CLIFFORD
CHANCE

31 January 2024

Consultation response

Basel Committee on Banking Supervision—Disclosure of cryptoasset exposures

The Global Financial Markets Association[1], the Institute of International Finance, the International Swaps and Derivatives Association, and the International Capital Market Association (collectively, the "**Associations**"[2]) appreciate the opportunity to respond to the Committee's Consultative Document on the "**Disclosure of cryptoasset exposures**" (referred to hereafter as the "**Consultation**") and to assist the Committee in refining its approach to the disclosure of cryptoasset exposures.

EXECUTIVE SUMMARY

General issues

The Associations support the development of responsible, well-balanced disclosures of cryptoasset exposures in the financial sector. While noting that there are certain outstanding issues in the Committee's prudential treatment of cryptoasset exposures, including in relation to the use of permissionless blockchains for Group 1 cryptoassets and the parallel consultation on the criteria for stablecoins to receive a less conservative Group 1b treatment, we remain of the view that an appropriately calibrated disclosure regime would support responsible adoption of novel technologies in the financial markets by helping to improve the confidence of investors and the wider market around this developing asset class.

However, we have a number of concerns with the general policy approach, and level of detail, reflected in the Consultation's proposed disclosure requirements. The proposed disclosure ultimately may impact the safe and responsible development of a sound global cryptoasset market and could detrimentally affect the overall transparency of this market, as well as associated resource allocation by investors and market participants.

In addition to providing our feedback on the Consultation's specific questions, we have identified a number of other areas of concern related to the correct calibration of any disclosure requirements for banks' exposures to cryptoassets.

Policy approach—It is critical that any final disclosure framework be appropriately tailored to meet the policy objectives of the Committee's Pillar 3 regime. According to Basel's Disclosure Requirements (DIS)[3], disclosures should enable market participants to access key information relating to a bank's regulatory capital and risk exposures and be meaningful to users, represent a bank's significant risk, and not include information that does not add value to users' understanding. The proposed disclosure requirements would call for a level of detail that well exceeds traditional notions of materiality, leading to the anticipated disclosure of significantly more information than is necessary for market participants to understand banks' cryptoasset exposures and related activities. This may introduce more confusion than clarity, and result in disproportionate operational complexity for users, disclosing institutions and supervisors. In some cases, the proposed disclosure

[1] GFMA brings together three financial trade associations, including the Association for Financial Markets in Europe (AFME), the Asia Securities Industry & Financial Markets Association (ASIFMA), and the Securities Industry and Financial Markets Association (SIFMA).

[2] See the Appendix for information regarding each of the Associations.

[3] See https://www.bis.org/basel_framework/chapter/DIS/10.htm, Principle 3.

requirements would not contribute to the market discipline or transparency that Pillar 3 aims to accomplish, and instead would be more akin to a confidential supervisory information request intended to facilitate authorities' supervision of the cryptoasset market. Any final disclosure framework also should balance the level of disclosure with the level of risk-taking in which a bank may engage. For example, Group 2 cryptoassets will have a relatively low impact on a bank's overall risk exposure due to the quantitative limitations the Committee's prudential standard imposes relative to Tier 1 capital. We strongly urge the Committee to reconsider whether the highly granular proposed disclosure requirements are appropriate for what we understand the aims of Pillar 3 to be.

Duplicative disclosures—The Committee must also be mindful of, and avoid, potential duplication of disclosure requirements across the Basel Framework (for example, for Group 1a cryptoassets, which are subject to existing Pillar 3 non-cryptoasset disclosure requirements), which would add little to market participants' understanding of banks' activities, exposures, and risk profiles while disproportionately adding to operational complexity. In practice, duplicative disclosures can also result in confusion and therefore result in a reduction of clarity around a financial institution's activities, exposures, and risk profile, which is contrary to the aims of Pillar 3. While we do not believe a duplicative separate disclosure of Group 1a cryptoassets is warranted, we recognize that there is an expectation that the volume of such transactions will grow in the future. Therefore, we propose that a disclosure could include Group1a cryptoassets by tokenized instrument type (equity, fixed income, commodity, etc.) and total value at the end of the reporting period.

Forward-looking requirements—The development of any final disclosure framework must consider the substantial likelihood of wider adoption of innovative technologies across financial markets over time and the further growth and evolution of cryptoasset markets. Any cryptoasset–specific disclosure regime must be appropriate in scale and remain fit for purpose when the market is in a more developed future state. For a final disclosure framework to remain appropriate over time, it must be calibrated so that the utility provided to its intended users, in furtherance of the objectives of the Committee's Pillar 3, continues to outweigh the attendant costs and operational complexity. For example, Group 1a assets (tokenized traditional assets) are expected to increase in volume in the future. It would be impractical to disclose the detailed level of information for hundreds or thousands of different Group 1a cryptoassets and inconsistent with the disclosures for current traditional assets. This also demonstrates the necessity of the principle of materiality being appropriately defined and applicable to the disclosure regime. The disclosure regime for banks' cryptoasset exposures also must properly account for the number and diversity of financial products that fall under the Committee's definition of cryptoasset; we are concerned that the proposed disclosure requirements do not adequately distinguish between Group 1a, Group 1b and Group 2 cryptoassets despite the critical differences in their characteristics and risk profiles. Critically, we also note that Group 1a cryptoassets would already be subject to the existing Pillar 3 disclosure framework, as the Committee describes throughout the Consultation.

Classification condition assessment detail

The level of detail contemplated by the Table CAEA disclosure requirements for the classification conditions for Group 1 cryptoassets is not consistent with the disclosure-related goals embedded in the Basel Framework. The detailed, complex information banks would be required to disclose would make it more difficult, relative to a more general disclosure, for market participants to understand how banks approach assessing the classification conditions. A more general disclosure for banks' approaches to assessing the classification conditions also would be better suited to a future where tokenization becomes more widespread, as it would be impractical and of limited utility for banks to produce detailed information for numerous Group 1 cryptoassets. For similar reasons, we therefore also disagree with the proposed addition of the potential elements listed in Annex 2 to the Consultation. Finally, we support the exclusion of confidential and proprietary information in the proposed disclosure requirements related to the classification conditions. However, the appropriate exclusion of such information could have the unintended result of producing incomplete, confusing, or misleading descriptions of banks' approaches to assessing the classification conditions. A more general disclosure of banks' approaches to the classification conditions would avoid this suboptimal policy outcome.

Window dressing

We disagree with the Committee's suggestion that there would be merit in requiring banks to disclose daily average values for the amounts in Template CAE1. We do not believe that such a requirement would yield

accurate depictions of banks' risk, though it would present significant and disproportionate operational complexity and cost. More fundamentally, concerns about "window dressing" at this stage are speculative: as there is no existing cryptoasset exposure-specific disclosure, any judgment that banks are or could be engaging in "window dressing" is necessarily premature. We recommend instead aligning cryptoasset disclosures with existing Pillar 3 requirements for market risk.

Materiality

The role of materiality in the proposed disclosure requirements does not align with existing principles of appropriate disclosure. Parts of the proposed templates appear to necessitate the disclosure of all cryptoasset exposures, even if they are immaterial for a particular bank. Such extensive disclosure requirements for potentially immaterial aggregate exposures could discourage the testing and adoption of innovative technologies. It is critical that the final disclosure requirements align carefully with the Committee's longstanding policy objectives for banks' disclosures. Further, the proposed introduction of a specific disclosure threshold for "material" cryptoasset exposures is inconsistent with existing disclosure regimes and Basel Framework principles. Typically, materiality tests are instead based around a subjective user test.

If a specific threshold were to be included in order to determine when a bank's overall exposure to cryptoassets is considered material and therefore subject to any disclosure requirements, it would need careful consideration in relation to a bank's total risk-weighted assets. A second-stage test would then be required to determine whether an individual cryptoasset exposure is material and subject to applicable individual disclosures. We would suggest that this is based on a quantitative test, for example 10% of a bank's total exposures to cryptoassets. The threshold contemplated in the Consultation (i.e., a cryptoasset exposure is material if it exceeds 5% of total cryptoasset exposures) inappropriately conflates these two separate assessments. A materiality calculation on this basis would likely include immaterial exposures while potentially excluding subjectively material ones.

Operational risk losses

We do not support the public disclosure of operational risk losses linked to cryptoassets. We support sharing this information with a national supervisor on a confidential basis, when it meets the current supervisory reporting requirements, but we do not think this information should be shared with the public in general, primarily for reasons of operational security. In addition, such disclosure would be inconsistent with the treatment for other financial products and with existing Basel categories for operational risk losses. The lack of precision of this requirement may also lead to different interpretations in different jurisdictions, making the disclosed information inconsistent and unable to be compared.

GENERAL FEEDBACK

Policy rationale

- It is critical that the Committee clearly articulates the specific goals of the proposed disclosure requirements and ensures that they are aligned with the policy objectives of the Committee's Pillar 3 regime. Any final disclosure framework should be carefully calibrated to require only what is necessary to achieve these policy objectives.

- Generally speaking, prudential disclosure requirements are intended to promote market transparency and market discipline. Section 10.1 of DIS states that such requirements "enable market participants to access key information relating to a bank's regulatory capital and risk exposures in order to increase transparency and confidence about a bank's exposure to risk and the overall adequacy of its regulatory capital."[4] According to Principle 3 of DIS, disclosures should be meaningful to users, represent a bank's most significant current and emerging risks, and should not include information that does not add value to users' understanding. In parallel, supervisory reporting requirements enable supervisors to obtain confidential information about regulated entities in order to discharge supervisory or regulatory functions. It is important that any set of disclosure requirements for banks' cryptoasset exposures do not conflate these different aims. We are concerned that the current proposed disclosure framework would see the Pillar 3 framework being used for additional purposes which are more aligned to supervisory oversight and monitoring market developments than providing market discipline and transparency to market participants. Similarly, the Committee should not impose Pillar 3 disclosure requirements for banks' cryptoasset exposures because some market participants, for example credit rating agencies, may find such disclosures useful—commercially or otherwise—as market intelligence on the development of cryptoasset markets. Rather, it is critical that any new disclosure requirements adhere to the underlying, risk-related purpose of Pillar 3 disclosure.[5]

- The original rationale for introducing Pillar 3 included encouraging "market discipline by developing a set of disclosure requirements which will allow market participants to assess key pieces of information on the scope of application, capital, risk exposures, risk assessment processes, and hence the capital adequacy of the institution."[6] If the Committee intends to maintain this objective in the case of banks' cryptoasset exposures, any final disclosure requirements should only include those elements necessary for market participants to impose such discipline and should be closely aligned to traditional notions of materiality. The proposed disclosures, however, would require information to be disclosed at a level of granularity that eschews traditional notions of materiality. These detailed requirements, and the potential additional disclosures included in Annex 2, would require banks to disclose substantially more information than market participants need to understand banks' cryptoasset exposures and related activities and to gauge the associated risks. These types of disclosure would be more appropriate in the context of a national supervisor's confidential request for information, rather than to meet the market discipline-centric objectives of Pillar 3 disclosures.

- Additionally, the Committee should not introduce duplicative disclosure requirements that would add little to, or which may ultimately introduce confusion and result in market participants having a less clear understanding of, banks' cryptoasset-related activities, exposures and risk profiles overall. For example, in addition to the proposed disclosure requirements, banks still would be required to include Group 1a cryptoasset exposures in existing disclosure templates that apply to traditional assets. It is not clear what incremental value market participants would derive from information they receive from existing reporting and they may not appreciate that the same information is duplicated across different disclosures. This duplicative disclosure requirement therefore fails to advance the objectives of Pillar 3 disclosure frameworks, and may even hinder them.

- If the ultimate goal of the proposed disclosures is instead to aid national authorities' oversight of this

[4] See https://www.bis.org/basel_framework/chapter/DIS/10.htm

[5] In the case of credit rating agencies, we note that most will benefit from additional disclosure already via ongoing dialogue with many banks. Typically, this would involve non-disclosure agreements being put in place that allow the credit rating agencies to receive any additional confidential information necessary to conduct a complete rating assessment for a particular bank.

[6] See https://www.bis.org/publ/bcbsca10.pdf

nascent market, the Associations urge the Committee to (a) evaluate carefully what, if any, additional information supervisors require over and above what they already have the power to receive from regulated entities and (b) refrain from requiring banks to provide national authorities with additional information by means of highly granular public disclosures.

- For example, the Associations are aware that supervisors in a number of jurisdictions are already engaging in active supervision of financial institutions' cryptoasset-related activity, and in some jurisdictions receiving granular position data, policy documents, and other relevant information. In the United States, the Federal Reserve has established a Novel Activities Supervision Program "to enhance the supervision of novel activities conducted by banking organizations supervised by the Federal Reserve," including "[c]rypto-asset related activities".[7] Similarly in the United Kingdom, the Prudential Regulation Authority has issued various "Dear CEO" letters that make it clear that regulated financial institutions are expected to incorporate their risk assessment in respect of cryptoassets as part of their normal prudential risk management practices, including disclosures. To the extent that national supervisors generally consider there to be a need for additional information on financial institutions' cryptoasset-related activities and the overall development of these markets, that information should be furnished as part of a separate engagement with industry—which the Associations stand ready to facilitate if necessary—rather than overly extensive public disclosure.

Market development and conflation of Group 1 and Group 2 cryptoassets

- Given the current trajectory of innovation within the financial services sector, it is reasonable to expect that, in the future, as banks move toward greater digitalization, they will incorporate more cryptoassets (including tokenized products) in their business-as-usual offerings. Although the proposed disclosure requirements are being introduced at a point when cryptoasset markets are nascent, it is imperative that any final disclosure regime works at scale when the market is in a more developed future state. For any final disclosure framework for cryptoasset exposures to work at scale, it must provide utility to its intended users that outweighs the attendant costs, avoid undue operational complexity, and properly account for the number and diversity of financial products that fall under the Committee's definition of cryptoasset.

- The general treatment of Group 1 and Group 2 cryptoassets set out across the proposed disclosure table and templates does not account for the key differences in their basic characteristics and respective risk profiles. Based on the proposed table and templates and given the Committee's broad definition of cryptoassets which embraces a range of assets from tokenized traditional assets to unbacked cryptoassets, it is contrary to the basic policy rationale underlying Pillar 3 that all types of cryptoassets would be treated in the same way independently of their inherent risk profile. In addition, the distinction between different types of cryptoassets should be made clear in any final disclosures in order to avoid potential misinterpretation of banks' involvement in cryptoasset markets, especially given the varying risk characteristics across types of cryptoassets.

- It is inappropriate for banks to be required to disclose the detailed level of information proposed for Group 1 cryptoassets. The proposed disclosure framework should be adapted to account for the fact that Group 1a cryptoassets (i.e., tokenized traditional assets) are already subject to stringent Pillar 3 disclosure requirements. In particular, under the current SCO60.130 requirements, and as similarly contemplated by the proposed instructions to Templates CAE1 and CAE2, banks must continue to include tokenized traditional assets (including equities, fixed income, and other instruments) in existing disclosure templates applicable to traditional assets. The disclosure requirements for Group 1a cryptoassets should be consistent with, and not duplicative of, those applicable to their traditional asset counterparts, especially as the Committee has already determined that their risk profiles are equivalent. This would also be consistent with the principle of technology-neutrality. As explained above, duplicative disclosure requirements do not contribute to market participants' ability to exercise market discipline; they therefore deviate from the Committee's intent in promulgating Pillar 3 disclosure standards. The proposed disclosure requirements would result in duplication of disclosure efforts for banks, impose significant associated costs, and require complex system builds which would stifle innovation and delay

[7] See SR 23-7.

adoption of prudently managed cryptoasset-related technologies in return for little incremental benefit. Taking a consistent approach would be helpful in ensuring that disclosures serve their intended purpose (as discussed above) and that the market can understand banks' overall exposures.

- Any final disclosure framework also should balance the level of disclosure with the level of risk-taking in which a bank may engage. For example, Group 2 cryptoassets will have a relatively low impact on a bank's overall risk exposure due to the quantitative limitations the Committee's prudential standard imposes relative to Tier 1 capital. The level of detail requested in the proposed disclosure requirements would, therefore, be out of proportion with the risk, given the total level of relevant activity in which a bank may engage. Given the low level of overall risk a bank may take in relation to Group 2 cryptoassets, the applicability and contents of the relevant disclosures should more closely align to traditional notions of materiality in respect of a bank's overall balance sheet.

- In addition, for Group 2b assets, SCO60.83 specifies that "there is no separate trading book and banking book treatment for Group 2b cryptoassets. The conservative treatment is intended to capture both credit and market risk, including credit valuation adjustment (CVA) risk." The disclosure should therefore not mix risk categories, including in relation to long and short positions, but instead have one single risk category for Group 2b cryptoassets that allows a linkage with OV1 and other B3f tables.

- As further discussed below in the section on Template CAE1, subdividing the disclosure into three separate sub-templates for cryptoasset Groups 1b, 2a and 2b and limiting the disclosure for Group 1a cryptoassets to either Template CAE1 or the existing Pillar 3 non-cryptoasset credit risk templates would address some of these concerns.

RESPONSES TO THE SPECIFIC REQUESTS FOR FEEDBACK

Classification condition assessment detail

- The level of detail contemplated by the Table CAEA disclosure requirements for the classification conditions for Group 1 cryptoassets is not consistent with the disclosure-related goals in the Basel Framework.

- The Group 1 classification condition assessment details, as reflected in row (f) of Table CAEA, require banks to disclose the approach they have used to assess compliance with each of the four Group 1 classification conditions (as noted in SCO60.8-60.19) for each cryptoasset. This would include any public information used but exclude any confidential and proprietary information. We propose instead that a more streamlined disclosure approach is taken which requires more general background on banks' assessment approach to be provided. This would allow market participants to understand how a bank screens cryptoassets in accordance with the Committee's prudential standard, while minimizing the operational complexity introduced by any final disclosure framework. This would also be more aligned with the stated purpose of Table CAEA, which is to "provide an overview of the bank's activities related to cryptoassets…as well as the approach used in assessing the classification conditions."

- For the same reason, we strongly urge the Committee not to incorporate the additional elements contemplated in Annex 2 in respect of each classification condition in any final disclosure framework. In addition to generating undue operational complexity for reporting banks, overly complex or detailed information may have the unintended effect of preventing a variety of stakeholders from receiving an overview of a bank's cryptoasset-related activities, risks, and approaches. Additionally, public documents published by issuers of Group 1 assets, and the networks they operate on, would, in most cases, contain the information in Annex 2, rendering such disclosure here duplicative.

- In addition, it is reasonable to expect that, in the coming years, tokenization will be more widely adopted across the financial services sector, including by banking organizations. It would be impractical to disclose the information at the level of detail proposed for hundreds or thousands of different Group 1a cryptoassets, which also would be inconsistent with the disclosures required in respect of traditional assets. In a future market state where there is more widespread tokenization of traditional assets, the volume of information that would be required by row (f) of Table CAEA for each individual cryptoasset

would be overly burdensome to prepare for banks with a variety of tokenized assets and provide little utility to market participants relative to a more general description of how banks assess the classification conditions across all Group 1 cryptoassets. This also demonstrates the necessity of the principle of materiality being appropriately defined and applicable throughout the disclosure regime.

- Additionally, as per the BCBS's Prudential treatment of cryptoasset exposures[8], "banks are required to notify supervisors of classification decisions and supervisors will have the power to override these decisions if they disagree with a bank's assessment." This means that the classification assessments are already subject to supervisory scrutiny, making the additional transparency required superfluous.

- A more general disclosure with respect to banks' approaches to assessing the classification conditions is also warranted, given the appropriate exclusion of confidential and proprietary information. Banks may rely heavily on confidential or commercially sensitive information when assessing the classification conditions—for example, by including items such as specific provisions included in confidential legal documentation, a bank's approach to auditing smart contracts, and specific aspects of the control framework (e.g., segregation of duties). The Associations strongly agree that such information should not be disclosed publicly. However, detailed disclosures based on only a subset of the information banks use to assess the classification conditions would result in incomplete, confusing, or misleading descriptions of banks' approaches that would be of less utility to users of the proposed disclosures than a more general, broadly applicable description.

- At a minimum, any final disclosure requirement related to banks' approach to assessing the classification conditions for Group 1 cryptoassets should require descriptions by categories of Group 1 cryptoassets, rather than for each individual cryptoasset. As the cryptoasset market grows and develops, the Committee could revisit this approach in an iterative manner if necessary.

Window dressing

- We do not agree that disclosing the amounts in Template CAE1 using daily average values would be an appropriate addition to the proposed disclosure requirements. Such data averaging is unlikely to achieve the stated aim of giving a more accurate picture of risk, and presents significant operational complexity and costs that are not justified.

- We believe the proposed requirement to be disproportionate and unnecessary in addressing a concern relating to a group of assets to which banks have a relatively small exposure and, above all, for which there is no observable evidence of window dressing. As an initial matter, it would therefore be beneficial for the Committee to more clearly articulate the underlying policy objective for a data averaging requirement and, importantly, any evidence of the risk to which the Committee would be responding by requiring such averaging. Prior "window dressing"-related work the Committee has undertaken typically has been responsive to specific risks and behaviors identified over a period of monitoring[9]. Therefore, the inclusion of such a data averaging requirement from the outset of any new cryptoasset exposure-related disclosure regime would necessarily be premature and inconsistent with disclosure requirements in the context of traditional assets. Put differently, the disclosure requirements under consultation would be brand new to the Basel Framework; as a logical consequence, there is no historical evidence of "window dressing" on which to base a data averaging requirement, and any concern about "window dressing" in the proposed disclosures is purely speculative at this time.

- Further, banks have little incentive to make material changes to their activities to artificially reduce period-end reporting of cryptoasset exposures. As the disclosure requirements themselves do not impact the applicability of point-in-time prudential regulations, semiannual point-in-time reporting would not independently create incentives for a bank to manage the amounts disclosed pursuant to the proposed requirements of Template CAE1 in order to reduce its capital requirements. At the same time, "window-dressing" activity would disrupt a bank's related business, impede market functioning, and potentially

[8] See https://www.bis.org/bcbs/publ/d545.pdf.
[9] See previous work considering adjustments to leverage ratio disclosure requirements in the context of window dressing, for example, in relation to securities finance transactions.

harm customers, which creates a strong incentive against managing cryptoasset-related activity around semiannual point-in-time reporting.

- Looking again to the future state of cryptoasset markets, if Group 1 cryptoassets eventually include a large number of discrete tokenized asset classes, it would not be desirable or practicable for a bank to manage its asset class-wide exposure amounts around this disclosure at period-end.

- The strict limits on Group 2 cryptoasset exposures also necessarily make it difficult for any bank to undertake "window dressing" to an extent that would meaningfully impact its semiannual disclosures.

- Such a detailed level of disclosure may also risk revealing strategic positions not intended for the public domain, which could amount to disclosing material non-public information.

- We do not agree that daily average values would provide clarity around banks' cryptoasset exposure-related risk, as insights into risk exposure are better reflected over a longer period.

- Finally, inconsistent disclosure standards for different types of assets introduce compliance-related frictions and disproportionate operational complexity. The disclosure of daily average values would be inconsistent with all other banking book and trading book disclosures. The current proposal would therefore discourage banks from adopting new technologies and developing new products in the cryptoasset market.

- We recommend alignment with existing Pillar 3 disclosure requirements for market risk. For Group 2 cryptoassets, disclosure consistent with existing market risk disclosures would avoid the challenges mentioned above. Group 1 cryptoassets would already be included in existing disclosures. However, if a separate additional disclosure is required, then trading book Group 1 cryptoasset reporting frequency would align with the above. Group 1 banking book disclosures should only be required for the period-end date on a point-in-time basis.

Materiality—overall

- The role of materiality in the Consultation does not align with the existing principles of disclosure.

- The Committee has previously stated, in relation to the role of disclosure more generally, that a "bank should decide which disclosures are relevant for it based on the materiality concept" and that, "[i]nformation would be regarded as material if its omission or misstatement could change or influence the assessment or decision of a user relying on that information for the purpose of making economic decisions."[10] While the document where this discussion is found was subsequently superseded, many jurisdictions continue to assess materiality in this way. For example, it applies in the EU under the Capital Requirements Regulation and in the UK under the PRA's framework.

- Particularly relevantly for the purposes of the Consultation, the notion of materiality is reflected further in current SCO60.129, which contemplates disclosure of information regarding "any *material* Group 1a, Group 1b, Group 2a and Group 2b cryptoasset exposures" (emphasis added).

- Eschewing the appropriate role of materiality in disclosure—and in a significant departure from current SCO60.129—Table CAEA, Template CAE1, Template CAE2, and Template CAE3 would appear, as a preliminary matter, to require certain disclosure related to *all* of a bank's cryptoasset exposures, regardless of their materiality in the aggregate (and in addition to further required disclosure related to material exposures for certain cryptoassets, as we discuss below). Disclosure requirements for cryptoasset exposures that exclude a baseline materiality standard are inconsistent with the overall policy aims of bank disclosure requirements, as they would mandate the detailed disclosure of exposures that may be immaterial for a particular bank. Disclosure requirements that provide users of the disclosures with relatively little insight into the overall risk profile of a bank—especially in relation to the operational complexity involved in producing the required disclosures—would discourage the adoption

[10] Part 3 of the Basel II framework at "E. Materiality: 817." See https://www.bis.org/publ/bcbs128.pdf

of innovative technologies, especially given the de minimis exposures that may stem from early uses of such technologies.

- It is critical that any final disclosure requirements be carefully aligned with the Committee's policy objectives. We do not believe that the disclosure of exposures that are immaterial in the aggregate would aid transparency or market discipline, and therefore recommend that banks only be required to comply with the proposed disclosure requirements if their cryptoasset exposures are material in the aggregate. This is in line with Principle 3 of DIS referenced above, that disclosures "that do not add value to users' understanding or do not communicate useful information should be avoided."[11]

Materiality—specific threshold

- The Consultation suggests the Committee is considering a threshold whereby a specific cryptoasset exposure could be material, and therefore subject to additional, individual disclosure, if it exceeds 5% of the bank's total cryptoasset exposures.

- The setting of a specific, defined materiality threshold as contemplated in the Consultation would be inconsistent with existing disclosure regimes and Basel Framework principles.

- The Committee has previously stated that, "[it] is not setting specific thresholds for disclosure as these can be open to manipulation and are difficult to determine, and it believes that the user test is a useful benchmark for achieving sufficient disclosure."[12] The user test is satisfied when a user of financial information considers an item to be material. As outlined above, while the document where this discussion is found was later superseded, the discussion reflects the way that many jurisdictions assess materiality.

- If a specific, defined materiality threshold were nevertheless included in a final disclosure framework, much more careful consideration would need to be given as to how it should be calculated and the proper calibration of the threshold relative to a bank's total risk-weighted assets, balance sheet or Tier 1 capital. Five percent of a bank's total cryptoasset exposures is not an appropriate threshold to apply; if a bank's cryptoasset exposures were very low overall, 5% of that figure would result in a threshold that would capture exposures that would be extremely immaterial in practice. For example, if a bank had total holdings of $100 in cryptoassets, which could be a residual balance after paying gas fees, using 5% of total cryptoasset exposures as the measure of materiality would mean any holding of $5 in a single cryptoasset would constitute a material cryptoasset exposure, whilst being immaterial relative to the bank's capital base and meaningless from a risk perspective. Additionally, if a bank has large but diverse cryptoasset exposures in the aggregate, such a threshold could mean that some subjectively material exposures would not be separately disclosed if they do not meet the 5% threshold. Materiality provides users with an important view of risk—setting it in terms of total cryptoasset exposures as suggested in the Consultation would divorce the concept of materiality from risk.

- Further, the Committee's final standard for the prudential treatment of cryptoasset exposures contemplates that a bank's total exposure to Group 2 cryptoassets should not generally be higher than 1% of the bank's Tier 1 capital, and it must not exceed 2% of the bank's Tier 1 capital.[13] Given the minimal contributions that Group 2 cryptoassets are permitted to make towards a bank's overall exposure, the inclusion of a specific threshold that is calibrated incorrectly may inappropriately capture exposures that necessarily pose a de minimis risk.

- We therefore suggest the disclosure templates are amended to provide that a bank should decide which disclosures are relevant for it based on the materiality concept in accordance with the Basel Framework and as originally contemplated by SCO60.129. This would include maintaining the use of qualitative judgment towards the definition of material, ensuring that this is consistent with the definition of material according to relevant established and recognized accounting standards such as GAAP or under the

[11] See https://www.bis.org/basel_framework/chapter/DIS/10.htm
[12] Part 3 of the Basel II framework at "E. Materiality: 817."
[13] See SCO60.117.

International Accounting Standards, as set out in IAS 1.

- If a specific, defined materiality threshold were deemed to be necessary notwithstanding the concerns outlined above, the introduction of a two-stage test is suggested, as there should be a consideration of materiality at two levels, which is not addressed in the current proposal. For example:

    1. The first stage would be to assess in an objective way overall the materiality at a macro level of aggregate cryptoasset exposures, relative to a bank's total risk-weighted assets. This could be by way of a specific threshold calculation. If this threshold is passed, the second stage would be assessed.

    2. The second stage would then look at a micro level to whether an individual cryptoasset exposure is material and would be subject to applicable individual disclosure as contemplated in Table CAEA and Template CAE1. We would suggest that this is based on a quantitative test, for example 10% of total exposures to cryptoassets.

ADDITIONAL FEEDBACK

Risk of unintended consequences

- The cryptoasset market is evolving quickly. If disclosure requirements are not calibrated correctly, and result in a required level of detail that is not operationally feasible or commercially viable for reporting banks, it will likely be more difficult for such institutions to engage in cryptoasset-related activity that they could otherwise conduct in a safe and sound manner with positive ultimate impacts for customers and market function.

- While regulation of cryptoasset service providers is beginning to be developed in many jurisdictions, the disclosure and prudential requirements applicable to such firms are in no way comparable to the sophisticated regime that already applies to banks pursuant to the Basel Framework. Making it more difficult for banks to integrate new products and technologies may unintentionally result in *less* transparency for the market overall and ultimately present greater risk for businesses and consumers when dealing with cryptoasset firms that are subject to lighter regulatory and supervisory requirements. In the Associations' view, this would be detrimental to the overall development and health of the market.

- There is also a risk that extensive granular disclosures by banks could result in market participants making inferences that banks are riskier than non-bank competitors, which are not required to disclose the same level of information about their cryptoasset exposures.

Risk of reverse engineering

- The level of detail contemplated by the Consultation's proposed qualitative disclosure requirements could result in the risk of market reverse engineering of banks' actual positions, which would be exacerbated by any reporting of daily average values. Banks do not disclose details on specific positions as this is material non-public information which may lead to the possibility of other market participants specifically trading against banks' positions, and therefore we urge caution around the over-disclosure of exposures, especially where sufficient disclosures are already made.

Custody

- We think the disclosure requirements for the custody of cryptoassets should be consistent with the disclosure requirements that apply under Pillar 3 in relation to the custody of traditional assets.

- The disclosure templates contemplate the disclosure of cryptoassets under custody in several places, including in column (g) in Template CAE1 and row (a) under Table CAEA. However, cryptoassets under custody do not belong to the custodian and therefore do not give rise to credit, market, or liquidity risk for the custodian. Before the finalization of any disclosure framework for banks' cryptoasset exposures, the proposed requirements should be revised so that banks would not be required to provide quantitative

or qualitative disclosures related to the cryptoassets they hold in custody for clients. If such requirements remain, there is a risk that such disclosures of assets held in custody may be misconstrued as reflecting the cryptoasset exposures of the bank, which would not accurately represent the risk profile of the bank and its financial activities.

- Given that the intent of the proposed disclosure requirements is to foster transparency around banks' cryptoasset exposures, it would not be appropriate to require disclosures related to business activities that traditionally do not give rise to exposures, and so column (g) of Template CAE1 should be removed. Disclosure would be appropriate in certain specific circumstances in relation to client assets, for example when a broker is an intermediary clearing the trading activity of a client where the broker becomes obligated for the transaction, or where the bank is financing the trading activity of a client or is otherwise lending against the cryptoassets in the custody account. However, the resulting exposures would be picked up in the other intended quantitative disclosures, where relevant, and do not necessitate a separate column for cryptoassets under custody.

- The obligation to describe trading of cryptoassets on clients' accounts under Table CAEA does not make sense if the financial institution is merely providing custodial services. Cryptoassets held in custody are not an on balance sheet obligation of the bank, and the financial institution is agnostic to the trading activity or the resulting change in value of the cryptoassets being custodied (other than the custody fee which would impact income, but this is in line with traditional custody and does not necessitate special disclosure of cryptoassets under custody). The reference to "trading of cryptoassets on clients' accounts" in Table CAEA should therefore be adjusted so that this is only required to include assets being financed by the bank or which the bank is obligated to clear.

- To the extent that the proposed disclosure requirements for cryptoassets under custody are intended to address the potential operational risk related to cryptoasset custody activities, such operational risk would be adequately disclosed in the narrative accompanying Template CAE1 and the qualitative disclosures of Table CAEA, as adjusted above. Separate disclosures for cryptoassets under custody therefore would not be necessary to achieve such a goal.

- Taking the example of the stablecoin arrangement described in paragraph 60.36 of SCO60[14], it is not clear that the paying institution facilitating the redemption has exposure to the cryptoassets that should be disclosed. The paying institution is merely the conduit of cash from the reserve custodian to the stablecoin holder. Even where the paying institution is also the custodian for the reserve cash, the deposit liability of the financial institution is no different than the deposit liability of any financial institution for highly mobile deposits. If the paying institution is also the custodian for reserve non-cash assets, there is no balance sheet liability for the financial institution, as it merely acts as custodian for non-balance sheet assets. Therefore none of these scenarios should be required to be disclosed.

- If a financial institution is acting as custodian of reserve assets of a stablecoin (again in an arrangement of the type described in paragraph 60.36 of SCO60) where another financial institution is the payments processor, it is not clear whether the reserve custodian would be caught by the proposed disclosure obligations under this new framework. However, similarly we would argue that the reserve asset custodian is operating in a traditional role for traditional assets and does not have novel risk, and would therefore argue against the imposition of any additional disclosure obligations.

- If, notwithstanding the above comments, the suggestion to remove column (g) of Template CAE1 in its entirety is not taken, we would strongly recommend that at least the requirement for the disclosure of Group 1a cryptoassets (i.e. tokenized traditional assets) is removed, for the reasons outlined above (for example, duplication with existing stringent Pillar 3 disclosure requirements for traditional securities, and overly burdensome complexity).

- Ultimately, if the provision of such custodial activities were deemed to result in RWA exposure and required to be disclosed accordingly, then the resulting capital treatment of this would likely drive provision of these custodial activities outside of regulated financial institutions as it would not be viable

[14] See https://www.bis.org/bcbs/publ/d545.pdf.

from a commercial perspective. This would operate to the detriment of the development of the market as well as potentially to end users who may therefore be reliant on such services being provided by less regulated, less secure and less stable providers.

- Granular disclosures around custody also raise operational security concerns. Publicly disclosing information in relation to client assets under custody (even on an aggregate total basis) as a proxy for operational risk from cryptoasset-related activities would not be justified in line with the aims of Pillar 3 and would introduce additional market confusion. There are a number of structures that banks might use to hold cryptoassets for clients (both proprietary and not), including wallets ranging from hot to warm to true, air-gapped, only physically accessible cold. Even within these categories, there are many different varieties and security setups in practice. The operations of any particular bank are therefore likely to be unique, and this results in vastly different operational risk profiles for different banks. As outlined further below in the "Operational risk losses" section, disclosing details of a bank's individual systems, structures and processes and the related security procedures would present both a commercial risk to the bank and, more significantly, give information to bad actors that could be used against the bank to increase both the occurrence, and the likelihood of success, of cyber attacks.

Activities related to cryptoassets

- Table CAEA includes at row (a) a requirement for a description of business activities "related to cryptoassets," including a non-exhaustive list of examples. However, such a broad description lacks sufficient clarity and would appear to potentially require disclosures related to activities that do not give rise to exposures. This would be inconsistent with the stated aim of the Consultation and the overall framework, which is framed in terms of banks' cryptoasset *exposures*.

- We recommend clarifying that, for the purposes of row (a) of Table CAEA, "activities related to cryptoassets" comprise only those activities that give rise to cryptoasset exposures for a bank.

Template CAE1

- In relation to Template CAE1, subdividing the disclosure into three separate sub-templates for cryptoasset Groups 1b, 2a and 2b would be more appropriate. We believe that Group 1a assets should be disclosed either in Template CAE1 or in the existing Pillar 3 non-cryptoasset credit risk templates, but not both. We also consider that the term "Total exposure" should be replaced with "carrying value" and be aligned with other Pillar 3 templates.

- As mentioned previously, a distinction should be made between disclosing Group 1a cryptoassets and other cryptoassets to avoid conflating the risks of traditional tokenized assets with other asset classes. While we do not believe a duplicative separate disclosure of Group 1a cryptoassets is warranted, we recognize that there is interest in seeing disclosure for these assets separately and that there is an expectation that the volume of such transactions will grow in the future. Therefore, we propose that such a disclosure should include Group1a cryptoassets by tokenized instrument type (equity, fixed income, commodity, etc.) and total value at the end of the reporting period. RWAs would already be reported in market risk and the banking book. We would suggest that this is shown in a table separate from Group 2 cryptoassets.

- It would be helpful for the BCBS to provide further guidance on how the cryptoasset-specific Templates, including this one, link to the overall disclosure template. For example, the BCBS could provide additional clarity as to how Template CAE1 links to templates on all RWAs and as to whether the totals in columns (c) and (f) of Template CAE1 would also be included in OV1.

- We also note that current market risk disclosures are not disaggregated into long and short exposures. In order for requirements to be consistent with current disclosures, we suggest that one market risk RWA amount should be presented.

- Exposure limits above 1% and 2% would result in confidential supervisory discussions and remediation plans. Therefore, the proposal that such information is included in this template would likely not be

allowed to be disclosed in practice and should be removed from the proposal. We recommend instead disclosing what the limits are for 1% and 2% only and qualitatively whether a limit had been breached at the reporting period.

Operational risk losses

- Table CAE1 requires financial institutions to disclose the amount of their operational risk losses related to cryptoassets, which are defined as "total amount of operational losses related to cryptoassets net of recoveries and net of excluded losses within the 10-year window or fewer years in accordance with OPE25.10 that is relevant for the Loss Component calculation. Amounts should be reported if the financial institution is required to calculate the Loss Component under the standardised approach to operational risk set out in [OPE25]."

- We do not support the public disclosure of operational risk losses linked to cryptoassets. While we think that this information could be subject to reporting to the supervisor on a confidential basis when it meets the current supervisory reporting requirements, it should not be disclosed to the public in general.

- Our primary concern relates to operational security. If a financial institution faces operational problems in relation to cryptoassets, it would not be wise to publicly disclose these losses from a security perspective, since this would mean identifying potential weaknesses which could encourage other potential hackers and lead to further challenges. See the section on "Custody" above, for an example of the potential impact in the context of disclosures in relation to cryptoassets under custody.

- As the proposed disclosure requirement would only apply to regulated financial institutions, they would be the only institutions disclosing such losses in this manner which may lead the general public to think that financial institutions are less secure overall, which does not reflect the reality of the market when, in practice, the majority of activity is carried out by non-financial institutions who are less likely to have robust security and wider operational resilience frameworks in place and may therefore be subject to a greater degree of risk.

- This requirement is inconsistent with existing disclosure requirements, and it is not clear why this additional inclusion is necessary from a policy perspective. Having to disclose operational risk losses for cryptoassets when equivalent disclosure is not required for other financial products will necessitate the introduction of a bespoke compliance process and systems for this identification, which will result in a disproportionate operational cost for financial institutions which may result in a financial institution being discouraged from adopting this new technology, which does not seem to be justified.

- Such disclosure is also not in line with the principles of DIS. Operational risk is impacted by a wide variety of factors, including: individual organizational structure; the various products and services being offered and their technical implementation; internal systems, processes and controls; and the thoroughness of a bank's risk management practices. The proposed disclosure in relation to operational risk losses for cryptoassets would be very difficult for market users to meaningfully interpret without oversight of these factors, most of which should not be visible to market users. More granular information in relation to operational risk losses will be shared by each bank with its supervisors on a confidential basis where necessary to meet supervisory expectations. This means that supervisors will have this information along with details of the relevant technical implementation, security, risk management, systems and controls and other factors in order to effectively review operational risk, in line with established supervisory processes.

- According to the Basel Standards[15], financial institutions need to disclose their aggregate operational risk loss, which we think is the right level of disclosure, and, therefore, we would ask for the removal of this additional requirement. Also, this disclosure would not be consistent with the existing Basel categories for operational risk losses, which are: internal fraud; external fraud; employment practices and workplace safety; clients, products, and business practices; damages to physical assets; business disruption and

[15] See Template OR1 https://www.bis.org/bcbs/publ/d455.pdf.

system failures; and execution, delivery, and process management.

- The scope of what is an operational loss linked to a cryptoasset is also not clearly defined. This could lead to different interpretations by different jurisdictions and, therefore, very different scopes that would ultimately make the information inconsistent and unable to be compared by stakeholders, particularly in the case of large international banking groups.

Cryptoliabilities

- Templates CAE2 and CAE3 request that information be provided on cryptoliabilities. This concept has the potential to be interpreted differently by financial institutions without clear guidance as to what "cryptoliabilities" comprise. We request that the Committee include a definition for cryptoliabilities and/or clear guidance on what should be disclosed in respect of cryptoliabilities in order to ensure consistency in disclosure practices and comparability of bank disclosures.

Template CAE3

- We would welcome further guidance on the required exposure amount value for disclosures to avoid inconsistency between disclosure templates and their interpretation across the industry. For example, should accounting value or market value be used?

- For derivative disclosures, it would also be helpful to clarify whether financial institutions should report gross net present value or netted against collateral. If the latter, guidance will be required on how to present netted exposures as these may be part of broader portfolios with non-crypto derivatives.

- Guidance will also be required for financial institutions to understand how to calculate derivative contingent outflows such as HLBA relating to cryptoassets. Cryptoasset liquidity risk cannot be easily ringfenced and assumptions will be required to be made in this regard.

Paragraph 60.2 of SCO60

- In order to fulfill disclosure obligations under the new framework, it is critical that it is clear what is within and outside of the scope of such disclosure obligations. To this end, paragraph 60.2 of SCO60 would benefit from clarification.

- The section currently reads:

  "Dematerialised securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through DLT or similar technologies are considered to be within the scope of this chapter and are referred to as tokenised traditional assets, whereas those dematerialised securities that use electronic versions of traditional registers and databases which are centrally administered are not within scope."

- In our view, the scope should also explicitly exclude dematerialized securities issued through DLT that are "electronic versions of traditional registers and databases which are centrally administered." As currently drafted, if any registrar, including central securities depositories, were to switch to a DLT-based books and records system to record issuance of traditional securities, then such traditional securities[16] would also become subject to this requirement, which we do not think is intended or warranted.

[16] Such adoption is being actively explored or implemented by many central securities depositories. See, e.g., Euroclear launches DLT solution, Euroclear, October 24, 2023. Available at https://www.euroclear.com/newsandinsights/en/press/2023/2023-mr-14-euroclear-launches-dlt-solution.html; DTCC's Project Ion Platform now Live in Parallel Production Environment, Processing Over 100,000 Transactions per Day on DLT, DTCC, August 22, 2022. Available at: https://www.dtcc.com/news/2022/august/22/project-ion; HKEX Launches Synapse, A Settlement Acceleration Platform for Stock Connect, HKEX, October 4, 2023. Available at: https://www.hkex.com.hk/News/News-Release/2023/231004news?sc_lang=en; Blockchain/distributed ledger technology, A game changer for the financial markets, Deutsche Boerse, retrieved January 12, 2024. Available at: https://www.deutsche-boerse.com/dbg-en/our-company/deutsche-boerse-group/business-areas/blockchain-business-areas.

Implementation timeline

- The legislative / rulemaking agenda in various jurisdictions is currently under unusual amounts of stress, which is likely to lead to delayed implementation of the cryptoasset prudential framework in some major jurisdictions. This would result in misaligned implementation dates and a lack of consistency in applicable standards which would have a disproportionate impact on entities operating on a global basis.

- As such, we propose extending the effective date from 1 January 2025 to 1 January 2026, so as to allow member jurisdictions sufficient time to implement the Committee's standards within a consistent time frame globally.

Conclusion

We urge the Committee to reconsider its proposal in line with our feedback with a view to creating a well-balanced disclosure framework that is consistent with (and not duplicative of) existing disclosure requirements where relevant, and that takes into account the unique characteristics and risks of different cryptoassets, the evolving nature of the market, and operational realities.

Ultimately, we advocate for a disclosure framework that is practical, efficient, and effective in promoting market transparency and discipline without stifling innovation or imposing unnecessary complexity.

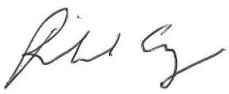
* * *

The Associations appreciate your consideration of our comments and proposals and remain at your disposal to discuss any of these views in greater detail.

Respectfully submitted,

Allison Parent
Executive Director
Global Financial Markets Association

Gabriel Callsen
Senior Director
FinTech and Digitalization
International Capital Market Association



Richard Gray
Director, Regulatory Affairs
Institute of International Finance

Panayiotis Dionysopoulos
Head of Capital
International Swaps and Derivatives Association

Appendix
Overview of the Associations

The **Global Financial Markets Association** ("GFMA") represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. GFMA brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe ("AFME") in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association ("ASIFMA") in Hong Kong and the Securities Industry and Financial Markets Association ("SIFMA") in New York and Washington are, respectively, the European, Asian and North American members of GFMA.

The **International Capital Market Association** ("ICMA") promotes well-functioning cross-border capital markets, which are essential to fund sustainable economic growth. It is a not-for-profit membership association with offices in Zurich, London, Paris, Brussels, and Hong Kong, serving over 610 members in 67 jurisdictions globally. Its members include private and public sector issuers, banks and securities dealers, asset and fund managers, insurance companies, law firms, capital market infrastructure providers and central banks. ICMA provides industry-driven standards and recommendations, prioritising three core fixed income market areas: primary, secondary and repo and collateral, with cross-cutting themes of sustainable finance and FinTech and digitalisation. ICMA works with regulatory and governmental authorities, helping to ensure that financial regulation supports stable and efficient capital markets. www.icmagroup.org

The **Institute of International Finance** is a global association of the financial industry, with around 400 members over 60 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks.

Since 1985, the **International Swaps and Derivatives Association** ("ISDA") has worked to make the global derivatives markets safer and more efficient. Today, ISDA has over 1,000 member institutions from 79 countries. These members comprise a broad range of derivatives market participants, including corporations, investment managers, government and supranational entities, insurance companies, energy and commodities firms and international and regional banks. In addition to market participants, members also include key components of the derivatives market infrastructure, such as exchanges, intermediaries, clearing houses and repositories, as well as law firms, accounting firms and other service providers. Information about ISDA and its activities is available on ISDA's website: www.isda.org.