To:

4 February 2022

Raymond Chan
Executive Director, Banking Supervision
Hong Kong Monetary Authority

ASIFMA/GFMA/BPI/IIF response to HKMA Consultation on Operational Resilience, Operational Risk Management and Business Continuity Planning

Dear,

The Asia Securities and Financial Markets Association (ASIFMA[i]), the Global Financial Markets Association (GFMA[ii]), the Institute of International Finance (IIF[iii]) and the Bank Policy Institute (BPI[iv]) (collectively 'the Associations') welcome the opportunity to respond to HKMA's new draft SPM module OR-2 on Operational Resilience, revisions to SPM module TM-G-2 on Business Continuity Planning and SPM module OR-1 on Operational Risk Management ('Proposals'). The Associations recognise that these Proposals have been drafted and revised to more closely align with the Basel Committee on Banking Supervision ('BCBS') Principles for Operational Resilience[1] and the BCBS Revisions to the Principles for the Sound Management of Operational Risk[2].

The GFMA, IIF and BPI have been closely engaged with global standard setters and regulators on operational resilience for nearly four years working with our financial institution members through a joint Operational Resilience Steering Committee. Whilst ASIFMA has held the pen of this response which is substantially based on feedback from the Hong Kong ('HK')-based membership, the response also benefited from review and input from members of the GFMA/IIF/BPI Steering Committee so as to provide the HKMA with both local and international input in a single response.

Operational resilience is extremely important for the public and private sectors to maintain confidence in the financial industry and to support financial stability and economic growth. The Associations and their members acknowledge the importance of operational resilience for individual institutions, and across the financial sector, in support of customers, markets and the communities and broader economies they support nationally and globally. In support of this goal, our members recognise and appreciate the global

[1] The BCBS Principles for Operational Resilience (March 2021) can be found at: https://www.bis.org/bcbs/publ/d516.pdf

[2] The BCBS Revisions to the Principles for the Sound Management of Operational Risk (March 2021) can be found at: https://www.bis.org/bcbs/publ/d515.pdf

coordination and alignment among policymakers and financial authorities on policy outcomes, terminology, and supervisory approaches.

The potential for fragmentation due to divergences in regulatory standards and supervisory oversight poses substantial risks and operational challenges for financial services firms that operate globally and, in turn, for the strength of the financial system. We therefore fully support and appreciate how the HKMA is closely aligning its proposed approach to that of the BCBS. We also support the development of a standalone SPM module on operational resilience to enhance the HKMA's existing guidance in support of a holistic, forward-looking approach to the resilience of Authorised Institutions ('AIs'), whilst at the same time leveraging and linking to relevant existing guidance.

The bulk of our feedback is in relation to the new draft SPM OR-2, and is outlined in section I of the below response. We also have more limited feedback in relation to the revisions to SPM module TM-G-2 and SPM module OR-1 which are provided in sections II and III respectively.

I. Feedback on draft new SPM on Operational Resilience (SPM OR-2)

Whilst we are generally supportive of the approach and agree on most key concepts in the draft SPM OR-2, there are a few areas where further refinement might strengthen the framework. In what follows, we share our feedback which is mainly centred around the need for clarity on some of the concepts, the Board and Senior Management roles and the need for an extended implementation timeline. Specifically:

- Terminology and Concepts: We seek confirmation that HKMA's 'critical operations' (in the context of Operational Resilience) and 'Tolerance for disruption' are interchangeable with 'Important Business Services' and 'Impact Tolerance' respectively which are terms being used by other regulators (e.g. UK Financial Sector Authorities' Operational Resilience rules);
- Ability of AIs to adopt global operational resilience frameworks;
- Greater clarity and consistency in relation to the discussion of Board and Senior Management responsibilities; and
- Timelines for implementation.

The following sections will provide additional detail on these points and make recommendations to strengthen the framework.

1. Operational resilience concepts

We have some suggestions and questions in relation to some of the concepts and definitions, which would increase clarity for implementation and lead to further international alignment:

- **1.3 Tolerance for disruption:**
    - Operational resilience is an outcome that benefits from the effective management of operational risk. Therefore, operational resilience and operational risk management are linked but are two different concepts. Broadly, operational risk management defines risk

tolerance/appetite as the maximum level of risk that a financial institution is willing to accept. Further, the Proposals define tolerance for disruption as, '*the maximum level of disruption to a critical operation that an AI can accept and is in practice the point after which further disruption would pose risks to the viability of the AI or impact its role within the Hong Kong financial system'*. The level of risk that an AI is willing to accept is, in most cases, lower than the risk that would impact the viability of the institution or cause a material impact to the financial markets.

- We also commend the HKMA for aligning its terms to the BCBS Principles for Operational Resilience. Aligning terminology fosters regulatory harmonisation and a consistent implementation of operational resilience principles and furthers the goals of extending operational resilience across geographies. As stated in the draft, tolerance for disruption is currently defined as, '*the maximum level of disruption to a critical operation that an AI can accept, and is in practice the point after which further disruption would pose risks to the viability of the AI or impact its role within the Hong Kong financial system.*' Whilst this definition is similar to the definition of "tolerance for disruption" of the BCBS[3], there are a few instances within the Proposals where the concepts of risk and resilience could be confused. As HKMA recognises that risk and resilience are different concepts, we suggest that it may be helpful for HKMA to remove the phrase *'the maximum level of disruption to a critical operation that an AI can accept'* in relation to tolerance for disruption. This would further differentiate the risk and resilience concepts given that a bank is typically expected to accept risk and the level of risks that a bank is prepared to accept is often less than what it can actually tolerate. We also note that the HKMA includes in the current definition of tolerance for disruption materiality when discussing viability of the AI but not in terms of the impact on the HK financial system. To bring further alignment of this term with the BCBS Principles for Operational Resilience and the UK Authorities Impact Tolerance, we recommend that the definition be edited to read, '*HKMA describes "tolerance for disruption" as being the point after which further disruption to the critical operation would pose risks to the viability of the AI or threaten the stability of the Hong Kong financial system*'. This reflects the fact that tolerance is not something that a bank is willing to accept, but rather is what a bank can tolerate (before becoming insolvent) or what the HK financial system can tolerate (before financial instability). This definition would allow HKMA to remain aligned with the BCBS principles, and at the same time benefit from the experience the industry has been gathered from applying the BCBS and other principles.

- **1.3 Critical operation:**
  - We suggest the term (and scope of the guidance on) "critical operation" would benefit from further clarity and narrower scoping. In some paragraphs (such as 1.3 and 4.1.3.) in the draft SPM-OR2 it can be interpreted that HKMA is referring to Recovery and Resolution Planning

[3] the level of disruption from any type of operational risk a bank is willing to accept given a range of severe but plausible scenarios

('RRP')-type operations only, but in other paragraphs it reads to be broader than that. For example, paragraph 4.1.2 on 'Identifying critical operations' includes '*For the avoidance of doubt, while the set of criteria defined by AIs for identifying critical operations should encompass elements of both (a) and (b) above, a given operation need not impact both (a) and (b) in order for it to be classified as a critical operation*.' This opens the definition to wide interpretation. Harmonisation and alignment with RRP is relevant but it would be useful for firms to have flexibility to determine to what extent this harmonisation should be done, and what to do in cases where a critical operation is identified for operational resilience, but not for resolution planning, given that the underlying policy drivers for each are based on different scenarios and assumptions.

- We are pleased to see that HKMA's definition of critical operations has many similarities with that of other regulators. We do note however that – as compared to other regulatory bodies - the definition makes relatively limited mention of end users / customers. We suggest HKMA clarifies the extent to which the impact on customers is to be considered when determining critical operations.
- We would be grateful if the HKMA can confirm that HKMA's "critical operations" is interchangeable with "Important Business Services" which is being used by other regulators (e.g. UK Financial Sector Authorities' Operational Resilience rules).
- We also hope it can be further clarified that the criticality pertains to the HK jurisdiction only (vs. a reference to other jurisdictions). The United States Joint Agencies' Sound Practices to Strengthen Operational Resilience[4] make this clarification.
- We note that the HKMA includes in the current definition of critical operations "material" when discussing viability of the AI but not in terms of the impact on the HK financial system ('*…which if disrupted, could pose material risks to the viability of the AI itself or impact the AI's role within the Hong Kong financial system'.* We suggest rephrasing to '*…which if disrupted, could pose material risks to the viability of the AI itself or threaten the stability of the Hong Kong financial system*'.

2. Operational resilience framework

- Many of the Associations' members are international firms operating in multiple jurisdictions and subject to operational resilience requirements in several of these. It is key for international banks to be able to implement a scalable and consistent global framework. We hope that the HKMA will allow AIs to adopt global frameworks that have been instituted at Group level as long as it enables the AI's HK operations to comply with the SPMs. We encourage the HKMA to include in the final SPM a statement reflecting the BCBS Operational Resilience Principles which read: '*The Committee recognises that many banks have well-established risk management processes that are appropriate for their individual risk profile, operational structure, corporate governance and culture, and conform*

[4] The US Interagency Sounds Practices to Strengthening Operational Resilience (2020) at: https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf. Page 2 contains this clarification.

to the specific risk management requirements of their jurisdictions.' Leveraging global frameworks will support coordinated and effective efforts across jurisdictions and enhance AIs' operational resilience capabilities.

- Further, Paragraph 2.2 refers to the importance of operational resilience for an AI to operate smoothly. Operational resilience allows for an AI to rapidly restore operations in the face of extreme but plausible disruptive events. These events impede the smooth operating of the business' operations. Therefore, we recommend that '*operate smoothly'* be removed from the text and replaced with '*rapidly and safely recover'*. The language would read, '*Given the importance of operational resilience for an AI to rapidly and safely recover and remain viable under extreme scenarios…*'
- Diagram 1: *Step-by-step approach to developing a holistic operational resilience framework on Operational Resilience Framework* (Paragraph 2.4): we submit that the steps to develop an operational resilience framework are best left to the AI's discretion, based on their nature, scale, set-up etc.

3. Role of the Board and senior management

We wish to clarify the role of an AI's local Hong Kong Board and Senior Management. We appreciate that the draft SPM-OR2 seeks to provide greater guidance around the responsibilities of the Board and Senior Management. However, some of the language in the guidance as drafted shifts the Board responsibilities away from oversight and into day-to-day managerial responsibilities. We encourage the HKMA to consider a more proportionate approach with a more balanced allocation of responsibilities between the Senior Management and the Board, and align to the language used in 4.2.1 of SPM OR-1 for Board oversight of operational risk…*'the Board, (or its delegated committee)'.*

Some specific practical areas of concern in the current draft are as follows:

- Paragraph 3.1 reads, '…[w]*hen formulating the framework, the Board should take into consideration the AI's risk appetite*.'
    - This could be read to insinuate that the Board is responsible for the development of the operational resilience framework instead of providing assurance that a framework exists and that it is appropriate for the risk profile of the organisation. Furthermore, it is Senior Management's role to set the risk appetite. The Board is accountable for understanding how the risk appetite was set by senior management. Separately, risk appetite, in general, is managed through the AI's operational risk management function. While operational risk management supports operational resilience, it is a separate concept from operational resilience.
    - We would also like to seek further clarification on how HKMA expects a global firm, with a Hong Kong branch, to delineate activities between the (Global) Board and the Hong Kong Senior Management. By way of example, where a global firm has a global framework, the

(Global) Board would typically provide oversight of the operational resilience framework, but regional implementation would be a responsibility of the regional Senior Management.

- We note that in the SPM TM-G-2, the HKMA refers to the Chief Executive whilst the draft SPM OR-2 and draft revised SPM OR-1 refer to Board and Senior Management responsibilities (subject to clarification of the above and below points). We submit that for better alignment between the three SPMs, there should be consistent terminology.
- Paragraph 3.3 (a) reads, *'…Board is responsible for setting the tolerance for disruption'*. We recommend that Senior Management is responsible for developing a process for setting the tolerance for disruption and defining these measures. The tolerance for disruption and the supporting processes and functions used to manage this tolerance are best understood at this level. As part of its oversight, the Board should understand the process taken by Senior Management to set the tolerance for disruption, challenge the process as necessary, and approve the tolerance for disruption for critical operations.
- Paragraph 3.3 (b) reads, '[S]*enior management should identify and the Board should approve the severe but plausible scenarios which will be used to review whether an AI is operationally resilient*.' We recommend that Senior Management should develop severe but plausible scenarios and use these scenarios to determine if the AI is operationally resilient. The Board, as an oversight function, should understand the process used by the AI to develop severe but plausible scenarios and provide effective challenge to that process. The Board should not be placed in a position to approve severe but plausible scenarios because they will not have visibility into the detailed operational impacts that may be necessary to conduct this function.
- Paragraph 3.4 reads, '[T]*he Board bears ultimate responsibility for ensuring that an AI remains operationally resilient.'*
    - We recommend that Senior Management is ultimately responsible for ensuring operational resilience. The Board should be accountable for oversight of the operational resilience framework and program which means understanding how the AI developed the framework, scenarios for testing the performance of business operations under extreme but plausible events, tolerance for disruption and critical function determination.
    - Further, Senior Management should identify and prioritise deficiencies in the delivery of operational resilience and provide this information to the Board. The Board should challenge this prioritisation, but they should not be responsible for setting the order in which deficiencies should be addressed.
- Paragraph 3.6 reads, '[T]*he Board should play an active role in establishing a broad understanding of the AI's operational resilience framework. It should clearly communicate the objectives of the framework to all relevant parties, including staff, intragroup entities, and third parties. Regular training on the AIs operational resilience framework should be provided to these parties to reinforce their understanding*.'
    - We agree with the statement in Paragraph 3.6 that the Board should have a broad understanding of the AI's operational framework which is why we suggest they should not be responsible for some of the aspects of the operational resilience framework as

mentioned above (e.g., tolerance for disruption, issue prioritisation) that requires a more granular understanding of business operations.

- Conversely, Paragraph 3.6 also reads that it is the role of the Board to communicate the objectives of the framework as needed to all relevant parties once the objectives have been agreed. We suggest it should not be the responsibility of the Board to communicate to an AI's third parties or staff, but that the responsibility should sit with the Senior Management instead.

5. Mapping interconnections and interdependencies underlying critical operations

- The draft SPM OR-2 also aligns with the BCBS Principles for Operational Resilience by requiring the mapping of interconnections and interdependencies. For many large AIs, this mapping may require a significant effort and investment. To this end, it is important that any mapping exercise be appropriately scoped based on the size, complexity, and interconnectedness of the AI.
- Paragraph 5.4 states '*AIs are expected to update their mapping documentation on a regular basis, but no less than annually or following any material changes to their operations.*' We suggest this should be a review, which is performed annually and/or following change, with updates only taking place where the review identifies that an update is required.

6. Preparing for and managing risks to critical operations delivery

- Paragraph 6.2 Third party dependency management reads: '*Prior to entering into arrangements that support the delivery of critical operations, an AI should verify whether the relevant third parties or intragroup entities have at least equivalent level of operational resilience to that of the AI.'*
  - We suggest that "verify" be replaced by "ascertain".
  - Intra-group services are subject to well-controlled and globally consistent AI policies and processes, and those intra-group services which are compliant with recovery and resolution and ring-fencing rules have already met the intended outcomes of several third-party risk management requirements, including those around exit, business continuity planning, and sub-contracting. Unlike external third parties which sit outside the institutional protection scheme and provide a limited and specific set of service (e.g., ICT providers), AIs use intragroup relationships to provide numerous technology and technology-based services which include but are not limited to risk management (e.g., third-party, cyber, operational), compliance, human resources, finance and technology (e.g. server maintenance / support, file sharing / distribution, email, internet/web services, network administration, storage). Therefore, requiring AIs to develop exit strategies for this wide range of intragroup services (especially technology services) may create a ripple effect by rendering other intra-group services ineffective. For example, the novation of the technology intra-group relationship may impact the ability of the parent organisation to provide information/cyber risk, finance,

and HR services. This separation would at best require AIs to significantly alter these agreements or worse, it would require the novation of numerous intra-group agreements.

- Further, the probability of an affiliate novating numerous intra-group services by (1) having those services provided externally or (2) by hiring numerous individuals and purchasing systems to provide these services internal to the legal entity is remote. In both instances, the associated costs make these solutions cost-prohibitive. Second, each solution decreases the AI's operational resilience due to:
  1. Multiple Governance Models: in the first instance, the risk governance and oversight would be split across numerous third parties which may use different risk and resilience frameworks. This increases the risk governance complexity and decreases visibility into the AI's risk and results in decreased operational resilience.
  2. Technology Complexity: in both scenarios, the technology used to implement the security architecture may differ (e.g., the AI may select technology products with less functionality based on their size). This increases the technology complexity which may decrease resilience and the effectiveness of resilience strategies.
- AIs often use the parent organisation to provide services that are required across the organisation. This maximizes resource usage, creates consistent governance and framework implementation, and provides sophisticated services (e.g., threat intelligence, red teaming) that may otherwise not be available if the legal entity was a standalone entity. We therefore suggest intra-group services should be excluded from the requirement to develop exit strategies.
- We agree with the HKMA that requirements for third parties should be treated in proportion to the nature, complexity and criticality/materiality of the services provided. That stated, AIs should be allowed time to work with third parties where operational resilience controls are not aligned to the third party's size, complexity, and market interconnectedness to raise their preparedness in this area. We also agree with the HKMA that AIs should consider and prepare for (where possible) extreme scenarios where the third party is unable to provide its services.
- We suggest that HKMA works with standard setters (e.g., FSB, BCBS) or encourages the Hong Kong Association of Banks to develop expectations that increase the assurance that critical third parties adhere to the Operational Risk and Operational Resilience requirements.
- While we agree that exit strategies are appropriate for material third-party relationships, we request clarity that exit strategies are not for use when experiencing a disruption. Exiting services in these scenarios may exacerbate the event and further disrupt services or create new disruptions for other unaffected business areas.

9.1. Application

Paragraph 9.1. reads *'…locally incorporated AIs should endeavour to implement the guidance of this module with respect to their subsidiaries and overseas operations, and for overseas incorporated AIs with respect to*

their operations in Hong Kong'. As currently drafted, this could be interpreted in a number of ways and could refer to:

1. HK territory and HK financial stability focused: i.e. for international third country banks, all their subsidiaries and branches in HK only – not including subsidiaries and branches of their HK subsidiaries in other countries; or
2. HK territory and HK financial stability, including where operations in other countries would affect that – which would be the same as 1. But with the additional requirement to look at intragroup interdependencies; or
3. Wider scope of application: HK banks (including HK subsidiaries of foreign banks) and all their subsidiaries and branches in third countries.

We hope that the scope is intended to cover either case 1. or 2. above, but that the wider scope referenced in case 3. is excluded. It would be helpful for the HKMA to confirm this in the final text.

We are concerned that the Proposals would require a single legal entity in one jurisdiction to apply both home country regulations and host country regulations. For example, there could be a scenario in which a US bank's Japanese subsidiary is a subsidiary of the US bank's subsidiary in HK. In this a scenario, it would be helpful for the HKMA to avoid a situation in which US, HK and any Japan rules apply to that Japanese subsidiary with their differing timelines and expectations.

9.2 Timeline for implementation

On the basis of practical experience implementing the BCBS Operational Resilience principles in other jurisdictions, we submit that the HKMA "1+2" years implementation timeline is considerably more demanding for global firms compared to other jurisdiction's (e.g. UK) "1+3" years.

Even with a mature framework available for imminent roll-out, we submit that it will require 3 years to:

- Define local critical operations;
- Set tolerance for disruptions and map interconnectedness and interdependencies;
- Validate solutions to help meet tolerances (and apply lessons learned) and ensure proper governance and due diligence for investments, implementing solutions, testing and deploying.

We recommend balancing the need for firms to take action now with the time required to drive cultural change towards resilience, and therefore suggest the HKMA considers a 1+3 years implementation timeframe.

II. Feedback on amendments to SPM OR-1 on Operational Risk Management

Section 5.4.4. states '*As appropriate, the CORF – corporate operational risk management function- should assess and propose control measures to manage the operational risk inherent in the third line of defence'.*

- The expectation that the second line of defence (as that is where the CORF sits) is assessing the operational risk in the third line of defence is not in the PSMOR and is a departure from industry practice. Further clarification on what is required here would be helpful.

III. Feedback on amendments to TM-G-2 on Business Continuity Planning

- We note that the term "critical operations" was replaced by "critical services", assumingly in line with BCBS terminology. We would be grateful if the HKMA can confirm whether this has any impact on the scope of the SPM TM-G-2.
- Paragraph 1.2.4: the use of '*may find it useful*' suggests this to be optional. We would welcome clarification if that is the case. Creating and maintaining two types of plans is not practical, e.g. a list of 'additional premises' suppliers would not help to get the office space with no contract in the first place.
- Paragraph 1.2.5: we acknowledge that certain data may be required, but specific plans should not be included in BCPs. Any data required should be stored within appropriately secure systems.
- Paragraph 2.2.3: we suggest that the Chief Executive of AIs may delegate or assign a designated team or person to prepare the annual statement for review and sign-off of by the Chief Executive.
- Paragraph 6.1.1: testing against severe but plausible scenarios is required for operational resilience and it is unclear how this would be different. We suggest further clarity is needed on the differentiation between the two capabilities.
- Paragraph 6.1.2 reads that '*AIs are expected to conduct testing of their BCP at least annually*'. This is not in line with Paragraph 7.2 of the Draft SPM OR-2 which reads '*The frequency of testing should be determined based on a variety of factors, including the potential impact of a disruption, how many critical operations an AI has, and whether the operating environment has materially changed*.' We agree with Paragraph 6.1.2 of TM-G-2 and suggest that the AI should be allowed to decide on the frequency of testing depending on their own facts and circumstances and we hope that this can be reflected in Paragraph 6.1.2 and aligned with Paragraph 7.2 of the Draft SPM OR-2.
- Paragraph 6.1.3: We would like to clarify that AIs may determine "major components" in their own circumstances. We would also like to suggest HKMA to name a few consideration factors as examples which may be helpful for AIs to determine the major components.
- Paragraph 6.1.4 on formal testing documentation: we suggest the language and requirements be aligned with Paragraph 7.4 of the Draft SPM OR-2.

We are grateful for the opportunity to share our feedback on the Proposals. We hope our suggestions will be reflected in the final SPMs and are more than willing to discuss our response in more detail during a meeting. We remain at your disposal for any questions you might have in relation to the above response.

Best regards,

Laurence Van der Loo

Executive Director, Technology and Operations

ASIFMA

lvanderloo@asifma.org

Martin Boer

Director, Regulatory Affairs

Institute of International Finance

mboer@iif.com

Allison Parent

Executive Director

Global Financial Markets Association

aparent@gfma.org

Brian R. Anderson

Senior Vice President, Technology Regulation

Bank Policy Institute

Brian.Anderson@bpi.com

[i] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, and competitive Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region. More information about ASIFMA can be found at: www.asifma.org.

[ii] GFMA represents the common interests of the world's leading financial and capital market participants to provide a collective voice on matters that support global capital markets. It also advocates on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows to end users. GFMA efficiently connects savers and borrowers, thereby benefiting broader global economic growth. The Association for Financial Markets in Europe (AFME) located in London, Brussels, and Frankfurt; the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong; and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian, and North American members of GFMA.

[iii] The Institute of International Finance is the global association of the financial industry, with more than 450 members from more than 70 countries. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, sovereign wealth funds, hedge funds, central banks and development banks.

[iv] The Bank Policy Institute is a nonpartisan public policy, research, and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost 2 million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.