identify the senior executive(s) responsible when a supervisory concern arises and, if warranted, to hold them accountable for actions taken by their subordinates.

Despite the similarities, differences exist among the three IARs. While all three regimes cover senior roles, the treatment of non-executive directors (NEDs) varies.

These range from including NEDs (Australia), excluding NEDs (Singapore) or including a subset of NEDs (United Kingdom (UK)) within the scope of application.

The latter is the only jurisdiction that imposes heightened conduct standards on senior executives relative to other staff and prescribes certain responsibilities that must be allocated to a senior executive(s).

Finally, both Singapore and the UK extend their IARs beyond senior executives to include staff whose activities may cause material harm to the bank or consumers.

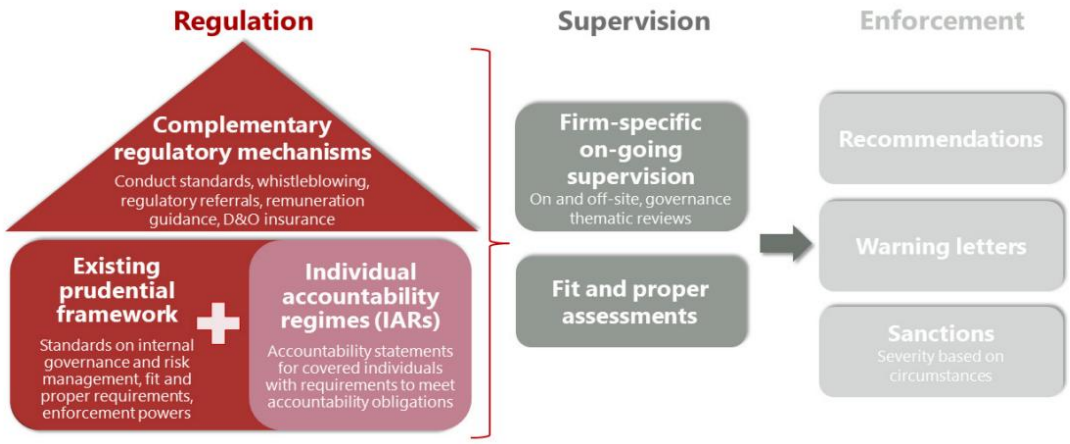
Regulatory approaches also vary among the jurisdictions without a specific IAR. The Single Supervisory Mechanism (SSM) of the European Central Bank considers individual accountability mainly during fit and proper (FAP) assessments, which applies to some senior roles.

Hong Kong SAR and the United States assess individual accountability during ongoing supervision, using common law definitions of "duty of care", "duty of loyalty" and broader prudential guidance, under which senior executives can be held accountable for misconduct.

Of the three jurisdictions without a specific IAR for banks, Hong Kong SAR comes closest, as its framework contains several elements that we identify as characterising IARs.

Of all six authorities, the US casts the broadest net, extending the reach of accountability to encompass banks' senior executives, their staff and bank-affiliated parties such as significant shareholders.

Components of individual accountability supervision — Graph 1



To read more: https://www.bis.org/fsi/publ/insights48.pdf

FSB Chair's letter to G20 Finance Ministers and Central Bank Governors

This letter was submitted to G20 Finance Ministers and Central Bank Governors (FMCBG) ahead of the G20's meeting on 24-25 February.

FSB FINANCIAL STABILITY BOARD

THE CHAIR

20 February 2023

To G20 Finance Ministers and Central Bank Governors

The financial stability outlook remains challenging. While expectations of a 'soft landing' for the global economy have grown, the outlook remains clouded by uncertainty.

The combination of near record-high levels of debt, rising debt service costs and stretched asset valuations in some key markets can pose serious threats to financial stability.

The letter lays out the FSB's work during 2023 to monitor and address these conjunctural vulnerabilities, as well as a number of structural vulnerabilities.

The letter introduces the reports the FSB is delivering to the February G20 FMCBG meeting, which cover:

The financial stability aspects of commodity markets, which forms part of the FSB's work programme to strengthen the resilience of the NBFI sector.

The financial stability risks of decentralised finance (DeFi), a fast-growing segment of the crypto-asset ecosystem. The report forms part of the FSB's work programme, jointly with sectoral standard setters, for the delivery of a consistent and comprehensive regulatory framework for crypto-assets.

Priority actions for achieving the G20 targets for enhancing cross-border payments. The report contains a detailed set of next steps to achieve the G20 cross-border payments roadmap's goals and is being accompanied by

the establishment of two new taskforces to work in partnership with the private sector.

The letter also outlines forthcoming work to enhance cyber and operational resilience; and to address climate-related financial risks, through the FSB's climate roadmap.

Crypto-assets and decentralised finance

The events of the past year, such as the collapse of FTX, have highlighted the intrinsic volatility and structural vulnerabilities of crypto-assets.

We have now seen first-hand that the failure of a key intermediary in the crypto-asset ecosystem can quickly transmit risks to other parts of that ecosystem. And, if linkages to traditional finance grow, risks from crypto-asset markets could spill over onto the broader financial system.

The G20 has charged the FSB with coordinating the delivery of an effective and comprehensive regulatory framework for cryptoassets, for which we and the sectoral standard setters have jointly put forth an ambitious 2023 work programme.

This year, the FSB will finalise its recommendations for the regulation, supervision and oversight of crypto-assets and markets and its recommendations targeted at global stablecoin arrangements, which have characteristics that may make threats to financial stability more acute.

The recommendations for global stablecoin arrangements include guidance to strengthen governance frameworks, clarify and strengthen the redemption rights and the need to maintain effective stabilisation mechanisms, among other revisions.

Importantly, the FSB's work concludes that many existing stablecoins would not currently meet these high-level recommendations, nor would they meet the international standards and supplementary, more detailed BIS Committee on Payments and Market Infrastructures-International Organization of Securities Commissions guidance.

Collectively, these recommendations seek to promote the comprehensiveness and international consistency of regulatory and supervisory approaches, recognizing that many crypto-asset activities and markets are currently not compliant with applicable regulations or are unregulated. We are working with our members, including the sectoral standard-setting bodies, to complete this critical work.

Additionally, we will deliver a joint paper with the IMF later this year that synthesises the policy findings from IMF work on macroeconomic and

monetary issues and FSB work on supervisory and regulatory issues associated with cryptoassets.

We will also explore how to address the cross-border risks specific to EMDEs. Publication of the FSB's recommendations will only be the beginning of the next phase of work in this area, as the standard-setting bodies will need to make their own, more detailed, recommendations, and member jurisdictions will need to implement the recommendations.

The FSB will continue to coordinate that work, as necessary, and going forward will monitor implementation of the recommendations together with the standard-setters.

Once the work is completed, the appropriate regulation of crypto-assets, based on the principle of 'same activity, same risk, same regulation' will provide the beginning of a strong basis for harnessing potential benefits associated with this form of financial innovation while containing its risks.

Within the crypto-asset ecosystem, so-called decentralised finance (DeFi) has emerged as a fast-growing segment, and we are delivering to this meeting a report on DeFi.

Our report points to the need for proactive monitoring, filling data gaps, and exploring to what extent the cryptoasset recommendations may need to be enhanced to cover DeFi risks.

We will build on this work to examine whether additional policy recommendations are needed to deal with this growing segment.

The FSB continues to conduct forward-looking analysis to assess the implications of cryptoassets for financial stability.

This year we are undertaking in-depth analysis of the large cryptoasset intermediaries that provide a wide range of services to the ecosystem.

We will also undertake analysis of the increasing trend toward the tokenisation of assets and how that could affect financial stability.

Enhancing cross-border payments
One factor that has helped spur the development of the crypto-asset ecosystem is dissatisfaction with the existing system of cross-border payments.

In 2020, G20 Leaders endorsed the Roadmap for Enhancing Cross-border Payments, in order to address the frictions that such payments currently face and thereby achieve faster, cheaper, more transparent and more inclusive cross-border payment services.

Last year we reported to the G20 that this work had reached the next phase, focused on implementation.

For this meeting, the FSB is delivering a report with detailed next steps under the new phase of the Roadmap, comprising high-priority, practical steps to achieve the Roadmap's goals.

This is being accompanied by the setting up of two new taskforces to work in partnership with the private sector as we take the work forward. Continued G20 support remains vital here.

To read more: https://www.fsb.org/wp-content/uploads/P200223-1.pdf

European Parliament resolution on the adequacy of the protection afforded by the EU-US Data Privacy Framework

European Parliament
2019-2024

Committee on Civil Liberties, Justice and Home Affairs

DRAFT MOTION FOR A RESOLUTION, to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)) Juan Fernando López Aguilar, on behalf of the Committee on Civil Liberties, Justice and Home Affairs

The European Parliament,

– having regard to the Charter of Fundamental Rights of the European Union ('the Charter'), in particular Articles 7, 8, 16, 47 and 52 thereof,

– having regard to the judgment of the Court of Justice of 6 October 2015 in Case C-362/14 Maximillian Schrems v Data Protection Commissioner ('Schrems I'),

– having regard to the judgment of the Court of Justice of 16 July 2020 in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'),

– having regard to its enquiry into the revelations made by Edward Snowden on the electronic mass surveillance of EU citizens, including the findings in its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,

– having regard to its resolution of 26 May 2016 on transatlantic data flows,

– having regard to its resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield,

– having regard to its resolution of 20 May 2021 on the ruling of the CJEU of 16 July 2020 – Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ('Schrems II'), Case C-311/18,

– having regard to the Commission draft Implementing Decision 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,

– having regard to President of the United States' Executive Order 14086 of 7 October 2022 on Enhancing Safeguards For United States Signals Intelligence Activities,

– having regard to the Regulation on the Data Protection Review Court issued by the US Attorney General ('AG Regulation'),

– having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ('GDPR'), in particular Chapter V thereof,

– having regard to the Commission proposal of 10 January 2017 for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010), to the decision to enter into interinstitutional negotiations confirmed by Parliament's plenary on 25 October 2017, and to the Council's general approach adopted on 10 February 2021 (6087/21),

– having regard to the European Data Protection Board (EDPB) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, and to the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures,

– having regard to the EDPB Opinion of [to be added],

– having regard to Rule 132(2) of its Rules of Procedure,

A. whereas in the 'Schrems I' judgment, the Court of Justice of the European Union (CJEU) invalidated the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, and pointed out that indiscriminate access by intelligence authorities to the content of electronic communications violates the essence of the fundamental right to confidentiality of communications provided for in Article 7 of the Charter;

B. whereas in the 'Schrems II' judgment, the CJEU invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield and concluded that it did not provide sufficient legal remedies against mass surveillance for non-US nationals and that this violates the essence of the fundamental right to a legal remedy as provided for in Article 47 of the Charter;

C. whereas on 7 October 2022, the President of the United States of America signed Executive Order 14086 on Enhancing Safeguards For United States Signals Intelligence Activities ('EO');

D. whereas on 13 December 2022 the Commission launched the process to adopt an adequacy decision for the EU-US Data Privacy Framework;

E. whereas, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the rules applicable in that country deriving from its domestic law or its international commitments, as well as the practice designed to ensure compliance with those rules;

F. whereas the ability to transfer personal data across borders has the potential to be a key driver of innovation, productivity and economic competitiveness; whereas these transfers should be carried out in full respect for the right to the protection of personal data and the right to privacy; whereas one of the fundamental objectives of the EU is the protection of fundamental rights, as enshrined in the Charter;

G. whereas the GDPR applies to all companies processing the personal data of data subjects in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the Union, or the monitoring of their behaviour as far as their behaviour takes place within the Union;

H. whereas mass surveillance, including the bulk collection of data, by state actors is detrimental to the trust of European citizens and businesses in digital services and, by extension, in the digital economy;
I. whereas controllers should always be accountable for compliance with data protection obligations, including demonstrating compliance for any data processing whatever its nature, scope, context, purposes and risks for data subjects;

J. whereas there is no federal privacy and data protection legislation in the United States (US); whereas the EU and the US have differing definitions of key data protection concepts such as principles of necessity and proportionality;

1. Recalls that privacy and data protection are legally enforceable fundamental rights enshrined in the Treaties, the Charter and the European Convention of Human Rights, as well as in laws and case-law; emphasises that they must be applied in a manner that does not unnecessarily hamper trade or international relations, but can be balanced only against other fundamental rights and not against commercial or political interests;

2. Acknowledges the efforts made in the EO to lay down limits on US Signals Intelligence Activities, by referring to the principles of proportionality and necessity, and providing a list of legitimate objectives for such activities; points out, however, that these principles are long-standing key elements of the EU data protection regime and that their substantive definitions in the EO are not in line with their definition under EU law and their interpretation by the CJEU; points out, furthermore, that for the purposes of the EU-US Data Privacy Framework, these principles will be interpreted solely in the light of US law and legal traditions; points out that the EO requires that signals intelligence must be conducted in a manner proportionate to the 'validated intelligence priority', which appears to be a broad interpretation of proportionality;

3. Regrets the fact that the EO does not prohibit the bulk collection of data by signals intelligence, including the content of communications; notes that the list of legitimate national security objectives can be expanded by the US President, who can determine not to make the relevant updates public;

4. Points out that the EO does not apply to data accessed by public authorities via other means, for example through the US Cloud Act or the US Patriot Act, by commercial data purchases, or by voluntary data sharing agreements;

5. Points out that the decisions of the Data Protection Review Court ('DPRC') will be classified and not made public or available to the complainant; points out that the DPRC is part of the executive branch and not the judiciary; points out that a complainant will be represented by a 'special advocate' designated by the DPRC, for whom there is no requirement of independence; points out that the redress process provided by the EO is based on secrecy and does not set up an obligation to notify the complainant that their personal data has been processed, thereby undermining their right to access or rectify their data; notes that the proposed redress process does not provide for an avenue for appeal in a federal court and therefore, among other things, does not provide any possibility for the complainant to claim damages; concludes that the DPRC does not meet the standards of independence and impartiality of Article 47 of the Charter;

6. Notes that, while the US has provided for a new mechanism for remedy for issues related to public authorities' access to data, the remedies available for commercial matters under the adequacy decision are insufficient; notes that these issues are largely left to the discretion of companies, which can select alternative remedy avenues such as dispute resolution mechanisms or the use of companies' privacy programmes;

7. Notes that European businesses need and deserve legal certainty; stresses that successive data transfer mechanisms, which were subsequently repealed by the CJEU, created additional costs for European businesses; notes that continuing uncertainty and the need to adapt to new legal solutions is particularly burdensome for micro, small and medium-sized enterprises;

8. Points out that, unlike all other third countries that have received an adequacy decision under the GDPR, the US still does not have a federal data protection law; points out that the EO is not clear, precise or foreseeable in its application, as it can be amended at any time by the US President; is therefore concerned about the absence of a sunset clause which could provide that the decision would automatically expire four years after its entry into force;

9. Emphasises that adequacy decisions must include clear and strict mechanisms for monitoring and review in order to ensure that decisions are future proof and that EU citizens' fundamental right to data protection is guaranteed;

Conclusions

10. Recalls that, in its resolution of 20 May 2021, Parliament called on the Commission not to adopt any new adequacy decision in relation to the US, unless meaningful reforms were introduced, in particular for national security and intelligence purposes;

11. Concludes that the EU-US Data Privacy Framework fails to create actual equivalence in the level of protection; calls on the Commission to continue negotiations with its US counterparts with the aim of creating a mechanism that would ensure such equivalence and which would provide the adequate level of protection required by Union data protection law and the Charter as interpreted by the CJEU; urges the Commission not to adopt the adequacy finding;

12. Instructs its President to forward this resolution to the Council, the Commission and the President and Congress of the United States of America.

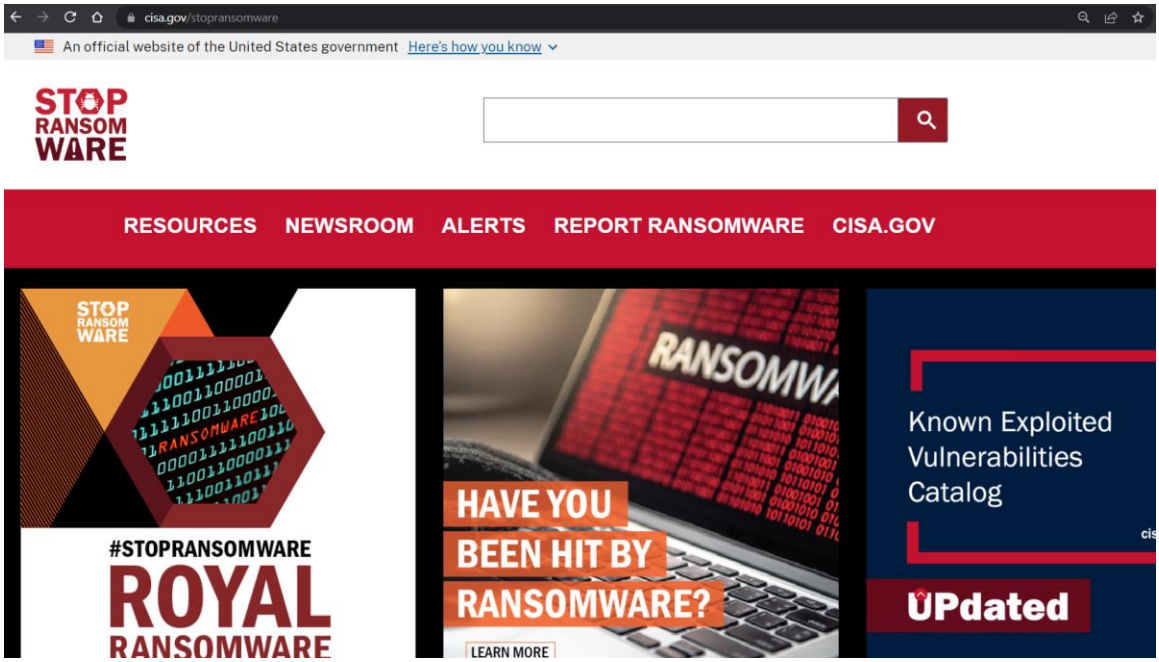
Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA)

#StopRansomware: Royal Ransomware

This joint Cybersecurity Advisory (CSA) is part of an ongoing effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors.

These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware.

Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.



The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Royal ransomware IOCs and TTPs identified through FBI threat response activities as recently as January 2023.

Since approximately September 2022, cyber criminals have compromised U.S. and international organizations with a Royal ransomware variant.

FBI and CISA believe this variant, which uses its own custom-made file encryption program, evolved from earlier iterations that used "Zeon" as a loader.

After gaining access to victims' networks, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems.

Royal actors have made ransom demands ranging from approximately $1 million to $11 million USD in Bitcoin.

In observed incidents, Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note.

Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor via a .onion URL (reachable through the Tor browser).

Royal actors have targeted numerous critical infrastructure sectors including, but not limited to, Manufacturing, Communications, Healthcare and Public Healthcare (HPH), and Education.

Initial Access

Royal actors gain initial access to victim networks in a number of ways including:

- **Phishing.** According to third-party reporting, Royal actors most commonly (in 66.7% of incidents) gain initial access to victim networks via successful phishing emails [T1566].
  - According to open-source reporting, victims have unknowingly installed malware that delivers Royal ransomware after receiving phishing emails containing malicious PDF documents [T1566.001], and malvertising [T1566.002].[2]
- **Remote Desktop Protocol (RDP).** The second most common vector Royal actors use (in 13.3% of incidents) for initial access is RDP compromise.
- **Public-facing applications.** FBI has also observed Royal actors gain initial access through exploiting public-facing applications [T1190].
- **Brokers.** Reports from trusted third-party sources indicate that Royal actors may leverage brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs.

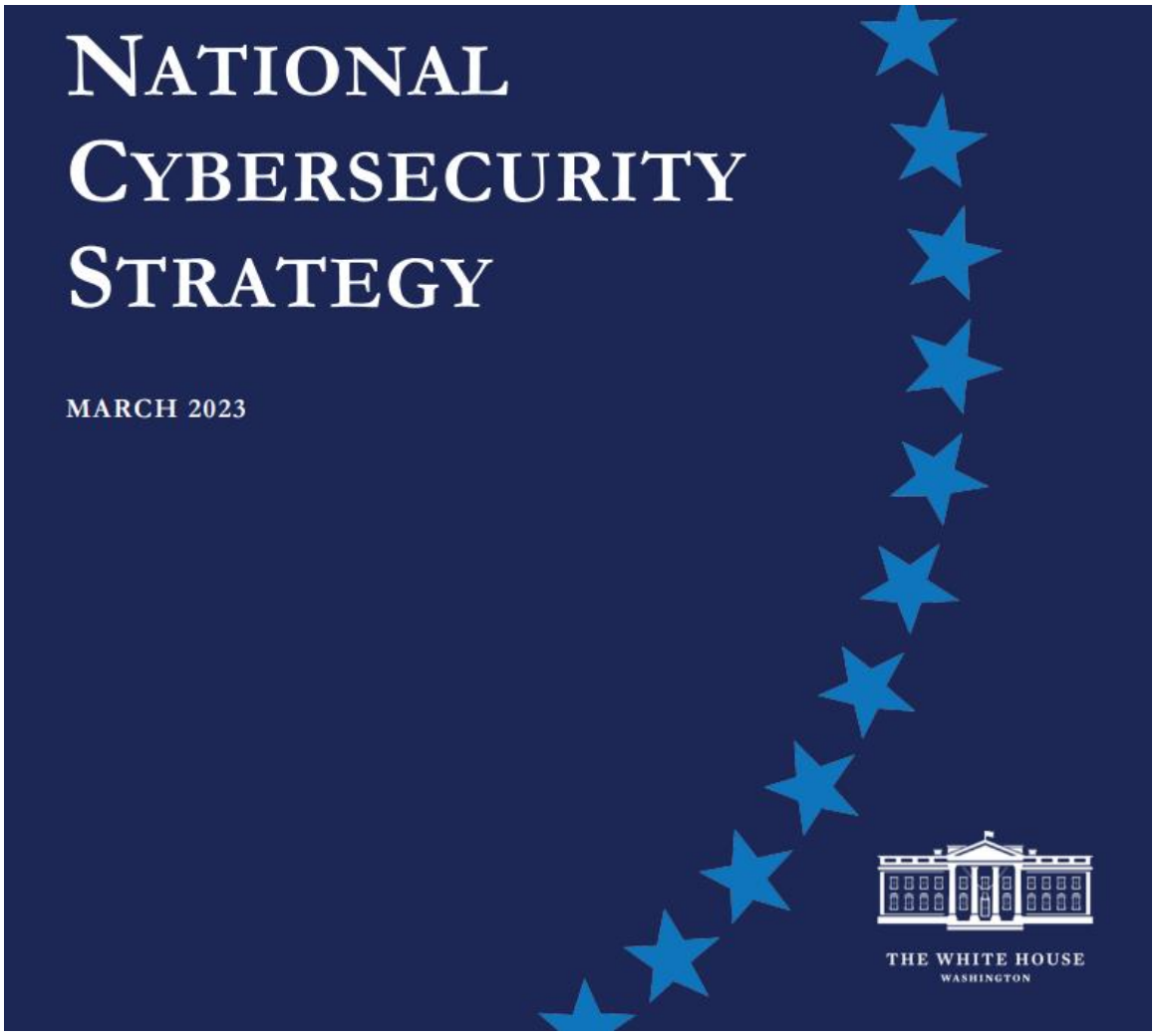
To read more: https://www.cisa.gov/sites/default/files/2023-03/aa23-061a-stopransomware-royal-ransomware.pdf

The new US National Cybersecurity Strategy

THE WHITE HOUSE

The Biden-Harris Administration released the National Cybersecurity Strategy to secure the full benefits of a safe and secure digital ecosystem for all Americans.

In this decisive decade, the United States will reimagine cyberspace as a tool to achieve our goals in a way that reflects our values: economic security and prosperity; respect for human rights and fundamental freedoms; trust in our democracy and democratic institutions; and an equitable and diverse society. To realize this vision, we must make fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.



1. We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.

2. We must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.

The Strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity.

TABLE OF CONTENTS

VISION

Our rapidly evolving world demands a more intentional, more coordinated, and more well-resourced approach to cyber defense. We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests. At the same time, next-generation technologies are reaching maturity at an accelerating pace, creating new pathways for innovation while increasing digital interdependencies.

This Strategy sets out a path to address these threats and secure the promise of our digital future. Its implementation will protect our investments in rebuilding America's infrastructure, developing our clean energy sector, and re-shoring America's technology and manufacturing base. Together with our allies and partners, the United States will make our digital ecosystem:

- **Defensible,** where cyber defense is overwhelmingly easier, cheaper, and more effective;

- **Resilient,** where cyber incidents and errors have little widespread or lasting impact; and,

- **Values-aligned,** where our most cherished values shape—and are in turn reinforced by— our digital world.

The Administration has already taken steps to secure cyberspace and our digital ecosystem, including the National Security Strategy, Executive Order 14028 (Improving the Nation's Cybersecurity), National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems), M-22-09 (Moving the U.S. Government Toward Zero-Trust Cybersecurity Principles), and National Security Memorandum 10 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems). Expanding on these efforts, the Strategy recognizes that cyberspace does not exist for its own end but as a tool to pursue our highest aspirations.

APPROACH

This Strategy seeks to build and enhance collaboration around five pillars:

1. **Defend Critical Infrastructure** – We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides, including by:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance;

- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services; and,

- Defending and modernizing Federal networks and updating Federal incident response policy

2. **Disrupt and Dismantle Threat Actors** – Using all instruments of national power, we will make malicious cyber actors incapable of threatening the national security or public safety of the United States, including by:

- Strategically employing all tools of national power to disrupt adversaries;

- Engaging the private sector in disruption activities through scalable mechanisms; and,

- Addressing the ransomware threat through a comprehensive Federal approach and in lockstep with our international partners.

PILLAR TWO | DISRUPT AND DISMANTLE THREAT ACTORS

The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests. These efforts may integrate diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities. Our goal is to make malicious actors incapable of mounting sustained cyber-enabled campaigns that would threaten the national security or public safety of the United States.

3. **Shape Market Forces to Drive Security and Resilience** – We will place responsibility on those within our digital ecosystem that are best positioned to reduce risk and shift the consequences of poor cybersecurity away from the most vulnerable in order to make our digital ecosystem more trustworthy, including by:

- Promoting privacy and the security of personal data;

- Shifting liability for software products and services to promote secure development practices; and,
- Ensuring that Federal grant programs promote investments in new infrastructure that are secure and resilient.

4. **Invest in a Resilient Future** – Through strategic investments and coordinated, collaborative action, the United States will continue to lead the world in the innovation of secure and resilient next-generation technologies and infrastructure, including by:

- Reducing systemic technical vulnerabilities in the foundation of the Internet and across the digital ecosystem while making it more resilient against transnational digital repression;

- Prioritizing cybersecurity R&D for next-generation technologies such as postquantum encryption, digital identity solutions, and clean energy infrastructure; and,

- Developing a diverse and robust national cyber workforce

5. **Forge International Partnerships to Pursue Shared Goals** – The United States seeks a world where responsible state behavior in cyberspace is expected and reinforced and where irresponsible behavior is isolating and costly, including by:

- Leveraging international coalitions and partnerships among like-minded nations to counter threats to our digital ecosystem through joint preparedness, response, and cost imposition;

- Increasing the capacity of our partners to defend themselves against cyber threats, both in peacetime and in crisis; and,
- Working with our allies and partners to make secure, reliable, and trustworthy global supply chains for information and communications technology and operational technology products and services.

Coordinated by the Office of the National Cyber Director, the Administration's implementation of this Strategy is already underway.

To read more: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

U.S. Department of Justice, Criminal Division

Evaluation of Corporate Compliance Programs (Updated March 2023)

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements.

These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one.").

- **Root Cause Analysis** – What is the company's root cause analysis of the misconduct at issue? Were any systemic issues identified? Who in the company was involved in making the analysis?

- **Prior Weaknesses** – What controls failed? If policies or procedures should have prohibited the misconduct, were they effectively implemented, and have functions that had ownership of these policies and procedures been held accountable?

- **Payment Systems** – How was the misconduct in question funded (*e.g.*, purchase orders, employee reimbursements, discounts, petty cash)? What processes could have prevented or detected improper access to these funds? Have those processes been improved?

- **Vendor Management** – If vendors were involved in the misconduct, what was the process for vendor selection and did the vendor undergo that process?

- **Prior Indications** – Were there prior opportunities to detect the misconduct in question, such as audit reports identifying relevant control failures or allegations, complaints, or investigations? What is the company's analysis of why such opportunities were missed?

- **Remediation** – What specific changes has the company made to reduce the risk that the same or similar issues will occur in the future? What specific remediation has addressed the issues identified in the root cause and missed opportunity analysis?

Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine.

Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate

(1) form of any resolution or prosecution;
(2) monetary penalty, if any; and
(3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs.

We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation.

Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program.

There are, however, common questions that we may ask in the course of making an individualized determination.

As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?

2. Is the program being applied earnestly and in good faith?
In other words, is the program adequately resourced and empowered to function effectively?

To read more: https://www.justice.gov/criminal-fraud/page/file/937501/download

Proposal for a regulation on Markets in Crypto-assets (MiCA)

This proposal seeks to provide legal certainty for crypto-assets not covered by existing EU financial services legislation and establish uniform rules for crypto-asset service providers and issuers at EU level. The proposed Regulation will replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation and also establish specific rules for so-called 'stablecoins', including when these are e-money. The proposed Regulation is divided into nine Titles.

Title I sets the subject matter, the scope and the definitions. Article 1 sets out that the Regulation applies to crypto-asset service providers and issuers, and establishes uniform requirements for transparency and disclosure in relation to issuance, operation, organisation and governance of crypto-asset service providers, as well as establishes consumer protection rules and measures to prevent market abuse.

Article 2 limits the scope of the Regulation to crypto-assets that do not qualify as financial instruments, deposits or structured deposits under EU financial services legislation.

Article 3 sets out the terms and definitions that are used for the purposes of this Regulation, including 'crypto-asset', 'issuer of crypto-assets', 'asset-referenced token' (often described as 'stablecoin'), 'e-money token' (often described as 'stablecoin'), 'crypto-asset service provider', 'utility token' and others.

Article 3 also defines the various crypto-asset services. Importantly, the Commission may adopt delegated acts to specify some technical elements of the definitions, to adjust them to market and technological developments.

Title II regulates the offerings and marketing to the public of crypto-assets other than asset-referenced tokens and e-money tokens.

It indicates that an issuer shall be entitled to offer such crypto-assets to the public in the Union or seek an admission to trading on a trading platform for such crypto-assets if it complies with the requirements of Article 4, such as the obligation to be established in the form of a legal person or the obligation to draw up a crypto-asset white paper in accordance with Article 5 (with Annex I) and the notification of such a crypto-asset white paper to the competent authorities (Article 7) and its publication (Article 8).

Once a whitepaper has been published, the issuer of crypto-assets can offer its crypto-assets in the EU or seeks an admission of such crypto-assets to trading on a trading platform (Article 10).

Article 4 also includes some exemptions from the publication of a whitepaper, including for small offerings of crypto-assets (below €1 million within a twelve-month period) and offerings targeting qualified investors as defined by the Prospectus Regulation (Regulation EU 2017/1129).

Article 5 and Annex I of the proposal set out the information requirements regarding the crypto-asset white paper accompanying an offer to the public of crypto-assets or an admission of crypto-assets to a trading platform for crypto-assets, while Article 6 imposes some requirements related to the marketing materials produced by the issuers of crypto-assets, other than asset-referenced tokens or e-money tokens.

The crypto-asset white paper will not be subject to a pre-approval process by the national competent authorities (Article 7). It will be notified to the national competent authorities with an assessment whether the crypto-asset at stake constitutes a financial instrument under the Markets in Financial Instruments Directive (Directive 2014/65/EU), in particular.

After the notification of the crypto-asset white paper, competent authorities will have the power to suspend or prohibit the offering, require the inclusion of additional information in the crypto-asset white paper or make public the fact that the issuer is not complying with the Regulation (Article 7).

Title II also includes specific provisions on the offers of crypto-assets that are limited in time (Article 9), the amendments of an initial crypto-asset white paper (Article 11), the right of withdrawal granted to acquirers of crypto-assets (Article 12), the obligations imposed on all issuers of crypto-assets (Article 13) and on the issuers' liability attached to the crypto-asset white paper (Article 14).

Title III, Chapter 1 describes the procedure for authorisation of asset-referenced token issuers and the approval of their crypto-asset white paper by national competent authorities (Articles 16 to 19 and Annexes I and II). To be authorised to operate in the Union, issuers of asset-referenced tokens shall be incorporated in the form of a legal entity established in the EU (Article 15).

Article 15 also indicates that no asset-referenced tokens can be offered to the public in the Union or admitted to trading on a trading platform for crypto-assets if the issuer is not authorised in the Union and it does not publish a crypto-asset white paper approved by its competent authority. Article 15 also includes exemptions for small-scale asset-referenced tokens

and for asset-referenced tokens that are marketed, distributed and exclusively held by qualified investors. Withdrawal of an authorisation is detailed in Article 20 and Article 21 sets out the procedure for modifying the crypto-asset white paper.

Title III, Chapter 2 sets out the obligations for issuers of asset-referenced tokens. It states they shall act honestly, fairly and professionally (Article 23). It lays down the rules for the publication of the crypto-asset white paper and potential marketing communications (Article 24) and the requirements for these communications (Article 25). Further, issuers are subject to ongoing information obligations (Article 26) and they are required to establish a complaint handling procedure (Article 27).

They shall also comply with other requirements, such as rules on conflicts of interest (Article 28), notification on changes to their management body to its competent authority (Article 29), governance arrangements (Article 30), own funds (Article 31), rules on the reserve of assets backing the asset-referenced tokens (Article 32) and requirements for the custody of the reserve assets (Article 33).

Article 34 explains that an issuer shall only invest the reserve assets in assets that are secure, low risk assets. Article 35 also imposes on issuers of asset-referenced tokens the disclosure of the rights attached to the asset-referenced tokens, including any direct claim on the issuer or on the reserve of assets. Where the issuer of asset-referenced tokens does not offer direct redemption rights or claims on the issuer or on the reserve assets to all holders of asset-reference tokens, Article 35 provides holders of asset-referenced tokens with minimum rights. Article 36 prevents issuers of asset-referenced tokens and crypto-asset service providers from granting any interest to holders of asset-referenced tokens.

Title III, Chapter 4, sets out the rules for the acquisition of issuers of asset-referenced tokens, with Article 37 detailing the assessment of an intended acquisition, and Article 38 the content of such an assessment.

Title III, Chapter 5, Article 39 sets out the criteria that EBA shall use when determining whether an asset-referenced token is significant. These criteria are: the size of the customer base of the promoters of the asset-referenced tokens, the value of the asset-referenced tokens or their market capitalisation, the number and value of transactions, size of the reserve of assets, significance of the issuers' cross-border activities and the interconnectedness with the financial system.
Article 39 also includes an empowerment for the Commission to adopt a delegated act in order to specify further the circumstances under which and thresholds above which an issuer of asset-referenced tokens will be considered significant. Article 39 includes some minimum thresholds that the delegated act shall in any case respect.

Article 40 details the possibility for an issuer of an asset-referenced token to classify as significant at the time of applying for an authorisation on their own initiative. Article 41 lists the additional obligations applicable to issuers of significant asset-referenced tokens, such as additional own funds requirements, liquidity management policy and interoperability.

Tittle III, Chapter 6, Article 42 obliges the issuer to have a procedure in place for an orderly wind-down of their activities.

Title IV, Chapter 1 describes the procedure for authorisation as an issuer of e-money tokens. Article 43 describes that no e-money tokens shall be offered to the public in the Union or admitted to trading on a crypto-asset trading platform unless the issuer is authorised as a credit institution or as an 'electronic money institution' within the meaning of Article 2(1) of Directive 2009/110/EC. Article 43 also states that 'e-money tokens' are deemed electronic money for the purpose of Directive 2009/110/EC.

Article 44 describes how holders of e-money tokens shall be provided with a claim on the issuer: e-money tokens shall be issued at par value and on the receipt of funds, and upon request by the holder of e-money tokens, the issuers must redeem them at any moment and at par value. Article 45 prevents issuers of e-money tokens and crypto-asset service providers from granting any interest to holders of e-money tokens.

Article 46 and Annex III sets out the requirements for the crypto-asset white paper accompanying the issuance of e-money tokens, for example: description of the issuer, detailed description of the issuer's project, indication of whether it concerns an offering of e-money tokens to the public or admission of these to a trading platform, as well as information on the risks relating to the e-money issuer, the e-money tokens and the implementation of any potential project.

Article 47 includes provision on the liability attached to such crypto-asset white paper related to e-money tokens. Article 48 sets requirements for potential marketing communications produced in relation to an offer of e-money tokens and Article 49 states that any funds received by an issuer in exchange for e-money tokens, shall be invested in assets denominated in the same currency as the one referenced by the e-money token.

Title IV, Chapter 2, Article 50 states that the EBA shall classify e-money tokens as significant on the basis of the criteria listed in Article 39. Article 51 details the possibility of an issuer of an e-money token to classify as significant at the time of applying for an authorisation on their own initiative. Article 52 contains the additional obligations applicable to issuers of significant e-money tokens. Issuers of significant e-money tokens must apply Article 33 on the custody of the reserve assets and Article 34 on the investment of these assets instead of Article 7 of Directive

2009/110/EC, Article 41, paragraphs 1, 2, and 3 on remuneration, interoperability and liquidity management, Article 41, paragraph 4 instead of Article 5 of Directive 2009/110/EC and Article 42 on an orderly wind-down of their activities.

To read more: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0593&from=EN

Remarks at the IIB Annual Washington Conference "Trust and Global Banking: Lessons for Crypto".

Acting Comptroller of the Currency Michael J. Hsu.

Office of the Comptroller of the Currency

Thank you for inviting me to the 2023 Institute of International Bankers (IIB) Annual Washington Conference. It is a pleasure and an honor to be here.

I would like to speak today about what it takes to build and maintain trust in global banking and what lessons this may hold for crypto. In particular, I believe there are strong parallels between FTX and the Bank of Credit and Commerce International – better known in bank regulatory circles as BCCI – which failed in 1991 and led to significant changes in how global banks are supervised.

Let me start by highlighting key features of the trust architecture for global banking that has been constructed over the past several decades. That will lead to a discussion of BCCI, parallels to FTX, and lessons for crypto.

Trust in Global Banking Banking is global, while bank regulation and supervision are local. This creates challenges for bank regulators located in different jurisdictions tasked with ensuring the safety and soundness of different parts of global banks.

There are two key risks. First, there is the risk of an unlevel playing field – where rules differ by jurisdiction – which can enable regulatory arbitrage by banks and drive races to the bottom by local authorities. Second, there is the risk of regulators having limited visibility into and influence over global banks – what one might call "supervisability" risk. Host and home regulators, having differing lines of sight and authorities into different entities within a global bank, may struggle to see the true risk profile of the enterprise and may be limited in their abilities to address gaps.

The risk of an unlevel playing field can be mitigated by coordination among home and host authorities, while the supervisability risk of global banks can only be solved through collaboration.

To read more: https://www.ots.treas.gov/news-issuances/speeches/2023/pub-speech-2023-23.pdf

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.

Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified and provide independent evidence that you are a Sarbanes-Oxley expert.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

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