Dino Kos
Chief Regulatory Officer
dkos@cls-bank.com

20 November 2017

Via email

CPMI Secretariat
Bank for International Settlements
CH-4002 Basel
Switzerland
Email: cpmi@bis.org

Re: Discussion note – Reducing the risk of wholesale payments fraud related to endpoint security – consultative document

Dear Sirs/Mesdames:

CLS Bank International ("CLS") welcomes the opportunity to comment on the Committee on Payments and Market Infrastructures ("CPMI") consultative document, *Discussion note: Reducing the risk of wholesale payments fraud related to endpoint security*, published on 28 September 2017 (the "Discussion Note").[1]

CLS was established by the private sector, in cooperation with a number of central banks, to mitigate the settlement risk (loss or principal) associated with the settlement of payments relating to foreign exchange transactions. CLS operates the world's largest multicurrency cash settlement system (the "CLS system") and provides payment-versus-payment ("PvP") settlement in 18 currencies directly to 67 members, some of which provide access to the CLS system for over 24,000 third-party institutions.

As an Edge Act corporation under Section 25A of the United States Federal Reserve Act, CLS is regulated and supervised by the Board of Governors of the Federal Reserve System and the Federal Reserve Bank of New York (collectively, the "Federal Reserve"). Additionally, the central banks whose currencies are settled in the CLS system have established the CLS Oversight Committee, organized and administered by the Federal Reserve pursuant to the *Protocol for the Cooperative Oversight Arrangement of CLS,*[2] as a mechanism to carry out the central banks' individual responsibilities to promote safety, efficiency, and stability in the local markets and payments systems in which CLS participates. As a systemically important financial market infrastructure ("FMI"), CLS is subject to the *Principles for financial market infrastructures* (the "PFMI"), as applicable to payment systems.[3] As a designated systemically

[1] http://www.bis.org/cpmi/publ/d170.pdf.

[2] https://www.federalreserve.gov/paymentsystems/cls_protocol.htm.

[3] http://www.bis.org/cpmi/publ/d101a.pdf.

important financial market utility (for which the Board of Governors of the Federal Reserve System is the "Supervisory Agency"), CLS is also subject to the risk management standards set forth in Regulation HH.

The strategy set forth in the Discussion Note (the "Proposed Strategy") would apply to CLS directly, as the operator of the CLS system, as well as indirectly, as a participant in multiple payment systems and messaging networks. As such, CLS's comments focus primarily on the implementation of the Proposed Strategy and the development of the forthcoming guidance to operationalize the elements therein (the "Operational Guidance") in these contexts and are directed to specific areas where CLS believes it can provide useful input. Section I provides general feedback and offers two high-level considerations, and Section II provides more specific input with respect to some of the elements for the CPMI to consider in developing the Proposed Strategy and Operational Guidance.

I. General Comments on the Proposed Strategy

CLS recognizes that the risk of wholesale payments fraud constitutes a significant and increasing threat to the confidentiality, integrity, and availability of the global financial markets, and thus CLS supports the CPMI's efforts to focus industry attention on enhancing endpoint security. The challenge is all the more difficult given the international nature of the risk and the need for an approach that is robust, yet sufficiently flexible, to enable market participants to adapt to the dynamic and complex threat landscape. With this in mind, CLS submits two overarching considerations to help guide the development of the Proposed Strategy and the forthcoming Operational Guidance.

A. Dynamic, principles-based approach

First, the Proposed Strategy and Operational Guidance should remain principles-based in order to afford stakeholders the flexibility to adapt to the dynamic nature of cyber threats. This consideration is reflected in the Discussion Note[4] and should be similarly emphasized in the Operational Guidance. As threats evolve, so do best practices and technical standards designed to address them. Prescriptive requirements would be detrimental as the constant evolution of threats would render such requirements inefficient or even obsolete, potentially before full implementation. This view was echoed in the final CPMI-IOSCO *Guidance on cyber resilience for financial market infrastructures* (the "CPMI-IOSCO cyber guidance"),[5] which "is principles-based, recognising that the dynamic nature of cyber threats requires evolving methods to mitigate these threats. Guidance requiring specific measures today may quickly become ineffective in the future."[6] In the context of remarks addressing the (then draft) CPMI-IOSCO cyber guidance, a Federal Reserve Bank of New York official posited that "it may be preferable for market infrastructures to develop alternative solutions for responding to the cyber challenge, lest a monolithic solution result in an unintended concentration risk or an unhealthy 'groupthink'."[7] With this in mind, he offered a military analogy and cautioned against constructing "an inflexible Maginot line whose rigidities

[4] *See e.g.,* Discussion Note § 6 ("In developing the guidance, the CPMI will be mindful that the risk environment and risk management tools may evolve over time.").

[5] https://www.bis.org/cpmi/publ/d146.htm.

[6] CPMI-IOSCO cyber guidance § 1.2.2.

[7] Richard Dzina, Remarks at the Securities Industry and Financial Markets Association (SIFMA) 43rd Annual Operations Conference: Toward a New Paradigm for Resiliency and Security (3 May 2016), available at https://www.newyorkfed.org/newsevents/speeches/2016/dzi160503.

are easily subverted by a creative and nimble adversary." CLS encourages the CPMI to continue to heed these concerns and develop Operational Guidance that allows stakeholders to remain "creative and nimble" as well.

A prescriptive, monolithic solution is likewise impractical given the Proposed Strategy is designed to be taken into account by a broad range of public and private sector stakeholders (*i.e.*, operators of payment systems and messaging networks, their respective participants, and the respective supervisors, regulators, and overseers of operators and participants). The scope of covered entities is underscored in Section 6 of the Discussion Note, which states:

> [W]hile payment systems and messaging networks share many commonalities with one another, they vary in several aspects, including the number and diversity of their participants; the volume and nature of the underlying obligations being settled; and the relevant legal, operational and technical structures and constraints under which they may operate.

Moreover, "[s]uch variations may have important implications for determining the most appropriate and effective approaches to operationalising the [Proposed Strategy]."[8] CLS wholeheartedly agrees. In the case of CLS, payment systems that provide PvP settlement for matched payment instructions, by design, do not face many of the risks that would arise in the context of unmatched payments submitted by an individual market participant. It would therefore be neither appropriate nor effective to require all payment system operators to implement prescriptive measures or utilize specific tools intended to prevent or detect fraudulent activity in the context of one-way payments.

Accordingly, CLS welcomes comprehensive yet flexible Operational Guidance that stakeholders could tailor with regard to their specific operational and threat landscape, role in the wholesale payments ecosystem, and legal and regulatory requirements.[9] Such approach would complement the relevant principles and expectations set forth in the PFMI and CPMI-IOSCO cyber guidance and "could be taken into account by payment systems and messaging networks as they consider their approaches for observing [the relevant] principles and expectations, *where applicable and appropriate.*"[10]

B. Proactive public-private collaboration

Second, effective endpoint security requires a proactive, collaborative approach amongst public and private stakeholders. This precept cannot be overstated. The Discussion Note explains that given the interconnectedness of financial networks, efforts of a given party may not achieve the expected benefits unless other connected parties do the same.[11] As interconnectivity increases in the wholesale payments

[8] Discussion Note § 6.

[9] In the United States, for example, financial institutions supervised by the agencies that comprise the Federal Financial Institutions Examination Council ("FFIEC") are expected to manage cybersecurity risks associated with interbank messaging and wholesale payment networks in accordance with the FFIEC IT Examination Handbook. *See also* FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks (7 June 2016), available at https://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf (alerting financial institutions to specific risk mitigation techniques related to cyber-attacks exploiting vulnerabilities and unauthorized entry through trusted client terminals running messing and payment networks).

[10] *See* Discussion Note § 5 (emphasis added).

[11] Discussion Note § 3.

ecosystem, endpoint security is no longer viewed as solely the responsibility of the endpoint (and infrastructure security, in turn, the responsibility of the operator). Security breaches have implications for public confidence of the network as a whole, even where an operator's infrastructure and applications have not been compromised.[12]

Nevertheless, operators alone cannot verify and control every aspect of endpoint security; they need to rely on those who control the endpoints (or are closer to them) to ensure appropriate controls are in place and operating effectively.[13] This does not mean operators can abdicate responsibility for their endpoints; rather, they may not be in the best position to perform transaction monitoring and detect certain types of fraudulent activity. CLS therefore generally welcomes the elements in the Proposed Strategy that aim to clarify roles and responsibilities in this context, and offers specific considerations for certain elements below.

II. Comments on Specific Elements of the Proposed Strategy

A. Element 2 – Establish endpoint requirements

CLS recognizes the objective of Element 2 of the Proposed Strategy, which provides that operators should establish endpoint security requirements for participants as part of its participation requirements. In line with the policy considerations described above, CLS recommends that the Operational Guidance promulgate a principles-based, risk-based approach for this element and afford operators the flexibility to establish requirements that are practical, appropriate, and effective given the unique attributes of a given system and its participants.[14]

B. Element 3 – Promote adherence

CLS appreciates that operators should promote adherence to their participant endpoint security requirements, but urges the CPMI to adopt a flexible, risk-based approach for operationalizing Element 3, that complements, rather than supersedes, applicable principles and regulatory expectations.[15]

[12] *See* Richard Dzina, Remarks at the SIFMA Operations Conference and Exhibition 2017: Advancing the Fed's wholesale services in an area of unprecedented challenge and change (9 May 2017), available at http://www.bis.org/review/r170511b.pdf (addressing roles and responsibilities via-a-vis endpoint security); and Discussion Note § 3 (explaining how fraud may undermine confidence in the ecosystem, which could impede economic activity and financial stability).

[13] Discussion Note § 3.

[14] CLS also notes that most (if not all) operators are also participants in other payment systems and messaging networks and, as such, would be expected to comply with participant requirements promulgated by those operators.

[15] *See i.e.,* PFMI Principle 18, Key Consideration 2 ("An FMI's participation requirements should be justified in terms of the safety and efficiency of the FMI and the markets it services, be tailored to and commensurate with the FMI's specific risks, and be publicly disclosed. Subject to maintaining acceptable risk control standards, an FMI should endeavour to set requirements that have the least restrictive impact on access that circumstances permit.").

C. Element 4 – Provide and use information and tools to improve prevention and detection

CLS agrees that "*[t]o the extent reasonably possible*, the operator and participants of a payment system or messaging network should support the provision and use of information and tools that would enhance their and each other's respective capabilities to prevent and to detect in a timely manner attempted wholesale payments fraud."[16] Operators should be afforded the discretion to select appropriate and effective tools to supplement their capabilities, keeping in mind their unique attributes and capabilities, their role in the payment ecosystem, their risk profile, and the evolving threat landscape. Conversely, a monolithic approach could provide a roadmap for malicious actors and stifle development of more effective endpoint detection and response tools and risk mitigation practices.

* * *

We appreciate the CPMI's consideration of the views set forth in this letter and would welcome the opportunity to discuss any of these comments in further detail.

Sincerely,

Dino Kos
Chief Regulatory Officer, CLS Bank International

cc: Vas Rajan, Chief Information Security Officer, CLS Bank International
Craig Rubin, Senior Legal Counsel, CLS Bank International
Kerry F. Denerstein, Regulatory Affairs Specialist, CLS Bank International

[16] Discussion Note § 5 (emphasis added).