



November 28, 2017

Morten Linnemann Bech
CPMI Secretariat
Bank for International Settlements
Centralbahnplatz 2
4051 Basel
Switzerland

Via Email (cpmi@bis.org)

Re: Proposed Strategy to Address Wholesale Payment Fraud

Mr. Bech,

The Clearing House Payments Company, as the operator of CHIPS, and the Clearing House Association¹ (together, TCH) appreciate the opportunity to respond to CPMI's discussion note² regarding fraud related endpoint security risk in wholesale payment systems. The Bank of Bangladesh incident in 2016 and a handful of other reported incidents of fraud perpetrated against banks through compromise of their connections to the SWIFT network were alarming to wholesale payment system operators and participants alike. Thus, it is appropriate that the incidents have prompted both the private and public sector to reevaluate the security of wholesale payments and to consider whether measures should be taken to strengthen existing roles and responsibilities of operators and participants in response to evolving threats.

TCH acknowledges and supports the need to ensure the security of wholesale payment systems, and in particular the need for minimum security standards in the international, wholesale payment community. Hence, we welcome efforts, such as CPMI's proposed strategy for reducing wholesale payments fraud (Proposed Strategy), that facilitate discussions between the private and public sectors about this important topic. While the Proposed Strategy is helpful in providing principles for the private

¹ The Clearing House is a banking association and payments company that is owned by the largest commercial banks and dates back to 1853. The Clearing House Payments Company L.L.C. owns and operates core payments system infrastructure in the United States and is currently working to modernize that infrastructure by building a new, ubiquitous, real-time payment system. The Payments Company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly \$2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume. Its affiliate, The Clearing House Association L.L.C., is a nonpartisan organization that engages in research, analysis, advocacy and litigation focused on financial regulation that supports a safe, sound and competitive banking system.

² CPMI Discussion Note: Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security (September 2017).

and public sectors to consider in their efforts to address endpoint security risk, TCH has a number of concerns with the strategy, including

- CPMI's suggestion that compromise of a single endpoint³ may undermine confidence in the entire wholesale payment system,
- elements of the strategy that would fundamentally alter the operation of wholesale payment systems and the liability frameworks that apply to them, and
- the assignment of certain endpoint security responsibilities to payment system operators that are inconsistent with their role in the wholesale payment system

Thus, TCH recommends that CPMI's Proposed Strategy:

- allow operators and other stakeholders within each country to work together to create guidelines for endpoint security that consider the legal, supervisory, and regulatory framework applicable to wholesale payment systems and participants in their jurisdiction;
- focus endpoint security guidelines on each participant's ability to secure its own environment;
- recognize the role of originating banks and supervisory authorities in reducing endpoint security risk in wholesale payments and allocate responsibilities appropriate to their roles, similar to the approach CPMI took in its recent continuity of access guidance⁴; and
- clarify that the strategy is intended to establish principles for consideration by the wholesale payment community globally but (i) is not intended to alter rights and responsibilities of parties to wholesale payments, as determined by applicable law and (ii) allows operators in each country to determine the appropriate approach to end point security.

A. CPMI's Characterization of Risk

TCH agrees with CPMI's observation that fraud in the wholesale payment ecosystem is becoming increasingly sophisticated and supports CPMI's call for a coordinated and holistic approach to addressing fraud related endpoint security risk. However, we have reservations about CPMI's suggestion that there is "an absence of appropriate arrangements"⁵ in place within the wholesale payment ecosystem and, thus, compromise of a single endpoint could undermine confidence in the entire payment system.

³ CPMI defines an endpoint for purposes of its discussion note as "a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem." p.1, CPMI Discussion Note: Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security (September 2017).

⁴ Guidance on Continuity of Access to Financial Market Infrastructures for a Firm in Resolution (July 2017). We note that this guidance sets out three categories of responsibilities: those that apply to providers of critical FMI services, those that apply to firms, and cooperation among public sector authorities, providers, and firms.

⁵ p.1, CPMI Discussion Note: Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security (September 2017).

The private sector has taken considerable steps over the past 18 months to address potential endpoint compromises in wholesale payments through cybersecurity information sharing arrangements, cybersecurity exercises involving endpoint compromise scenarios, and the development of industry playbooks for scenarios in which a bank suffers some form of cyberattack and must disconnect (or be disconnected from) wholesale payment systems. Insights gained from these exercises have enabled individual entities and the industry collectively to (i) better understand their capabilities and needs in the event of an endpoint compromise impacting wholesale payment systems and (ii) revise their processes, procedures, and technical capabilities to better address such potential situations. The private sector will continue to carry out these efforts and refine its preparations for potential compromise events. Given that the private sector has developed and will continue to improve “appropriate arrangements within the ecosystem”⁶, we suggest that CPMI take these private sector efforts into consideration in its evaluation of the potential impact of a compromise of a single endpoint. It is also critical that learnings and guiding principles from private sector efforts inform the manner in which operators approach endpoint security in their relevant jurisdictions.

B. Comments to Proposed Strategy

1. General Comments

CPMI has proposed seven principles as its Proposed Strategy. CPMI states that these principles were designed “to be taken into account by all relevant public and private stakeholders in reducing the risk of wholesale payments fraud”⁷ However, the principles primarily assign responsibility for endpoint security to operators and participants and not to public sector authorities. As detailed further below, TCH thinks that some of the principles should be addressed to (i) originating banks, rather than generically to all participants and (ii) public sector authorities rather than operators. We request that CPMI use an iterative process before finalizing its Proposed Strategy. In particular we ask that CPMI share another draft of the principles that comprise its strategy for reducing wholesale payment fraud for additional comment prior to issuing final guidance.

CPMI notes that the Proposed Strategy compliments certain risk management topics in the Principles for Financial Market Infrastructures (PFMI) as well as related CPMI guidance, such as its guidance on cyber resilience⁸. It also suggests that in observing the PFMI and related guidance operators could take the strategy into consideration “where applicable and appropriate.”⁹ This suggestion is consistent with TCH’s understanding that CPMI’s final Proposed

⁶ *Id.*

⁷ *Id.*, p. 3.

⁸ Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016).

⁹ *Id.*, p. 4.

Strategy will consist of principles for consideration by the private and public sectors and not binding regulation. TCH supports international efforts at consistent guidance.¹⁰

2. Comments to Principles

1. ***Identify and understand the range of risks.*** *The operator and participants of a payment system . . . should identify and understand the risks related to endpoint security that they face individually and collectively, including risks related to the potential loss of confidence in the integrity of the payment system or messaging network itself.*

TCH agrees that an operator and its participants should identify and understand risks related to endpoint security that they face individually and collectively. However, it is important that CPMI not be overly prescriptive in describing the manner in which operators and participants engage in this process.

We note that in addition to broader industry discussions in the U.S. about cyber threats in the payment space, efforts to identify and understand endpoint security risk and wholesale payments fraud have already taken place and continue to take place through discussions with TCH's Managing Board and CHIPS Business Committee. TCH has also formed working groups with its member banks to more closely consider how the industry can better protect against endpoint security risk. Finally, TCH and CHIPS Participants have explored the impact of potential endpoint security compromise through cybersecurity exercises, as discussed above.

2. ***Establish endpoint requirements.*** *The operator of a payment system or a messaging network should establish clear endpoint security requirements for its participants as part of its participation requirements. Such requirements should include those for the prevention and detection of fraud, for the immediate response to fraud and, when appropriate, for alerting the broader payments network community to evolving fraud threats. In addition to the requirements established by the operator of a payment system or a messaging network, each participant of the payment system or messaging network should identify and establish its own, supplemental risk-based endpoint security requirements as needed.*

Given the potential impact of endpoint security requirements on the liability frameworks for wholesale payments described further below, and the variety of legal, regulatory, and prudential regimes that apply to wholesale payment systems and participants, TCH believes CPMI should allow operators and stakeholders within each country to work together to provide an overarching, high level framework for endpoint security that is suited to their respective jurisdictions. Further, as part of a collaborative

¹⁰ Obviously, we would resist efforts by U.S. regulators to enforce the strategy as a binding requirement -- for example, the basis for a Matter Requiring Attention or an examination rating -- unless and until it was proposed and finalized at the Bank for International Settlements, published for notice and comment in the United States, adopted as a final rule and submitted to the Congress pursuant to the Congressional Review Act.

effort, endpoint security requirements are to be framed so that each participant is expected to secure its own environment without imposing a duty for participants or operators to identify and prevent compromise that may have occurred outside of their environments. As such, the second principle should be revised to (i) enable operators within a country to adopt an approach to endpoint security that is in line with high level CPMI guidance, but tailored to their jurisdiction and (ii) focus endpoint security requirements on each participant's ability to secure its own environment.

We further note that any CPMI expectations regarding the detection of fraud for in-flight payments should be considered in light of the impact such detection would have on customer experience and operational resources due to the likely need for intermediary banks or operators to stop and review or confirm payments that have alerted. We believe such impacts must be weighed against the potential risk mitigation benefits of in-flight fraud detection.

Robust U.S. Supervisory and Regulatory Framework. In our view, the US framework can be instructive to other jurisdictions in understanding how endpoint security requirements are implemented today in practice. Participants that are subject to U.S. supervision are required to comply with comprehensive information security requirements pursuant to law, regulation, and regulatory guidance. They are also subject to examination for such compliance. These regulatory obligations relate to information security programs generally and the use of payment systems specifically. In addition, they include requirements for "effective authentication controls applicable to high-risk online transactions involving ... the movement of funds to other parties."¹¹

With respect to payment systems specifically, regulated U.S. depository institutions are subject to examination regarding their management of risk associated with payments origination.¹² The Federal Financial Institution Examination Council's Information Technology Examination Handbook, which prescribes uniform "principles, standards and report forms" for the federal examination of financial institutions, includes a detailed

¹¹ FFIEC Guidance: Authentication in an Internet Banking Environment (October 12, 2005), available at https://www.ffiec.gov/pdf/authentication_guidance.pdf. This guidance establishes minimum supervisory expectations for customer authentication controls applicable to "high-risk online transactions" involving the movement of funds to other parties. Among other things, the guidance notes that payment transactions from commercial accounts "pose a comparatively increased level of risk to the institution and its customer" because of the increased frequency and dollar amount of such transactions. Accordingly, regulators expect financial institutions to offer multifactor authentication to business customers and "implement layered security ... utilizing controls consistent with the increased level of risk for covered business transactions."

¹² The Financial Institutions Examination Council ("FFIEC") is an interagency body that prescribes "principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) ..." <https://www.ffiec.gov/about.htm>.

section on wholesale payment systems.¹³ This section includes the expectation that financial institutions implement internal and operational controls to “mitigate or limit operational risks, such as authentication and encryption techniques to ensure the authenticity of the payer and payee as well as prevent unauthorized access to information in transit and edit checks and automated balancing to verify the integrity of the information relative to the payment order and funds transfer transaction.”¹⁴ U.S. depository institutions are further expected to put in place internal controls to “maintain overall integrity for any funds transfer operation” consistent with certain recommended control objectives.¹⁵

We note that all CHIPS participants conduct their CHIPS activity in the U.S. and are subject to either federal or state prudential supervision. The current regulatory and prudential framework that applies to CHIPS participants is pertinent to how TCH would propose to address endpoint security for CHIPS

Concerns with Establishment of Endpoint Security Requirements by Operators. It is important to emphasize that neither the functions an operator performs, nor the legal framework that applies to wholesale payment systems in the U.S., is suited to the role CPMI contemplates in its second principle. Wholesale payment system operators are designed to clear and settle payments for banks, not to act as quasi-regulators. The CHIPS Rules require a participant to be a depository institution and subject to U.S. supervision¹⁶ because TCH relies in large part on the supervisory and regulatory framework that applies to banks as the primary assurance that its participants operate in a safe and sound manner, including with respect to information security. A requirement that TCH establish endpoint security requirements for CHIPS participants beyond what is required by the robust U.S. prudential

¹³ FFIEC IT Examination Handbook, Wholesale Payment Systems: Internal Controls, available at: [https://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems/wholesale-payment-systems-risk-management/operational-\(transaction\)-risk/internal-and-operational-controls.aspx](https://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems/wholesale-payment-systems-risk-management/operational-(transaction)-risk/internal-and-operational-controls.aspx).

¹⁴ FFIEC IT Examination Handbook, Wholesale Payment Systems: Internal Controls, available at: [https://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems/wholesale-payment-systems-risk-management/operational-\(transaction\)-risk/internal-and-operational-controls.aspx](https://ithandbook.ffiec.gov/it-booklets/wholesale-payment-systems/wholesale-payment-systems-risk-management/operational-(transaction)-risk/internal-and-operational-controls.aspx).

¹⁵ These control objectives include “protecting original instructions from loss or alteration[,]” “authenticating the identity and authority of the sender[,]” “maintaining a physically secure environment[,]” and “maintaining appropriate separation of duties for employees involved in the payment process.” Id.

¹⁶ CHIPS Rule 19 (a). “A depository institution may become a Participant if (A) it carries on the business of a depository institution from an office located in the United States of America, (B) the office in the United States of America is subject to regulation by a federal or state depository-institution regulatory authority, (C) it is a “financial institution” within the meaning of § 402(9) of the Federal Deposit Insurance Corporation Improvement Act of 1991, 12 U.S.C. § 4402(9), (D) it shall transmit payment messages to and receive payment messages from the System only through a connection that meets the requirements of Rule 6, and (E) it shall maintain primary and back-up computer facilities required by Rule 7.”

framework would be a fundamental change in its role as an operator, which we do not think is warranted given the nature of CHIPS and its participants.

Moreover, if TCH were to establish endpoint security requirements for CHIPS participants that were not carefully tailored to fit within the construct of existing U.S. law, we think such requirements could expose both TCH and CHIPS participants to unwarranted liability. In the U.S. the legal framework that applies to wholesale payments¹⁷ places responsibility on a bank to establish a commercially reasonable security procedure agreement with its customer who instructs a payment order, whether such customer is an individual, business, or another bank. The legal framework allocates liability for transfers that arise from instructions that were not authorized by the customer to either the bank or the customer, based on the bank's adherence to those procedures and whether the bank accepted the customer's order in good faith.

This construct applies to each payment order within a funds transfer, i.e., between the originator and the originating bank, between the originating bank and its correspondent (intermediary bank), and between a correspondent and a beneficiary bank. However, the construct does not require or contemplate that an operator would interject security requirements that apply between banks, other than the operator's own security procedures for validating wires it receives from a participant, which would act as the security procedure between the sending and receiving participant in a wholesale payment system. Nor does the construct require or contemplate that a bank would identify or prevent fraud that occurred between another bank and its customer.

Hence, the Proposed Strategy's suggestion that an operator establish clear endpoint security requirements that would apply beyond its own communications with a sending participant could introduce legal ambiguity as to the operator's responsibility and liability to third parties, if not carefully tailored to fit within the construct of U.S. law. Similarly, the suggestion that endpoint security requirements might require banks to identify and prevent fraud that occurs as between another bank and its customer has no basis in U.S. law and could introduce legal ambiguity and potential liability for participants in the U.S. wholesale payment system. In both cases the introduction of such legal ambiguity and potential liability would be contrary to the first principle of CPMI's own PFMI, namely, a well-founded,

¹⁷ This legal framework is provided by Article 4A of the Uniform Commercial Code. The Uniform Law Commission promulgated Article 4A in 1989 to provide a customized set of rules to govern wire transfers among parties. Article 4A provides a comprehensive body of law on the rights and obligations connected with fund transfers made through the banking system. Article 4A has been enacted in all 50 states and the District of Columbia. It is important to emphasize that one of the most important aspects of Article 4A is the allocation of risk of loss among parties in a funds transfer. In fact, in drafting 4A "a critical consideration was that the various parties to funds transfers need to be able to predict risk with certainty, to insure against risk, to adjust operational and security procedures, and to price funds transfer services appropriately." Official Comment, 4A-102.

clear, transparent, and enforceable legal basis for financial market infrastructures.¹⁸ For these reasons we reiterate our recommendation that CPMI enable operators and stakeholders within a country to work together to determine the best means of addressing endpoint security within their jurisdiction.

3. **Promote adherence.** *Based upon the understanding of the risks and the endpoint requirements of a payment system or a messaging network, the operator and participants of the payment system or messaging network should establish processes as necessary to help ensure adherence to their respective endpoint security requirements.*

Assurance of adherence to sound information security practices should be addressed primarily to participants within their existing supervisory frameworks or, for countries in which standards need to be raised, revised supervisory and regulatory frameworks. While operators may seek certifications by internal or external parties of a participant's compliance with a common information security standard for the operators' own risk management purposes or risk-based reviews of particular participants' endpoint security practices, they should not be required to undertake an extensive assessment and validation of every participant's endpoint security practices. This is because assurance is not consistent with the role of an operator and could potentially lead to the imposition of liability on operators if participants or third parties relied on operators to discover faulty participant practices. As such, like CPMI's suggestion that operators establish endpoint security requirements, TCH believes assurance of adherence is a topic that must be carefully navigated based upon the laws, regulations, and prudential frameworks of each country.

4. **Provide and use information and tools to improve prevention and detection.** *To the extent reasonably possible, the operator and participants of a payment system or a 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.*

TCH thinks that guidance and recommendations on endpoint security requirements should be focused on information security procedures employed by participants to ensure the security of their environments rather than centralized fraud detection systems. Such guidance could help to ensure that all participants in a payment chain are employing consistent security guidelines. To the extent there are information and tools that are reasonably possible for operators to provide, and that participants believe will enhance their information security procedures, TCH is supportive of providing them. We further note that there may be opportunities for different operators to work together with participants to develop information and tools that may be useful in the end-to-end payment chain.

¹⁸ The key considerations for this PFMI principle include that the legal basis "should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions" and that the FMI's rules, procedures, and contracts be consistent with relevant laws and regulations. Principles for Financial Market Infrastructures (April 2012), p.21.

5. ***Respond in a timely way to potential fraud.*** *The operator and participants of a payment system or a messaging network should adopt procedures and practices, and deploy sufficient resources, to respond to actual or suspected fraud in a timely manner. This includes, where possible and appropriate, supporting the timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction when detected.*

An essential feature of wholesale payment systems is the irrevocability of payments. This is what enables high value payments to be made quickly and with certainty. While TCH supports efforts to improve the existing ability¹⁹ of participants to send and respond to requests for cancellation or requests for return of funds, such efforts must not entail a requirement that a bank receiving such a request has an obligation to cancel the payment order or return funds. Rather, such a receiving bank should only have a responsibility to acknowledge receipt of the request. Similarly, any efforts to encourage the transmission of a request for cancellation or request for return of funds through a chain of banks must not require that any bank, other than the original bank requesting the cancellation or return of funds, be required to offer an indemnity as part of its communication of the request.

6. ***Support ongoing education, awareness and information-sharing.*** *The operator and participants of a payment system or a messaging network should collaborate to identify and promote the adoption of procedures and practices, and the deployment of sufficient resources, that would support ongoing education, awareness and, to the extent appropriate and legally permissible, information-sharing about evolving endpoint security risks and risk controls.*

TCH supports education and awareness related to endpoint security. However, we think such efforts are best employed by existing industry groups whose mission it is to educate and raise awareness with the broader banking community. For example, in the U.S. FS-ISAC²⁰ serves as a cyber threat education and awareness resource for banks and operators. While operators and participants should be encouraged to participate in organizations such

¹⁹ CHIPS provides service messages today that can be used by a sending participant to request return of funds from a receiving participant. However, there is no requirement that a receiving participant acknowledge receipt or otherwise respond to such messages.

²⁰ Financial Services Information Sharing and Analysis Center (FS-ISAC) serves as a global financial industry resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members and operates as a member-owned non profit entity. FS-ISAC constantly gathers reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources. With this information, the FS-ISAC is uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information to your organization. This information includes analysis and recommended solutions from leading industry experts. FS-ISAC is currently active with members and partners across countries and regions throughout North and South America, Europe, the Middle East and Asia/Pacific. More information available at <https://www.fsisac.com>.

as FS-ISAC, we think it would be duplicative for TCH to create a separate endpoint security education and awareness program.

We recognize the value of information sharing but note, as the principle does, that there are significant legal considerations at play, including data privacy laws, data sharing restrictions, and potential liability for passing on unverified claims of fraud. As such, information sharing without the appropriate legal structure in place may be fraught with liability issues. There are fraud and cyber threat information sharing arrangements in place today, such as through FS-ISAC and other public-private sector groups. While the private sector has explored and continues to explore expanded information sharing arrangements related to wholesale payment fraud, the feasibility and usefulness of such arrangements remain to be determined. Hence, we think the Proposed Strategy should encourage information sharing efforts generally within the wholesale payment community but not place any specific expectations on operators or participants to develop procedures and practices regarding information sharing.

7. ***Learn, evolve and coordinate.*** *The operator and participants of a payment system or a messaging network should monitor evolving endpoint security risks and risk controls, and review and update their endpoint security requirements, procedures, practices and resources accordingly. In addition, the operators and, to the extent practicable, participants of different payment systems and messaging networks should seek to coordinate approaches for strengthening endpoint security across payment systems and messaging networks in order to obtain potential implementation efficiencies where possible and appropriate. Similarly, supervisors, regulators and overseers of payment systems and messaging network and participants of payment systems and messaging networks should review and update their supervisory/oversight expectations and assessment programmes to reflect the evolving risk mitigation strategies.*

CPMI should clarify its expectations for the monitoring of security risks and controls so that it is not construed as a constant, real-time process, but rather the need for operators and their participants to monitor evolving industry best practices, threat trends, etc. in order to maintain appropriate standards and controls. Additionally, operators should determine how and to what extent endpoint security applies within their risk management frameworks. Operators, like CHIPS, that do not utilize internet connections for payment initiation may not need the same level of scanning as those that do.

TCH believes coordination of endpoint security efforts already occurs in the US occurs through organizations like FSARC²¹, public-private sector efforts such as the Critical

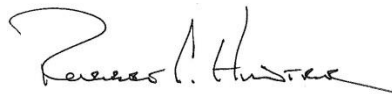
²¹ Financial Systemic Analysis & Resilience Center (FSARC) is affiliated with FS-ISAC. Its mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. Government. The FSARC's activities will continue enhancement and effectiveness of information exchange, sharing of greater sophisticated analysis techniques, and closer

Infrastructure Partnership Advisory Council Financial Services Sector Cybersecurity Profile Development Working Group²² and informal discussions between financial market infrastructures.

We think the principle's suggestion that regulators should update their expectations on an ongoing basis should be qualified based upon a country's existing supervisory and regulatory landscape. While there may be a need in certain countries for updated supervisory and regulatory expectations related to endpoint security, in the U.S. the financial services industry has been inundated with "evolving" guidance. As such, what is most needed in the U.S. is coordination among public sector actors and an approach to cybersecurity that is not regulatory-driven and compliance focused but industry-driven and security focused.

The Clearing House appreciates the opportunity to comment on CPMI's discussion note. If you have any question, please contact the undersigned by phone at (336) 769-5314 or by email at rob.hunter@theclearinghouse.org.

Respectfully submitted,



Robert C. Hunter
Executive Managing Director and Deputy General Counsel
The Clearing House Payments Company, L.L.C.

collaboration between large U.S. financial services firms and U.S. government agencies, including the Department of Treasury, the Department of Homeland Security and the Federal Bureau of Investigation and will leverage existing FS-ISAC controls to ensure the protection of private information. More information available at <https://www.fsisac.com/sites/default/files/news/FS-ISAC%20Announces%20the%20Formation%20of%20the%20Financial%20Systemic%20Analysis%20%28FSARC%29.pdf>.

²² CIPAC was established by the U.S. Department of Homeland Security to "facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators," on "a broad spectrum of activities to support and coordinate critical infrastructure security and resilience." Critical Infrastructure Partnership Advisory Council, DHS, <https://www.dhs.gov/critical-infrastructure-partnership-advisory-council>. Each critical infrastructure sector has developed councils to focus on sector specific issues, such as the Financial Services Sector Coordinating Council ("FSSCC"), which "serves as the primary private sector policy coordination and planning entity to collaborate with the United States Department of Treasury, Financial Services Government Coordinating Council (GCC) and other government entities to address the entire range of critical infrastructure security and resilience activities and sector-specific issues."