Basel Committee Finalizes Prudential Standard for Cryptoasset Exposures

In December 2022, the Basel Committee on Banking Supervision ("BCBS") finalized its prudential standard for cryptoasset exposures (the "Final Standard"). In June 2022, the BCBS had issued its second consultative document (the "Second Consultation") on a prudential framework for cryptoasset exposures (see our prior analysis here). The structure of the Final Standard remains unchanged from the Second Consultation and outlines classifications of different cryptoassets and minimum capital requirements based on various risks.

The BCBS expects regulators to implement the Final Standard by January 1, 2025 (the "implementation date"). Banks must inform their supervisor of their classification decisions for any cryptoasset exposures by the implementation date. The Final Standard encourages submission of the information well in advance, but if that is not possible and the information must be sent following the deadline, the bank must provide their supervisor with sufficient time to review and override the decision, if necessary, prior to publication of the bank's first set of Pillar 3 disclosures after the implementation date. The BCBS also expects to closely monitor the effects of the Final Standard and issue additional refinements and clarifications over time; the Final Standard identifies specific topics that will be subject to further monitoring and review: (*e.g.*, permissionless blockchains).

KEY TAKEAWAYS

- While current banks' exposures to cryptoassets are relatively low, the Final Standard may operate to shape aspects of the cryptoasset ecosystem in the coming years. For example, stablecoins may be designed to qualify for a less punitive capital treatment provided in the Final Standard, in order to encourage banks to hold or otherwise interact with such stablecoins. Similarly, banks likely will review any tokenized deposit arrangement to ensure the Final Standard permits them to be treated as traditional deposits.
- The Final Standard continues to take a conservative approach to banks' involvement in cryptoasset activities, although it exhibits some more flexibility relative to the Second Consultation. For example, the Final Standard generally retains the Second Consultation's limit on "Group 2" assets (those considered to be the riskier group of cryptoassets compared to "Group 1", as discussed below) to 1% of Tier 1 capital. The final requirement, however, measures exposures at the higher of gross long and gross short positions and does not require regulators to impose the consultation's fixed add-on to risk-weighted assets ("RWAs") for Group 1 exposures to account for infrastructure risk.
- Nonetheless, it remains unclear whether the Final Standard, as implemented by the various regulators, would allow banks to engage in such activities at scale or calibrate the prudential treatment so that cryptoasset activities may come within the prudential regulatory perimeter.
- The Final Standard clarifies that the BCBS did not intend the Second Consultation to have applied credit, market and liquidity risk requirements to custodial services involving the safekeeping or administration of client

cryptoassets on a segregated basis, and was revised to specify which elements are applicable to such services, such as the operational risk requirements and the risk management and supervisory review sections. Thus, the Final Standard appears to indicate that, unlike the Securities and Exchange Commission's Staff Accounting Bulletin 121, it would not effectively treat cryptoassets held in custody as balance sheet assets.

CHANGES FROM THE SECOND CONSULTATION

The Final Standard responded to some of the comments the BCBS received from the Second Consultation. The BCBS's changes include:

- Replacing the infrastructure risk "add-on" requirement for Group 1 cryptoassets, which was proposed as a fixed add-on to RWAs set at 2.5% of exposure value, with a more flexible approach that provides regulators the option to impose an infrastructure risk add-on based on any observed weaknesses in cryptoasset infrastructure.
- Declining to implement a basis risk test, a quantitative test based on the market value of the cryptoasset, for stablecoins to qualify for the Group 1 classification; however, there is a requirement for stablecoin issuers to be supervised and regulated by a supervisory authority that applies prudential capital and liquidity requirements. Given that the President's Working Group on Financial Markets in the United States has advocated for stablecoin issuers to be prudentially regulated at the federal level, it is unclear how the U.S. banking agencies will interpret this requirement.
- Modifying the 1% Group 2 exposure limit to measure exposures as the higher of the gross long and gross short position in each cryptoasset (rather than the aggregate of the absolute values of long and short exposures) and to limit the consequences of breaching the limit for Group 2b capital treatment to only the amount that is exceeded; however, if the exposure exceeds a threshold of 2% of Tier 1 capital, the whole of Group 2 exposures will be subject to the Group 2b capital treatment.
- Removing the supervisory pre-approval requirement for banks' classification decisions; however, banks are required to notify supervisors, and supervisors will have the power to override banks' classification decisions.

CATEGORIES OF CRYPTOASSETS

The Final Standard applies to "cryptoassets", which are "private digital assets that depend primarily on cryptography and distributed ledger technologies (DLT) or similar technologies". Dematerialized securities using electronic versions of traditional registers and databases that are centrally administered are not within scope of the Final Standard. Central bank digital currencies also are excluded from the scope of the Final Standard.

The Final Standard categorizes cryptoassets into two groups, each with two subgroups. Group 1 consists of cryptoassets that pass the Group 1 classification conditions. This group is subdivided into:

- Group 1a: Tokenized traditional assets (*i.e.*, tokenized versions of assets that are captured within the Basel Framework and not classified as cryptoassets) that meet the Group 1 classification conditions.[1]
- Group 1b: Cryptoassets with stabilization mechanisms (aka "stablecoins") that are effective at all times that meet the Group 1 classification conditions.

Group 2 consists of cryptoassets that do not meet the classification conditions. This group is subdivided into:

- Group 2a: Cryptoassets that pass Group 2a hedging recognition criteria.
- Group 2b: All other cryptoassets.

GROUP 1 CLASSIFICATION CONDITIONS

The Final Standard outlines four classification conditions required to be considered a Group 1 cryptoasset.

Condition 1

The first condition would require the cryptoasset to be either a tokenized traditional asset or have an effective stabilization mechanism. For a tokenized traditional asset to meet this classification condition, it must:

- Be a digital representation of a traditional asset using cryptography, DLT or similar technology.
- Pose the same level of credit and market risk as the traditional form of the asset. This means that the cryptoasset would need to confer the same level of legal rights as the traditional form of the asset.[2]

To meet the first classification condition, a cryptoasset with an effective stabilization mechanism must:

- Be designed to be redeemable for a predefined amount of reference assets (the "peg value").
- Have a stabilization mechanism designed to minimize fluctuations in value relative to the peg value.
- Have a stabilization mechanism that allows for risk management similar to that of traditional assets. (Evidence must be provided to satisfy supervisors of the effectiveness of the stabilization mechanism, including composition, valuation and frequency of valuation of the reserve assets and the quality of available data.)
- Have significant information for banks to verify the ownership rights of the reserve assets behind the cryptoasset.
- Have an issuer that is supervised and regulated by a supervisor that applies prudential capital and liquidity requirements to the issuer.
- Not be an algorithmic stablecoin or reference other cryptoassets as underlying assets.
- Meet the "redemption risk" test. This test is to ensure that the reserve assets are sufficient to enable redemption at par at all times, including during extreme stress. To pass the redemption risk test, the bank must ensure that the cryptoasset arrangement meets the following conditions:
    - The value of reserve assets at all times (including during extreme stress) must equal or exceed the aggregate peg value. If the reserve assets expose the holder to risks other than those arising from the reference assets (*e.g.*, credit, market and liquidity risks arising from the reference assets being USD whereas the reserve assets are USD-denominated bonds), the reserve assets should be sufficiently overcollateralized to ensure that their value would exceed the aggregate peg value after stress losses.
    - For cryptoassets that are pegged to one or more currencies, the reserve assets must be comprised of assets with minimal market and credit risk. The assets must be capable of being liquidated rapidly with minimal adverse price effect. Further, reserve assets generally must be denominated in the same currency or currencies in the same ratios as the currencies used for the peg value.[3]
    - The governance and management of reserve assets must be comprehensive and transparent and must ensure, among other things, that a robust operational resilience framework exists, that the value of the reserve assets are disclosed at least daily and that their composition is disclosed at least weekly. In addition, there should be an explicit legally enforceable objective of ensuring that all cryptoassets can be redeemed promptly at the peg value, including under periods of extreme stress, and the reserve assets should be subject to an independent external audit at least annually to confirm they match the disclosed reserves and are consistent with the mandate.

Condition 2

The second classification condition requires that all rights, obligations and interests arising from the cryptoasset are clearly defined and legally enforceable in all the jurisdictions in which it is issued and redeemed. In addition, the legal framework should ensure settlement finality. This classification condition requires that:

- Cryptoasset arrangements would need to include full transferability and settlement finality. Cryptoassets that have stabilization mechanisms must provide a robust legal claim against the issuer and / or underlying reserve assets and must be redeemable within five calendar days of a request.
- Unless the offering of the cryptoasset has been approved by the relevant regulator, banks are required to receive an independent legal opinion confirming that arrangements (*e.g.*, redemption obligations for stablecoins) are properly documented.

Condition 3

The third classification condition focuses on ensuring that the network on which the cryptoassets operate is designed to mitigate and manage material risks. This condition would be satisfied when functions of the cryptoasset network, such as issuance, redemption, validation and transfer, and the network itself do not pose any material risks to implementation of those functions. Companies should have governance and risk management policies in place to address credit, market, operational, liquidity, data security and anti-money laundering risks. Networks that fulfill this condition have well-defined key elements, which include operational structure, degree of access, technical role of nodes and validation mechanisms.

Condition 4

The fourth classification condition requires that entities that execute redemptions, transfers, storage or settlement, or entities that manage and invest in reserve assets, must (i) be regulated and supervised or subject to appropriate risk management standards; and (ii) have in place and disclose a comprehensive governance framework. Entities subject to this condition include operators of transfer and settlement systems, wallet providers and, for cryptoassets with stabilization mechanisms, administrators of the stabilization mechanism and custodians of reserve assets.

RESPONSIBILITIES FOR DETERMINING AND MONITORING COMPLIANCE WITH THE CLASSIFICATION CONDITIONS

Banks are responsible on an ongoing basis for assessments to determine whether the cryptoassets to which they are exposed are in compliance with the classification conditions and the hedging recognition criteria. Banks must fully document the information used in determining compliance with the classification conditions and make this available to supervisory authorities on request. Supervisors are responsible for reviewing and assessing banks' analysis and risk management and measurement approaches and reviewing banks' classification decisions. Supervisory authorities must have the power to override banks' classification decisions if they do not agree with the assessments undertaken by banks. The override should be exercised in a consistent way across banks. To ensure consistent application across jurisdictions, authorities are expected to routinely compare and share their supervisory information on banks' assessments of cryptoassets against the classification conditions.

MINIMUM CAPITAL REQUIREMENTS FOR CREDIT RISK FOR GROUP 1 CRYPTOASSETS

For Group 1a cryptoassets:

- Generally, tokenized assets are subject to the same credit RWA as the non-tokenized, traditional form of the asset (assuming the former confers the same level of legal rights and likelihood of on-time payment as the latter).
- The Final Standard notes, however, that there are areas of credit standards that try to capture risk that are not associated with legal rights. Banks should assess those risks too and not simply assume a given course of treatment because of the treatment of the traditional asset.

For Group 1b cryptoassets:

Banks with banking book exposures to Group 1b cryptoassets are required to analyze their structure and identify all risks that could result in a loss. Each credit risk should then be separately capitalized. Risks for Group 1b cryptoassets can arise from the following (though the Final Standard notes that the list is not exhaustive):

- Risk from reference asset:
  - Banks should apply the credit RWA that would apply to the underlying asset. If the asset gives rise to a foreign exchange or commodity risk, banks should apply the market RWA that would apply to a direct holding of such an asset.
  - If the underlying asset is a pool of assets, banks should apply the requirements applicable to equity investments in funds.
- Risk of default of the redeemer:
  - If the bank has a claim on the redeemer of the stablecoin, the bank is required to calculate a credit RWA equal to the credit RWA that would apply for a direct loan (with the amount equaling the amount of the redemption claim) to the redeemer. Whether the calculation will be based on a secured or unsecured loan will depend on whether the claim on the redeemer is secured or unsecured.

- Banks are not required to calculate this credit RWA if (1) the underlying, reserve assets are held in a bankruptcy remote special purpose vehicle on behalf of the cryptoasset holders, who have direct claims to the underlying reserve assets; and (2) the bank has received an independent legal opinion affirming that relevant courts would recognize such an arrangement.

- Risks arising when intermediaries perform the redemption function:
  - The Final Standard provides additional requirements for stablecoin arrangements in which only a subset of holders ("members") are permitted to redeem cryptoassets directly from the redeemer.
  - Where a bank is a member and has committed to buy cryptoassets from non-member holders, the bank needs to include the RWAs of the cryptoassets (1) it is legally obligated to purchase; and (2) it would nonetheless be obligated to purchase in order to satisfy expectations and protect the bank's reputation (if the bank or its supervisor determines such step-in risk exists).
  - When members have committed to buy cryptoassets in unlimited amounts and a bank is a non-member holder, the bank is required to sum the risk of the changing value or potential default of the reserve asset and the risk that all members default. When members have not committed to buy in unlimited amounts, the non-member bank is required to sum such risks and the risk that the redeemer defaults.

MINIMUM CAPITAL REQUIREMENTS FOR MARKET RISK FOR GROUP 1 CRYPTOASSETS

The Final Standard provides additional detail regarding how banks should apply the simplified standardized approach (the "SSA"), the standardized approach (the "SA") and the internal models approach (the "IMA") for calculating minimum risk-based capital requirements for market risk. Examples of this additional detail include:

- For the SSA, all instruments including derivatives and off-balance sheet positions that are affected by changes in Group 1 cryptoassets should be included, and netting and hedging are recognized between Group 1a / b cryptoassets and the traditional assets they represent / reference. If present in a Group 1b cryptoasset, the risk of default of the redeemer and the risks arising when intermediaries perform the redemption function should be treated in line with the minimum risk-based capital requirements for credit risk.
- For the SA, the Final Standard requires that the cryptoassets be mapped to the current risk classes under the sensitivities-based approach wherein the cryptoasset is decomposed into the traditional asset(s) the cryptoasset represents/references. The default risk capital ("DRC") requirements should be equivalent to those of the traditional asset, and banks should use the same approach for redeemer default risk as they did in the credit risk section.
- For the IMA, the non-DRC allows mapping of exposures similar to that for the SA (discussed above). Banks are not permitted to use IMA for instruments referencing Group 2 assets.

INFRASTRUCTURE RISK ADD-ON FOR GROUP 1 CRYPTOASSETS

In the Final Standard, authorities must have the power to apply an add-on for infrastructure risk since many of the technologies, such as DLT, that underly cryptoassets are new. The add-on will initially be set as zero but will be increased by authorities based on any observed weakness in the infrastructure used by Group 1 cryptoassets.

GROUP 2a HEDGING RECOGNITION CRITERIA

A Group 2a cryptoasset can be a:

- Direct holding of a spot Group 2 cryptoasset where there exists a derivative or exchange-traded fund ("ETF") or exchange-traded note ("ETN") that is traded on a regulated exchange that solely references the cryptoasset.
- Derivative or ETF/ETN that references a Group 2 cryptoasset, where the derivative or ETF/ETN has been explicitly approved by a jurisdiction's markets regulators for trading or the derivative is cleared by a qualifying central counterparty.
- Derivative or ETF/ETN that references a derivative or ETF/ETN that meets criterion in the bullet immediately above.

- Derivative or ETF/ETN that references a cryptoasset-related reference rate published by a regulated exchange.

A Group 2a cryptoasset is required to:

- Be highly liquid (meaning that, over the previous year, the average market capitalization was at least USD $10 billion and the 10% trimmed mean of daily trading volume with major fiat currencies was at least USD $50 million); and
- Have sufficient data associated with it (meaning at least 100 price observations over the previous year and there are sufficient data on trading volumes and market capitalization).

MINIMUM CAPITAL REQUIREMENTS FOR CREDIT AND MARKET RISK FOR GROUP 2 CRYPTOASSETS

For Group 2a cryptoassets (*i.e.*, cryptoassets that pass the Group 2a hedging recognition criteria described above), the capital requirements should be calculated by a modified version of the SSA or the SA. This treatment permits some recognition of hedging.[4]

For cryptoassets in Group 2b, there is not a separate trading book and banking book treatment. The more conservative approach is designed to capture both credit and market risk. For each Group 2b asset, banks would be required to apply an RWA of 1,250% to the greater of the absolute value of the aggregate long and short positions.

CAPITAL REQUIREMENTS FOR CREDIT VALUATION ADJUSTMENT ("CVA")

Derivatives and securities financing transactions ("SFTs") on Group 1a cryptoassets generally are subject to the same treatment for CVA as the non-tokenized version of the assets. Banks must still assess the tokenized asset because qualification for a given treatment does not always follow that of the non-tokenized asset. For example, the Final Standard states that the standardized approach ("SA-CVA") may not be applied to Group 1a cryptoassets in certain cases where sufficient data is not available to model different liquidity characteristics between the traditional asset and the cryptoasset.

Derivatives on Group 1b cryptoassets are subject to the same capital requirements for CVA as the non-tokenized assets.

Derivatives and SFTs on Group 2a cryptoassets are only subject to the basic approach ("BA-CVA"). The SA-CVA is not available for derivatives and SFTs referencing Group 2a cryptoassets.

See above for the capital treatment of Group 2b cryptoassets.

MINIMUM CAPITAL REQUIREMENTS FOR COUNTERPARTY CREDIT RISK ("CCR")

Groups 1a and 1b generally would be subject to the same CCR rules as the non-tokenized asset; this includes the internal models method ("IMM"). However, for Group 1a, problems with data availability may require application of the standardized approach ("SA-CCR").

Group 2a cryptoassets follow a modified SA-CCR, which includes a new asset class "crypto". There are separate hedging sets for each "crypto currency" priced in applicable fiat currencies or in another Group 2a "crypto currency".

Group 2b cryptoassets calculate the exposure for CCR as the sum of the replacement cost and the potential future exposure ("PFE") multiplied by an alpha factor, where the PFE is calculated as 50% of the gross notional amount. Netting is permitted only between exposures of the same Group 2b cryptoassets; netting sets containing derivatives related to Group 2b assets and other assets are split into two (separating Group 2b assets from other assets).

For SFTs, banks must apply the comprehensive approach formula set out in the credit risk mitigation section of the standardized approach to credit risk. Only Group 1a cryptoassets that are tokenized versions of the instruments included on the list of eligible financial collateral may qualify for recognition as eligible collateral. Group 1b, Group 2a and Group 2b cryptoassets are not eligible forms of collateral in the comprehensive approach and, therefore, when banks receive them as collateral, they will receive no recognition for the purpose of the net exposure calculation to the counterparty.

MINIMUM CAPITAL REQUIREMENTS FOR OPERATIONAL RISK

The operational risk resulting from cryptoasset activities should generally be captured in the operational risk standardized approach through the

business indicator (which should include income and expenses resulting from activities relating to cryptoassets and through the internal loss multiplier (which should include operational losses resulting from cryptoasset activities). To the extent that operational risks are not sufficiently captured in minimum capital requirements, banks and supervisors also should take appropriate steps to ensure capital adequacy and sufficient resilience in the context of the supervisory review process.

MINIMUM LIQUIDITY RISK REQUIREMENTS

Generally, the calculation of the LCR and the NSFR would follow treatments when calculating exposures of similar risks.

Group 1a cryptoassets that are tokenized versions of high-quality liquid assets ("HQLA") can be considered HQLA, but only if they separately satisfy the characteristics of HQLA. In contrast, Group 1b and Group 2 cryptoassets may not be considered HQLA.

Specific parameters for LCR and NSFR treatment are outlined below, depending on the scenario.

- Tokenized claims on a bank: Group 1a tokenized claims on banks are treated as unsecured funding instruments when they are issued by a regulated and supervised bank, represent a legally binding claim on a bank, are redeemable at par value in fiat currency and have a stable value. The Final Standard provides a number of additional considerations, including:
  - The maturity is based upon contractual redemption rights available to the holder.
  - For liabilities from own-issued tokenized claims on a bank, the LCR outflow rates and NSFR available stable funding factors are based on the earliest date the liability could be redeemed, and the associated liabilities are not treated as stable retail deposits.
  - If a bank holds another bank's tokenized liability, the holder would not recognize inflows in the LCR if the liability is not redeemable in 30 days or if it is held for operational purposes.
- Stablecoins: Group 1b assets (as well as Group 2 stablecoins that would be Group 1b assets but for the redemption restriction) would be treated similar to securities, subject to a number of considerations, including:
  - If the bank is the issuer and stablecoin represents legally binding claims on the bank, the bank should recognize 100% outflows in the LCR if the stablecoin is redeemable within 30 days.
  - If the bank holds a stablecoin on its balance sheet, it would generally be subject to an 85% required stable funding ("RSF") factor in the NSFR and not result in LCR inflows. Exceptions exist to the extent that the stablecoin has a final contractual maturity and the maturity would result in an inflow of fiat currency within the relevant time horizon.
- Other cryptoassets: These should generally follow the treatment of other non-HQLA, subject to a number of considerations, including:
  - A bank that holds other cryptoassets or loans denominated in these assets on its balance sheet must assign 100% RSF to the carrying value of these assets in the NSFR and must not recognize any inflows associated with the liquidation, redemption or maturity of these assets.
  - A bank that has borrowed other cryptoassets on an unsecured basis and has an obligation to return these assets within 30 days must apply a 100% outflow rate against the market value of the asset that would be returned to the bank's customer or counterparty (unless the obligation can be settled with certainty from the bank's own unencumbered inventory of the same asset).

LARGE EXPOSURE REQUIREMENTS

Cryptoassets will be subject to the BCBS's large exposure rule and will follow the same principles as other exposures. Cryptoasset exposures that give rise to a credit risk exposure would be included in the large exposure measure according to their accounting value, as set out in the large exposure standards.

GROUP 2 EXPOSURE LIMIT

The Final Standards would establish two limits on a bank's exposure to Group 2 cryptoassets. A bank's aggregate exposure from direct and indirect holdings

of Group 2 assets "should not generally be higher" than 1% of the bank's tier 1 capital and must not exceed 2% of the bank's tier 1 capital. Breaches of the 1% threshold should not generally occur, and any bank exposure in excess of the threshold will be subject to capital requirements that apply to Group 2b cryptoasset exposures. If the 2% threshold is breached, all Group 2 cryptoasset exposures will be subject to the capital requirements that apply to Group 2b cryptoasset exposures.

Exposures include direct (cash and derivatives) and indirect holdings (*i.e.*, those via investment funds, ETFs / ETNs or any legal arrangements designed to provide exposures to cryptoassets). Exposures to all Group 2 cryptoassets must be measured using the higher of the absolute value of the long and short exposures in each separate cryptoasset to which the bank is exposed (*i.e.*, the same methodology that applies for determining the Group 2b capital treatment).

The Final Standard states that the BCBS intends to review the Group 2 exposure limit in the future and may increase or eliminate it.

BANK RISK MANAGEMENT AND SUPERVISORY REVIEW

Banks with direct or indirect exposures or that provide related services to cryptoassets must establish policies and procedures to identify, assess and mitigate the risks (including operational risks, credit risks, liquidity risks including funding concentration risk and market risks). Banks must conduct ex-ante assessments of any cryptoasset exposures, and particular attention must be paid to the assessment of the effectiveness of any hedging techniques. Banks must inform their supervisory authorities of their policies and procedures, assessment results, actual and planned cryptoasset exposures and activities in a timely manner.

The Final Standard provides a non-exclusive list of risks associated with cryptoassets that banks should consider:

- Cryptoasset technology risks: Banks should consider the stability of the network and DLT, the design of the DLT, service accessibility and the trustworthiness of node operators.
- IT and cybersecurity risks: Banks should be aware that cryptoassets bring new IT and cybersecurity risks. These include cryptographic key theft, distributed denial of service attacks and compromised login credentials.
- Legal risks: The novelty and fast evolution of cryptoassets bring unique legal risks. Banks should be aware of accounting standards, control and ownership rules, disclosure requirements and bans associated with cryptoassets.
- Money laundering and financing terrorism risks: Banks should continue to apply risk-based anti-money laundering and countering financing terrorism practices for cryptoassets.
- Valuation risks: Cryptoassets are volatile and have variable prices on different exchanges. This can cause banks to face losses due to mispricing from operational deficiencies.

The Final Standard states that supervisory evaluation of cryptoasset activities is "particularly relevant" because the activities and related risks are new and evolving. Supervisors are expected to exercise their authority to require banks to address any deficiencies identified and may recommend that banks perform stress testing or scenario analysis to assess cryptoasset-related risks. Supervisory actions also could include additional capital charges, provisioning for losses related to cryptoassets or mitigations measures such as internal limits.

DISCLOSURE REQUIREMENTS

Banks should disclose their business activities related to cryptoassets and how those activities impact the risk profile of the bank, risk management policies for cryptoasset exposures, scope and main content of the bank's reporting for cryptoassets and significant and emerging risks for cryptoassets as well as how those risks would be managed. Banks should disclose any material exposure to Group 1a, 1b, 2a and 2b cryptoassets on a regular basis. This disclosure should include direct and indirect exposure amounts, capital requirements and accounting procedures.

1 Dematerialized securities (securities that have been moved from physical certificates to electronic book-keeping) that are issued through DLT or similar technologies are referred to as tokenized traditional assets in the Final Standard.

2 For bonds, loans, claims on banks, equities and derivatives, this also means that there must not be any feature of the cryptoasset that could prevent obligations to the bank from being paid in full when due as compared with the traditional version of the asset.

3 A *de minimis portion* may be held in other currency, provided that the holding of such currency is necessary for the operation of the cryptoasset arrangement and all currency mismatch risk between the reserve assets and peg value has been appropriately hedged.

4 This treatment is not further described herein because its complexity is not consistent with the summary nature of this document.

NEW YORK

David L. Portilla
+1-212-474-1410
dportilla@cravath.com

WASHINGTON, D.C.

Will C. Giles
+1-202-869-7728
wgiles@cravath.com

CRAVATH, SWAINE & MOORE LLP

NEW YORK

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

LONDON

CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

WASHINGTON, D.C.

1601 K Street NW
Washington, D.C. 20006-1682
+1-202-869-7700

cravath.com