December 7, 2015

Robert Lindley
CPMI Secretariat
Committee on Payments and Market Infrastructures
Centralbahnplatz 2
CH-4002 Basel Switzerland

Re: Comments in Response to Consultative Report–*Correspondent Banking*

Dear Mr. Lindley:

The Clearing House Association L.L.C. ("**The Clearing House**")[1] appreciates the opportunity to provide our comments and recommendations on the consultative report on correspondent banking (the "**Report**") published by the Committee on Payments and Market Infrastructures of the Bank for International Settlements (the "**CPMI**") at the request of the BIS Economic Consultative Committee Governors.[2] For many years, The Clearing House has been deeply engaged in policy discussions, both among its members and with government authorities, over how best to address and mitigate risks presented by correspondent banking, in particular with respect to anti-money laundering and countering the financing of terrorism ("**AML/CFT**") considerations.

The Clearing House shares the CPMI's concerns about recent trends in correspondent banking that "point to risks to its safe and efficient functioning," and we support efforts in the Report and elsewhere to analyze "technical measures that might alleviate some of the concerns and cost issues related to correspondent banking."[3] We believe that certain of the technical initiatives discussed in the Report—including development of know your customer ("**KYC**") utilities and other information-sharing

---

[1] Established in 1853, The Clearing House is the oldest banking association and payments company in the United States. It is owned by the world's largest commercial banks, which collectively hold more than half of all U.S. deposits and which employ over one million people in the United States and more than two million people worldwide. The Clearing House Association L.L.C. is a nonpartisan advocacy organization that represents the interests of its owner banks by developing and promoting policies to support a safe, sound and competitive banking system that serves customers and communities. Its affiliate, The Clearing House Payments Company L.L.C., which is regulated as a systemically important financial market utility, owns and operates payments technology infrastructure that provides safe and efficient payment, clearing and settlement services to financial institutions, and leads innovation and thought leadership activities for the next generation of payments. It clears almost $2 trillion each day, representing nearly half of all automated clearing house, funds transfer and check-image payments made in the United States. *See* The Clearing House's web page at www.theclearinghouse.org.

[2] Bank for International Settlements, *Consultative Report—Correspondent Banking* (Oct. 2015), *available at* http://www.bis.org/cpmi/publ/d136.htm.

[3] *Id.* at 1.

tools—can potentially enhance correspondent banks' efforts to combat money laundering while also supporting "an efficient provision of cross-border payment services globally."[4] At the same time, we share the CPMI's view that "the issues surrounding the withdrawal from correspondent banking are very complex"[5] and thus further technical measures are not sufficient to address these complex factors. While technical measures may serve as part of the solution, a broader review and reform of governmental policies are equally vital. Thus, we strongly caution against pursuing purely technical measures to improve the correspondent banking environment, and instead encourage the additional efforts reported to be underway by the Financial Action Task Force on Money Laundering (the "**FATF**") and other international organizations, especially to the extent they involve clarifying regulatory expectations and "domestic capacity building" for jurisdictions with AML/CFT deficiencies.[6]

Clearing House member banks together provide a very significant proportion of correspondent banking services worldwide, and we therefore understand the tremendous benefits—as well as the substantial risks—of correspondent banking. We also appreciate recent trends, sometimes referred to as "de-risking," that have seen banks generally "reducing the number of [correspondent banking] relationships they maintain and . . . establishing few new ones."[7] Contrary to the assertions of some, we absolutely and fundamentally disagree that such changes in the correspondent banking environment follow from Clearing House member decisions to indiscriminately close off broad classes of clients and jurisdictions.[8] Rather, The Clearing House believes that this trend is the result of a complex set of factors. These factors include individual banks' prudent risk management decisions. They also include the substantial and evolving expectations placed on correspondent banks by governments and supervisors to effectively perform a quasi-supervisory function and act as "gatekeepers" to those seeking access to the global banking system.

Disruption to the correspondent banking framework is a shared problem that requires a shared solution. Efforts to address the so-called "de-risking" phenomenon and the attendant risks to the safe and efficient functioning of the correspondent banking system should reflect the mutual and joint responsibility of the public and private sectors to mitigate the risk that bad actors will access the financial system through their misuse of correspondent banking services. Consistent with this principle, and in addition to the technical measures proposed in the Report and elsewhere, we believe it is crucial that governments and supervisors enact concrete reforms that enable correspondent banks to more fully rely on:

---

4 *Id.* at 4.

5 *Id.* at 1.

6 Financial Stability Board, *Report to the G20 on Actions Taken to Assess and Address the Decline in Correspondent Banking* (Nov. 2015), *available at* http://www.financialstabilityboard.org/2015/11/report-to-the-g20-on-actions-taken-to-assess-and-address-the-decline-in-correspondent-banking/ (the "**FSB Report**").

7 Report at 1. *See also* the FSB Report.

8 *See* Remarks by Treasury Acting Under Secretary Adam Szubin at the American Bankers Association/American Bar Association Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0264.aspx and remarks by Treasury Under Secretary Nathan Sheets at The Center for Global Development (Nov. 12, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0264.aspx.

(i) the regulation and supervision of the AML/CFT programs of their respondents (both domestic and foreign) by home country supervisors, so that correspondents do not have to act as the *de facto* supervisor of their respondents, which is becoming a U.S. supervisory expectation;

(ii) the accuracy and completeness of payment information provided by originating and beneficiary banks; and

(iii) KYC and other AML/CFT information provided by utilities.

For the same reasons, The Clearing House believes it is equally, if not more important that governments and regulators, on the one hand, and the correspondent banking community, on the other, work together to collectively, and transparently, clarify and define the roles and responsibilities of the various stakeholders for detecting, reporting and preventing money laundering through the global correspondent banking network. In particular, we suggest that this examination of roles and responsibilities should include an evaluation of whether current supervisory expectations, which increasingly look to banks to act as gatekeepers and, thus, *de facto* supervisors of their respondents, are undermining and frustrating financial inclusion and other public policy objectives.

Part I of this letter discusses some of the factors that have led to disruptions in the correspondent banking environment and possible ways to address them. Part II discusses our concerns around the need for further regulatory guidance on certain matters, in particular (i) the ability of correspondent banks to monitor payment messages for completeness and accuracy and (ii) the so-called "know your customer's customer" ("**KYCC**") obligations of correspondent banks referred to in the Report. Finally, Part III discusses our general support for further development of KYC utilities and other information-sharing systems that may facilitate and streamline correspondent banks' performance of their AML/CFT obligations, subject to certain limitations of those systems.

I. <u>The causes of the recent reduction in correspondent relationships noted in the Report are complex and include, in part, the substantial and quasi-supervisory obligations placed on correspondent banks.</u>

Correspondent banking is a vital component of the global economy, allowing banks "to serve their customers' global payment needs with the essential attributes of confidence, speed and efficiency."[9] These attributes are essential to the successful functioning of the global payment system, but they also render the system vulnerable to being used to launder money, finance terrorism or commit other crimes. The Report cites a recent reduction in the number of correspondent banking relationships and notes that these reductions are disproportionately affecting respondent banks that (i) do not generate significant correspondent banking volumes or (ii) are located in jurisdictions generally perceived as, or characterized by public sector actors as, risky.[10]

---

[9] The Clearing House, *Exposure Draft of Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking* (Sept. 2014), at 5.

[10] Report at 8. Of course, any "scaling back" of relationships with respondent banks impacts customers—both individuals and corporations—in the jurisdictions served by those respondent banks; therefore, if

In order to address these recent disruptions to correspondent banking services, it is important to acknowledge and confront the design of the AML/CFT regime, including the responsibilities placed upon correspondent banks and the incentives those responsibilities create. Further, while we understand that the Report is meant to address reductions in correspondent services that are driven by cost, lack of information or regulatory uncertainty, we note that there is some amount of de-risking that occurs because banks are faithfully carrying out the dictates of the AML/CFT regime and thereby wisely mitigating their exposure to AML/CFT risks that cannot be managed – not only because it is required by law, but also because it ensures the safety and soundness of the institution as well as the system as a whole.

A. De-risking by design.

As an initial matter, it is important to acknowledge that in many cases, a reduction in correspondent banking services is the function of express government policy. In particular, under current guidance there are certain jurisdictions and categories of customers for which banks are encouraged to avoid or exit any correspondent banking relationships.[11] For example, the FATF has suggested that in circumstances in which a bank cannot apply an appropriate level of customer due diligence ("**CDD**") to match a prospective or existing banking customer's risk profile, the bank should "not enter into the business relationship or [should] terminate the business relationship."[12] Additionally, as the FSB recently noted in its report, large banks appear to be reducing correspondent banking services in jurisdictions or segments that are highly susceptible to AML/CFT risk.[13] To the extent that such de-risking conflicts with other public policy incentives, such as humanitarian aid, financial inclusion or keeping financial flows in regulated systems, policy makers need to acknowledge that continuing certain relationships to meet these other objectives will necessarily expose banks to certain risks and provide banks (i) flexibility to manage those risks within the current regulatory architecture and (ii) comfort that their risk management efforts will be evaluated by supervisors according to the principles of the risk-based framework.

B. Due to regulatory expectations, correspondent banks are incentivized to disengage from correspondent banking relationships where the actual and unquantifiable costs associated with managing the AML/CFT risks of those relationships, outweigh any benefits.

Beginning shortly before—and accelerating after—the September 11th attacks, governments and regulators began focusing on the risks inherent in correspondent banking and adopted a series of measures designed to address them. In the United States, such measures included the adoption of Section 311 of the Patriot Act, which authorizes the Secretary of the Treasury to designate specific jurisdictions or individual entities that are deemed to be of high risk with respect to money

---

correspondent banking "cut-backs" are affecting banks in certain jurisdictions disproportionately, customers in those jurisdictions will be disproportionately affected as well.

11 FATF, *Guidance for a Risk-Based Approach: The Banking Sector* (Oct. 2014)

12 Id. at 20.

13 As the FSB Report notes, "[j]urisdictions most frequently exited by large global correspondent banks seem to be those with weak supervisory and regulatory frameworks, including those with weakness related to AML/CFT and those which are subject to United Nations sanctions." FSB Report at 8.

laundering activities and to require banks to take special measures to restrict the flow of funds to such entities.[14] Internationally, the FATF has maintained, since 2000, a list of jurisdictions with AML/CFT deficiencies that pose a risk to the international financial system.[15] At the same time, based on the requirements of Section 312 of the Patriot Act, the U.S. Treasury Department implemented regulations requiring banks to apply risk-based due diligence policies, procedures and controls with respect to correspondent accounts maintained in the United States for foreign financial institutions.[16]

To meet these enhanced standards, expectations and regulatory requirements, banks have invested considerable resources to develop the staff, controls and technological tools needed to carry out more robust AML/CFT efforts with respect to correspondent banking. At the same time, U.S. regulators and enforcement authorities have increasingly scrutinized bank efforts in this area and, in a number of high profile instances, have found banks' efforts and the speed with which certain banks have kept pace with regulatory developments to be inadequate, imposing substantial (multi-hundred million and even multi-billion dollar) civil money penalties, corrective action programs and even criminal settlements.[17] Similarly, banks' correspondent banking relationships are subject to increasing supervisory attention as banks face questions from their supervisors in bank examinations regarding their relationships with specific correspondent banking customers and their level of comfort with those relationships. All of these developments have resulted in an environment in which there is enormous focus by banks on the substantial legal, regulatory, and reputational risks associated with failure to adhere to ever-evolving and ever-increasing public sector expectations.

Accordingly, and understandably, some banks have simply chosen not to provide correspondent banking services to particular categories of customers, or all customers within a particular jurisdiction, that are deemed as "high-risk" for AML/CFT purposes. Regulators have expressed concern that this withdrawal from whole segments of customers is inconsistent with a bank's responsibility to manage risk and to take steps to mitigate risk where appropriate.[18] But banks have found that in certain segments, the cost to their institution of managing the risk in a way that meets regulatory expectations—particularly given the tangible risk of huge monetary penalties and the

---

[14] The Uniting and Strengthening America by Providing Appropriate Tools Require to Intercept and Obstruct Terrorism Act of 2001. 12 U.S.C. § 5318A.

[15] The most recent list, updated as of October 23, 2015, is *available at* http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/public-statement-october-2015.html.

[16] *See* 31 U.S.C. § 5318(i); 31 C.F.R. § 1010.610.

[17] *See, e.g.*, Office of the Comptroller of the Currency, In the Matter of JPMorgan Chase Bank, N.A., et al. (Jan. 7, 2014), *available at* http://www.occ.gov/news-issuances/news-releases/2014/nr-occ-2014-1.html; FinCEN, In the Matter of HSBC Bank USA, N.A. (Dec. 10, 2012), *available at* http://www.fincen.gov/news_room/ea/files/HSBC_ASSESSMENT.pdf; Office of the Comptroller of the Currency, In the Matter of HSBC Bank USA, N.A. (Oct. 6, 2010), *available at* http://www.occ.gov/news-issuances/news-releases/2010/nr-occ-2010-121.html, p. 3.

[18] [18] *See* Remarks by Treasury Acting Under Secretary Adam Szubin at the American Bankers Association/ American Bar Association Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0264.aspx and remarks by Treasury Under Secretary Nathan Sheets at The Center for Global Development (Nov. 12, 2015), *available at* https://www.treasury.gov/press-center/press-releases/Pages/jl0264.aspx.

intangible reputational risks that would arise if those clients were to carry out money laundering or terrorist financing activities through correspondent accounts—is too great to justify maintaining the correspondent relationship. This regulatory framework, which assigns individual banks liability for managing AML/CFT risks for services and transactions that necessarily require some level of reliance on other parties, results in banks making decisions that are reasonable and appropriate for their individual institutions, but may give rise to broader and counterproductive consequences in the aggregate. Specifically, we observe that as sophisticated, globally-active banks reduce correspondent services, the related AML/CFT risk for those banks may be eliminated, but will nonetheless persist as a systemic matter, and simply relocate to (i) banks that are not as well equipped to manage AML/CFT risk in correspondent relationships, (ii) nested correspondent relationships, or (iii) less regulated or unregulated portions of the market.

In our view, in order to address the "de-risking" phenomenon and the attendant risks to the safe and efficient functioning of the correspondent banking system, governments and regulators should engage with the correspondent banking community to clarify and perhaps redefine the roles and responsibilities of the various stakeholders for detecting, reporting and preventing money laundering through the global correspondent banking network. We believe that AML/CFT efforts will achieve the best results if they are viewed as a private sector-public sector partnership, with each side reviewing and identifying entities and jurisdictions that pose significant threats. With greater cooperation between governments and industry, individual banks should be able to understand and manage the risks of correspondent banking customers. Under this new AML/CFT "partnership" model, it would be critical to clearly identify the specific roles and expectations of individual banks and governments. Currently, certain jurisdictions are experimenting with "partnership" models that focus on law enforcement and bank collaboration to address specific high-priority crimes. One such example is the United Kingdom's Joint Money Laundering Intelligence Taskforce initiative, which brings various public-private sector organizations together to routinely share AML/CFT intelligence. This collaborative model may prove to be a workable framework for consideration and possible adoption by other jurisdictions, and we encourage policymakers to monitor and review these efforts.

II. Payment transparency is best addressed by focusing on the supervision of originating banks, not through transition to the exclusive use of MT 103 payment messages.

The Clearing House has been a strong proponent of transparency in payment messages. As we noted in our Guiding Principles exposure draft, preventive measures by correspondent banks can be effective only if originator, beneficiary and bank information is clearly apparent on the face of the payment message.[19] The Clearing House is concerned about the lack of clear and realistic guidance on requirements for monitoring payment messages for completeness and meaningfulness and for appropriate use of MT 202 COVs for cover payments. Further, we believe it is important to acknowledge that if the banks that are sending payments have the intent to engage in deceptive practices, it can be almost impossible for correspondent banks to detect, whether the message is in the form of a MT 103 or a MT 202 COV. In this regard, government cooperation in "setting and enforcing international standards for anti-money laundering and transparency in the financial system,"[20] particularly with

---

[19] The Clearing House, *Exposure Draft of Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking* (Sept. 2014), at 5.

[20] *Id.*

respect to originating institutions, is critical to strengthening the ability of correspondent banks to detect and report potential money laundering.

A. The MT 202 COV is a superior payment message format for certain types of transactions, and eliminating and replacing it with the MT 103 would not prevent the transmission of "meaningless" information in payment messages.

MT 202 COVs offer several advantages over MT 103s and are preferred by bank clients in certain scenarios. These advantages include principal being protected, greater speed and lower cost than MT 103s. In fact, regulators in the United States require the use of MT 202 COVs for certain types of payments.[21]

Banks invested considerable time and resources into the development of the MT 202 COV format in 2009, and the future success of the new message format depends no longer on overcoming technological hurdles regarding the use of the form but rather the international implementation and oversight of the use of the message type. A bank that deliberately chooses to use a MT 202 instead of a MT 202 COV in order to avoid including additional information about a transaction likely would be no more "honest" about a transaction when using a MT 103. The problem, therefore, is with the users—and the lack of sufficient supervision in originating jurisdictions of users—rather than the MT 202 COV message type itself. We want to emphasize the importance of enforcement, in originating jurisdictions, of public and private sector expectations for use of MT 202 COVs for cover payments, including the provision of complete and meaningful information to enable intermediary banks to monitor such transactions. It is nearly impossible for an intermediary bank to confirm these facts for a given transaction on its own.

B. Banks' monitoring and reporting obligations with respect to missing or "meaningless" information in payment messages is unclear and must be clarified.

Existing guidance on this type of monitoring is unclear and does not recognize the significant challenges banks may face in attempting to detect the absence of important information or the presence of "meaningless" information. Rather than seek to clarify this point, the Report appears to assume the answer is to use MT 103s for all customer payments based on the premise that:

> [w]hen using the MT 103 in the serial method, the risk that a bank is unaware of missing information does not arise because all relevant information is included in the MT 103. If some information is missing, this will be obvious to every involved bank as not all fields in the message will be completed with the required information.[22]

The Clearing House does not agree with this premise. Although it may be possible to determine whether a required field in a MT 103 payment message is not populated at all (as it will be rejected by

---

21 *See* FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual (2014), *available at* https://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_print.htm, at 209-210.

22 Proposal at 27.

SWIFT), it is a completely different exercise to seek to determine whether the information in the originator and beneficiary fields is meaningful (or accurate).

Guidance released by the U.S. banking regulators in 2009 indicates that intermediary banks should monitor funds transferred through their automated systems to identify suspicious activity.[23] The U.S. guidance indicates that intermediary banks should have policies to address circumstances where information provided in a field or fields is "manifestly meaningless or incomplete."[24] The BIS has previously stated that intermediary banks should have "reasonable policies in place to ensure . . . that required originator and beneficiary fields of cross border cover payment messages are not blank" and when such fields are blank, to take "appropriate measures."[25] The BIS guidance indicates that when fields are manifestly meaningless or incomplete, an intermediary bank should (a) contact the originator's bank or a preceding cover intermediary bank to clarify or complete the information, (b) consider whether to terminate the correspondent banking relationship with the respondent bank or preceding intermediary bank if there is a pattern of inadequate information provided, and/or (c) file a suspicious activity report with local authorities when such a filing is warranted under local reporting requirements.[26]

In neither instance, however, do the regulators provide intermediary banks with guidance on what actual steps they are expected to take to determine whether information is meaningful and whether those steps are realistic. Nor do we think it would be possible to develop practical ways to identify "meaningless" or inaccurate data, given the limited information that correspondent banks receive and the fact that no bank in a correspondent transaction has perfect knowledge of all parties or the purpose of a transaction. Accordingly, we respectfully submit that any discussion about ensuring the transparency and accuracy of information flowing through the global payment system, including the effective use of SWIFT message types, must recognize the responsibilities and supervision of originating and beneficiary banks as compared to intermediary banks. Originating banks by definition are in the best position to ensure that payment messages properly reflect the identity of a payment originator. Likewise, beneficiary banks are in the best position to know whether a payment message accurately identifies the beneficiary.

III. <u>The approach in the Report to correspondent banks' KYCC obligations confuses correspondent banks' efforts to obtain information about their customers' customers in the context of monitoring for suspicious activity with KYC done at onboarding.</u>

Under U.S. guidance, intermediary banks generally are not expected to conduct due diligence on the customers of an originator's bank or a beneficiary's bank; instead, they can rely on the

---

23 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and National Credit Union Administration, *Transparency and Compliance for U.S. Banking Organizations Conducting Cross-Border Funds Transfers* (Dec. 2009), at 3. Such monitoring may occur after the transfers are processed.

24 *Id.* (citing BIS, *Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers* (May 2009)), at 15.

25 BIS, *Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers* (May 2009), at 7.

26 *Id.* at 7-8.

due diligence of the originator's and beneficiary's banks.[27] This guidance is reasonable because the intermediary bank is not in a good position to gather such information. Under the prevailing guidance, as part of the onboarding of a new bank client with which it will have a corresponding banking relationship, an intermediary bank is expected to perform due diligence on the respondent bank, including to determine whether the correspondent account will be used to execute transactions for other banks and whether the client bank's AML/CFT procedures and controls are adequate to detect and prevent money laundering by its clients.[28]

Once a respondent bank has been onboarded, the intermediary bank has an ongoing obligation to monitor transactions processed through the respondent bank's correspondent account for suspicious activity. Suspect alerts might require further investigation by the intermediary bank's compliance department. Similarly, correspondent banks may need information regarding a party to a payment if there is a sanctions screening alert. Prevailing market practice typically would only require the intermediary bank to inquire of the originator's bank or precedent intermediary bank if it believed there may be suspicious activity or a sanctions obligation involving the underlying originator or beneficiary.

The Report recognizes this but goes further to provide that in the case of higher risk respondent banks, a correspondent bank may also have the obligation to do "due diligence" on the customers of its respondent bank.[29] We believe such a mandate would go beyond the current expectations of regulators and published guidance, and put an unfair and likely unmanageable burden on the correspondent bank, given that correspondent banks generally have "limited or no understanding of the originator or beneficiary, their ordinary account activity or the purpose of the payment" and therefore are not in a suitable position to assess the AML/CFT risks of a particular underlying customer or transaction.[30] We recognize the responsibilities of the correspondent bank to evaluate the risks of its respondent bank customers and in appropriate circumstances to request information on any other banks for which the respondent provides correspondent banking services through its account. This is a far cry, however, from a requirement to do a full onboarding due diligence review on any or each of a correspondent bank's customers' customers. Indeed, KYCC as an onboarding concept has repeatedly been rejected as a regulatory expectation. In a recent address, FinCEN Director Jennifer Shasky Calvery stated, "Understanding a customers' customer base is one thing, but knowing a customers' customer is another, and we have repeatedly confirmed that the latter is not an obligation under the BSA."[31] Any discussion of this issue should recognize the distinctions between requirements for onboarding due diligence and requests for information in the context of suspicious activity monitoring or sanctions alerts.

---

27 The Clearing House, *Exposure Draft of Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking* (Sept. 2014), at 6.

28 *Id.* at 10.

29 *See* Report at 18-20.

30 The Clearing House, *Exposure Draft of Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking* (Sept. 2014), at 6.

31 *See* Remarks of FinCEN Director Jennifer Shasky Calvery Remarks at the American Bankers Association/ American Bar Association Money Laundering Enforcement Conference (Nov. 16, 2015), *available at* https://www.fincen.gov/news_room/speech/html/20151116.html.

IV. While further development of information-sharing tools may be helpful, a more meaningful approach to reducing due diligence costs is permitting correspondents to more fully rely on the supervision of their respondents and information provided by utilities.

The Clearing House supports the development of information-sharing platforms, which may lower CDD costs incrementally for banks with respect to correspondent banking. The Report notes data collection, validation and sharing utilities that are available today. The Clearing House agrees that it would be useful for an independent entity to develop common standards for systems and controls that these utilities should use to ensure the accuracy of their information as well as a common set of KYC data that all utilities would hold, recognizing that this common set should serve only as a baseline and that certain jurisdictions or market segments will require additional information. It would also be useful if data within utilities could be provided through a direct data feed that banks could embed into their systems. Similarly, we also believe there is some efficiency to be gained through standardized correspondent bank KYC questionnaires, subject to the same understanding as above that this would serve as a baseline and that additional jurisdictional and market segment data likely would be needed.

However useful such information sharing tools may be, we think those tools are unlikely to materially reduce the cost of KYC compliance for correspondent banks, absent a change in regulatory expectations. This is because individual banks currently are required to maintain their own systems and programs to detect, prevent and report activity related to AML/CFT concerns, which limits the extent to which banks can ultimately benefit from these initiatives. These utilities' usefulness is further restricted by jurisdiction-specific privacy laws, which may prevent the sharing of information from an originating bank to a receiving bank.

Because of these limitations, a more productive and effective way to reduce initial onboarding costs and ongoing due diligence would be to permit banks to rely upon evaluations performed by other qualified entities, such as home country regulators, that a respondent bank has adequate AML/CFT controls in place. As the Financial Stability Board notes, "the more local authorities build trust in the AML/CFT frameworks and the quality of their supervision, the more foreign correspondents will be able to rely on the information they provide without multiplying costly due diligence and checks."[32] However, we observe that the inability to rely upon the supervision of a respondent bank's AML/CFT program also is occurring in the domestic market in the United States, which we are concerned may lead to reductions in correspondent banking services to U.S. depository institutions. In this respect, we also stress that it is important that permitting the type of reliance we propose is incorporated not only into governmental policy and regulation, but also supervisory practice. This is especially key in jurisdictions, such as the United States, where responsibility for AML/CFT regulation and supervision, respectively, is divided among different agencies with substantially different missions and approaches.

Finally, we agree that Legal Entity Identifiers ("**LEIs**") merit further consideration as a means of identifying banks and corporate entities for AML/CFT purposes. While we concur with the assessment that bank identifier codes currently are the cornerstone of the global payments network as the mechanism for message routing and as an account identifier, it is important to recognize that LEIs are the more reliable tool to unambiguously identify parties to financial transactions. As a result, both

---

[32] FSB Report at 9.

need to be considered as part of any complete solution. It would be helpful to consider the creation of a mapping facility to allow for the easy mapping of routing information in payment messages to the relevant LEI. We also note that some messaging systems currently are exploring the inclusion of the LEI in their messages, for example, ISO 15022 category 5 messages for securities activity. It is expected that further discussion around the inclusion of LEIs in payments systems for entity and account identification will evolve over time as the value of this global standard continues to evolve.

V. Conclusion.

The Clearing House shares the concerns of the CPMI with respect to the trends in correspondent banking and believes that certain of the initiatives discussed in the Report—including KYC utilities and other information-sharing tools—may have potential to enhance correspondent banks' efforts to combat money laundering while also helping "to ensure an efficient provision of cross-border payment services globally."[33] However, technical measures are not enough to address the complex incentives driving the "de-risking" phenomenon, and we encourage broader efforts between the public and private sector to clarify the roles and responsibilities of the various stakeholders for detecting, reporting and preventing money laundering through the global correspondent banking network.

* * *

We would welcome the opportunity to provide you with any assistance or input that you might find helpful. Should you have any questions or need further information about any of the matters discussed in this letter, please do not hesitate to contact me at (202) 649-4622 or *jeremy.newell@theclearinghouse.org*.

Respectfully submitted,

Jeremy R. Newell

Jeremy R. Newell
General Counsel
The Clearing House Association L.L.C.

---

[33] *Id.* at 4.

cc:

Board of Governors of the Federal Reserve System
Michael Gibson
Director, Division of Banking Supervision and Regulation
Michael Solomon
Associate Director, Division of Banking Supervision and Regulation
Suzanne Williams
Associate Director, Division of Banking Supervision and Regulation
Koko Ives
Manager, Bank Secrecy Act / Anti-Money Laundering Section

U.S. Department of the Treasury
Adam J. Szubin
Acting Under Secretary for Terrorism and Financial Intelligence
Daniel L. Glaser
Assistant Secretary for Terrorist Financing
Sarah K. Runge
Director of the Office of Strategic Policy for Terrorist Financing and Financial Crimes
Jennifer Shasky Calvery
Director, Financial Crimes Enforcement Network
Jamal L. El-Hindi
Deputy Director, Financial Crimes Enforcement Network

Office of the Comptroller of the Currency
Martin Pfinsgraff
Senior Deputy Comptroller for Large Bank Supervision
Jennifer C. Kelly
Senior Deputy Comptroller for Bank Supervision Policy and Chief National Bank Examiner
Daniel P. Stipano
Deputy Chief Counsel

Federal Deposit Insurance Corporation
Doreen Eberley
Director, Division of Risk Management Supervision
Lisa Arquette
Associate Director, Division of Risk Management Supervision

The Financial Action Task Force
Valeria Schilling
Senior Policy Analyst