Via Electronic Mail July 7, 2023

To: Office of Science and Technology Policy
Subject: Response to OSTP RFI: National Priorities for Artificial Intelligence
Docket ID: OSTP-TECH-2023-0007-0001

Executive Summary

The Bank Policy Institute[1], through its technology policy division known as BITS[2], appreciates the opportunity to respond to OSTP's National Priorities for Artificial Intelligence request for information.

The financial services industry recognizes the transformative potential of AI and its capacity to enhance our industry's services, promote economic growth and expand access to financial products and services, improve customer experiences, and bolster the security and integrity of financial transactions.

For decades, the financial services industry has been at the forefront of responsible technological innovation while maintaining the highest standards of trust, safety, security, and customer service. As we evaluate the increasing capabilities of AI and the potential benefits it may provide consumers and the economy more broadly, we bring with us this wealth of experience and a deep understanding of the importance of innovating responsibly.

We are committed to the responsible use and development of AI technologies, underpinned by strong governance, oversight, and risk management. The banking industry's foundational adherence to, and experience with, robust risk management practices, including model risk management, IT risk management, cyber risk management, enterprise risk management, operational risk management and resilience, data security, and privacy, can be effectively leveraged to assist in establishing a framework designed to allow for the responsible use of AI within the financial services sector. A programmatic and

[1] 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.
[2] BITS – Business, Innovation, Technology, and Security – is BPI's technology policy division that provides an executive level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the nation's financial sector.

coordinated risk-based approach, leveraging existing architectures, should be the cornerstone of the national AI strategy.

Existing banking regulations and guidance provide a comprehensive framework to manage the implementation of AI across various banking use cases. Banks are subject to extensive regulatory requirements[3], including how they manage model risk, store and protect sensitive information, ensure consumer privacy, defend against cyberattacks, manage third parties and engage in fair lending. To ensure appropriate compliance and oversight, banks are subject to regular supervision by prudential banking agencies and the CFPB.

Regulations should remain technology-neutral and focus on the activities that take place, rather than the technology itself. New specific regulations in the financial services sector related to AI would be counterproductive given the heterogeneity in which AI is used. AI is simply another technology, and when governed properly, does not pose unique risks that cannot be managed within existing regulations and risk frameworks over the specific activities in which AI is being used. Policymakers should avoid creating a new, prescriptive framework around AI that may prevent the financial industry and its customers from realizing future benefits of AI. Achieving the appropriate balance between regulations and innovation is critical for financial institutions to apply or develop innovative solutions if regulatory burdens become unnecessarily restrictive.

Each industry must be cognizant of unique issues and risks with specific AI applications, and our experience has shown us that these risks are best handled by regulators that already have knowledge and expertise in our industry. We cannot envision any scenario where establishing a distinct regulatory framework or institution, exclusively for AI, could foster an effective system that spans all sectors.

We also believe that it is important to regulate AI outcomes rather than the technology itself. This means that regulators should focus on the potential harms that AI systems can cause, rather than trying to regulate the specific technologies that are used to develop these systems. This approach would allow for more innovation in the AI space, while still protecting consumers and ensuring that AI systems are used in a responsible manner. Generative AI, encompassing Large Language Models (LLMs), should not be treated differently from other cutting-edge technologies during their deployment. The same principles and norms applicable to advanced technologies, which have guided the financial industry through other responsibly implementations, as it has to the adoption of machine learning, should be consistently applied to the use of other models.

For example, the EU AI Act[4] seeks to regulate artificial intelligence; however, the Act has been criticized for being overly prescriptive, which could stifle innovation. For instance, the AI Act consistently calls for increased transparency (explainability) and information about the purpose of the system, which are important elements of any AI system but also the data it uses, and the Act is more prescriptive regarding how the algorithms develop outputs. AI systems are often complex and the benefits and advantages they offer, and how they source and use data to develop sophisticated algorithms is their intended purpose and would be diminished if too prescriptive. The architecture and design of AI generally, and the advantages machine learning can offer can make it difficult to understand at a technical level. Even if developers are able to explain how their AI systems work, it

[3] Office of Management and Budget, Guidance for Regulation of Artificial Intelligence Applications, (Nov. 17, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.
[4] https://artificialintelligenceact.eu/the-act/

may still be more complicated and difficult for users to understand. Mandates that demand inflexible detailed explainability obligations would restrict the use and implementation of new AI advances, stifling innovation. Managing two of the more important concerns of fairness and bias in AI outputs can be achieved through other methods, including soundness practices (robust, independent, and ongoing testing). The EU's AI Act is an inflexible approach that regulates at the potential cost of innovation, which is the very DNA of AI technology. BPI would like to strongly note that the EU AI Act is a prescriptive model that we hope not to follow in the United States.

Explainability: In crafting an overarching national AI strategy, it is imperative that the United States foster an appropriate level of transparency throughout the AI systems and applications. Explainability is instrumental in cultivating trust, comprehension, and the assimilation of AI technologies at the national level. Nonetheless, it is of paramount importance to recognize that explainability is multifaceted and diverges based on the stakeholder. Consequently, it cannot be approached with a rigid blueprint.

Explainability is the ability to understand how an AI/ML[5], model makes its decisions. This is important for several reasons, such as ensuring that the model is making decisions in a fair and unbiased way, identifying and addressing any potential biases in the model, troubleshooting the model if it is not performing as expected, and explaining the model's decisions to users. There is no one-size-fits-all approach to explainability, and the best approach will vary depending on the specific application. The position on explainability is evolving, and it is important to consider the needs of all stakeholders when making decisions about explainability.

It is crucial to distinguish between (1) "explainability" in relation to a regulator's capacity to interpret and assess the AI system's effectiveness, and (2) "explainability" in the context of elucidating to citizens and stakeholders how decisions were made using AI, empowering them to understand and discern the rationale behind these decisions. These two realms of explainability entail distinct practical and policy objectives and considerations that vary according to the AI application. For instance, AI systems that have a direct substantive impact on citizens, such as financial, healthcare, or judicial applications, necessitate a more comprehensive level of external explainability compared to AI applications on a customer service line that helps improve service for routine matters.

It is critical to remember that human involvement is consistently applied in all facets of decision-making and ultimately dictates the usage of AI models or their outputs, including the selection and use of AI models. AI is an auxiliary tool to bolster or inform decision-making, rather than autonomously render decisions devoid of human scrutiny and control. The same approach should be applied to managing explainability risks on a national scale.

Soundness and robustness are two important properties of AI models that can contribute to trust and fairness. Soundness is the ability of a model to make correct predictions in a consistent manner. Robustness refers to the ability of a model to perform well even when it is presented with inputs that are different from the ones it was trained on. Over explaining how an AI model works can sometimes be counterproductive because of the complexity of describing models in a way that is both accurate and

[5] Artificial intelligence (AI) includes a family of technologies capable of performing tasks that traditionally would have required human cognitive intelligence, such as thinking and decision-making. Machine learning (ML) is a subset of AI that generally refers to the ability of a software algorithm to identify patterns and automatically optimize and refine performance from processing large data sets.

understandable. Practices and outputs that ensure soundness and robustness and which are examined and addressed by humans, can help identify and rectify biased or uneven outcomes in AI results.

The financial services industry is committed to engaging in an open and constructive dialogue with all relevant stakeholders, including regulators, policymakers, customers, employees, and the public. We believe that through an inclusive dialogue we can leverage the strengths of AI, while also addressing the implications and challenges it poses. We look forward to contributing to the National AI Strategy and to continuing to serve our customers and society in this new era of AI.

Protecting Rights, Safety, and National Security

The financial services industry with its long-standing commitment to consumer protection, safety, and national security, recognizes the importance of a comprehensive approach to risk management in the context of AI. As we navigate the transformative landscape of artificial intelligence, we are acutely aware of the multifaceted risks it presents. Given the inherent interdependencies of various processes and activities within the banking industry, these risks cannot be siloed into a single program or department; they demand a coordinated, cross-functional approach that leverages the industry's current robust risk management paradigm.

In response to questions 1,2 & 3:

1. "What specific measures – such as standards, regulations, investments, and improved trust and safety practices – are needed to ensure that AI systems are designed, developed, and deployed in a manner that protects people's rights and safety? Which specific entities should develop and implement these measures?"
2. "How can the principles and practices for identifying and mitigating risks from AI, as outlined in the Blueprint for an AI Bill of Rights and the AI Risk Management Framework, be leveraged most effectively to tackle harms posed by the development and use of specific types of AI systems, such as large language models?"
3. "Are there forms of voluntary or mandatory oversight of AI systems that would help mitigate risk? Can inspiration be drawn from analogous or instructive models of risk management in other sectors, such as laws and policies that promote oversight through registration, incentives, certification, or licensing?"

BITS members and affiliates support a principles-based approach to governing the use of AI in the financial services sector over a prescriptive one. We firmly believe that this approach, when applied judiciously, can provide a robust framework for managing the advantages and potential harms posed by the development and use of AI systems, including large language models.

A principles-based approach offers the flexibility and adaptability necessary to realize the benefits to AI and to manage the dynamic and evolving risks associated with AI technologies. It allows institutions to define appropriate decisions within their risk appetite and tolerance level, thereby enabling them to effectively manage the unique risks associated with their specific AI systems and applications. The banking industry is well-positioned to leverage its established governance, oversight, and risk management approach, which has been instrumental and effective in managing significant risks over time.

Leveraging the AI Bill of Rights and AI Risk Management Framework: The principles and practices for identifying and mitigating risks from AI, as outlined in the Blueprint for an AI Bill of Rights and the AI Risk Management Framework, provide a robust foundation for tackling potential harms.

In this context, we endorse the National Institute of Standards and Technology's (NIST) Artificial Intelligence Risk Management Framework (AI RMF). This voluntary framework, crafted by a leading standards-setting U.S. governmental body, offers a comprehensive and adaptable structure for managing AI-associated risks. The AI RMF is a dynamic document which, aligned to NIST's prior frameworks, could be updated to keep pace with the rapid evolution of AI technology and best practices.

The AI RMF comprises four interconnected components: govern, map, measure, and manage. Each of these components integrates seamlessly with other NIST risk management frameworks[6] that use consistent risk management tenants and the risk functions already entrenched in the banking industry, including model risk management, IT risk management, cyber risk management, enterprise risk management, operational risk management and resilience, and privacy.

In particular, the governance component aligns with the banking industry's robust tradition of corporate and risk governance.[7,8] Having well-structured governance models, reinforced by the appropriate policies and processes to harmonize various risk departments, establishes a strong supervisory framework. This, in turn, enables the banking industry to adopt technology responsibly by comprehensively considering the risks posed by new developments, while seeking out the advantages that AI technology offers.

It is only through such a robust, programmatic approach to risk management that we can ensure the successful and safe implementation of AI technologies across industries. The banking industry has a proven track record of responsible adoption of leading-edge technologies, such as the widespread adoption of machine learning, which has already been successfully integrated within this robust structured framework.

In evaluating AI capabilities and risks, one of the primary guidance documents that banks utilize to ensure risks are appropriately managed is the Supervisory Guidance on Model Risk Management (hereafter, "Model Risk Management Guidance" or "Guidance").[9]

The Model Risk Management Guidance (MRM) is principles-based and flexible enough to cover risks

---

[6] NIST Risk Management Framework; NIST Cybersecurity Framework; NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management

[7] *Comptroller's Handbook, Corporate and Risk Governance;* Office of the Comptroller of the Currency; Version 2.0, 2019

[8] OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations; 12 CFR Appendix D to Part 30; OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches establishes minimum standards for the design and implementation of a covered bank's risk governance framework and minimum standards for the covered bank's board of directors in providing oversight to the framework's design and implementation (Guidelines).

[9] FRB, SR 11-7, Supervisory Guidance on Model Risk Management (Apr. 4, 2011), https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf; OCC, Bulletin 2011-12, Supervisory Guidance on Model Risk Management (Apr. 4, 2011), https://occ.gov/news-issuances/bulletins/2011/bulletin-2011- 12a.pdf; FDIC, FIL-22-2017, Adoption of Supervisory Guidance on Model Risk Management (June 7, 2017), https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.pdf.

related to AI. The Guidance requires banks to develop effective model risk management frameworks, including robust model development, implementation and use effective validation, sound governance, policies, and controls. In certain circumstances, the guidance has been applied to require banks to dedicate substantial compliance resources to anything deemed a "model," including multiple layers of internal and regulatory review. Importantly, embedded within the model risk guidance is the principle of materiality, that model risk management activities should be commensurate with the risk being managed, and also that the application should be tailored based on the unique characteristics of the bank. These principles are being applied to address risks related to AI. Further, controls to mitigate these risks can be scaled or enhanced appropriately depending on the complexity, materiality and application of AI models and the overall risk entailed. However, the introduction of excessively complex MRM regulations can impede this innovative momentum due to the slow pace of regulatory oversight. It's crucial that regulations are designed in a manner that doesn't stifle creativity but encourages safe and ethical AI implementation in risk models.

We encourage OSTP to consider the Model Risk Management framework in the banking sector as a common model, oversight, and accountability structure for other industries that are not as heavily regulated or mature in their formalized risk management practices.
In response to question 4:

4. What are the national security benefits associated with AI? What can be done to maximize those benefits?

Our members are committed to using AI to focus on consumer protections, safety, and national security. We believe that AI is a powerful tool that can be used to make the financial system more secure and to protect the public.

Banks, through their existing robust risk governance and management structures have responsibly implemented AI and ML in a wide variety of operations, including but not limited to, fraud detection and prevention, marketing, cybersecurity, anti-money laundering, and credit underwriting. The current application of AI to financial services varies by institution and continues to evolve as the applications of AI expand. In fact, fraudsters and cyber criminals are increasingly using AI technologies to advance their malicious activities. This reality makes it necessary for industries to innovate and incorporate AI technologies to continue to defend against these threats.

In BPI's interagency response[10] to the Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning[11] we illustrated some of the bank functions where AI is currently being utilized and where further potential exists to enhance bank operations, including fraud detection and prevention, customer service, cybersecurity, anti-money laundering, credit underwriting, and back-office management.

[10] BPI Interagency Response to Request for Information and Comment on Financial Institutions Use of Artificial Intelligence, Including Machine Learning

[11] Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning: A Notice by the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Consumer Financial Protection Bureau, and the National Credit Union Administration on 03/31/2021.

The banking industry encourages investments in AI safety research and the development of improved trust and safety practices. Proper risk-based implementation of AI can have positive impacts on protecting rights, safety, and national security.

National Security Benefits of AI: Artificial intelligence can significantly enhance national security by improving threat detection, enhancing, and accelerating decision-making, and bolstering cybersecurity. Benefits are best realized through collaboration between the financial services sector and national security agencies, as well as continued investment in AI research and development with a focus on security, anti-money laundering, and fraud prevention applications. The government and private sector may need to leverage AI tools to counter international adversaries. An overly restrictive approach, stifling AI advances, may provide adversaries who are not bound by similar controls an unnecessary advantage.

AI for Cybersecurity and Fraud: The rise in AI applications has led to more complex fraud and cyber threats, such as generating convincing fraudulent identities, manipulating deep fakes, crafting phishing emails, and creating harder-to-detect malware. To counter these malicious activities, banks utilize AI for purposes of developing fraud and cybercrime defenses, such as identifying fraudulent patterns through data analysis, building malware-detecting algorithms, and creating chatbots for fraud prevention. Although AI's role in fraud and cyber threats presents an escalating challenge, it also necessitates organizations building stronger defenses. By leveraging AI to comprehend the latest threats and devise novel solutions, organizations can better safeguard against increasingly advanced attacks.

Protect privacy: AI can be used to develop new encryption techniques and design systems that are more resistant to data breaches, protecting consumer privacy and yielding more timely identification of ongoing data breach incidents.

Enforce laws, sanctions, and regulations: AI can be used to enforce laws and regulations. For example, AI is used today to identify potential violations of anti-money laundering laws and to monitor financial transactions for signs of fraud or terrorist financing, and future developments will further improve the reliability and efficiency of these applications.

Public/Private threat intelligence Information Sharing will be a Necessity: In an age where AI's rapid advancement presents a kaleidoscope of risks, it is imperative that the government and private sector take immediate and decisive action to enhance threat and vulnerability information sharing.

Historical precedents demonstrate that when the public and private sectors bridge their expertise and resources, the yield in cybersecurity awareness and defenses is exponential. This mutually reinforcing network is tried and tested, and would be particularly effective in combatting AI threats given the speed of innovation. In fact, using AI tools could enhance public/private partnerships through cyber information and threat intelligence sharing. Intelligence sharing has been shown to be an invaluable investment in protecting the nation's financial system and national security more broadly.

Advancing Equity and Strengthening Civil Rights

The financial industry in the United States is committed to harnessing the transformative potential of artificial intelligence. AI can promote access to financial services by advancing access to financial tools and opportunities for financial inclusion. For instance, AI-powered financial education tools may enhance financial literacy and empower individuals to make more informed financial decisions. The industry is committed to working with regulators and policymakers to ensure that proposed guidelines are informed

by a deep understanding of AI technologies and their potential impacts, while also understanding the potential to reduce unequal access to financial products.

Provide financial education: AI can be used to develop personalized financial education programs that are tailored to the needs of different individuals and groups. Financial literacy is the bedrock of a financially resilient and prosperous society. AI can be harnessed to revolutionize financial education through personalized learning platforms and intuitive tools. By analyzing an individual's financial behavior, AI-driven platforms can offer tailored educational content and recommendations that cater to the person's unique financial circumstances and goals. Chatbots and virtual financial advisors powered by AI can engage with individuals, providing them with real-time guidance on financial matters.

Bias in AI systems: The banking industry, fully cognizant of the importance of this issue, has acknowledged the potential for bias in AI systems, and is actively engaged in pioneering cutting-edge techniques to mitigate biases. This is a mission of both fair and practical dimensions. It is about safeguarding the moral compass of financial services and ensuring that the outcomes through the use of any technology, including AI as an instrument of change is realized and impactful in a positive manner for every consumer.

One of the most promising avenues being explored is the analysis of de-biasing outputs. Through sophisticated analytical tools, these algorithms identify potential of bias within the training data and neutralize them before they can be assimilated into the AI system. This ensures a more egalitarian data set with the express intent to result in fairer outcomes.

Improving Access to Financial Services: AI may have the potential to promote financial inclusion by improving access to financial services. The advent of AI stands poised to dismantle barriers that have historically impeded access to financial services. AI-driven credit scoring models, for instance, can consider a broader array of alternative data, such as how well an individual pays your financial commitments (rent, utilities) that are not typically considered for traditional credit scoring models. AI should be able to better detect behavior and extrapolate results for populations historically not included within certain development sets, enabling a more nuanced assessment of creditworthiness. This is particularly salient for those with limited credit histories. AI-driven data analysis can help financial institutions identify and understand the needs of different demographics, leading to the development of financial products that serve a broader community. Financial institutions could harness AI not just as a tool for efficiency, but as a conduit for expanding the horizons of what is possible in delivering financial services.

Promoting Economic Growth and Good Jobs

AI can be a significant driver of economic growth and job creation. McKinsey concluded in its report on The Economic Potential of Generative AI[12] that "Generative AI's impact on productivity could add trillions of dollars in value to the global economy." McKinsey's latest research estimated "that generative AI could add the equivalent of $2.6 trillion to $4.4 trillion annually across the 63 use cases we analyzed." We

[12] McKinsey & Company. (2021, March). The economic potential of generative AI: The next productivity frontier. Retrieved from https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20economic%20potential%20of%20generative%20ai%20the%20next%20productivity%20frontier/the-economic-potential-of-generative-ai-the-next-productivity-frontier-vf.pdf.

believe that AI can improve productivity across the economy, and reduce costs associated with products and services. AI technologies have the potential to transform the economy, and while recognizing the potential labor market disruptions, we also recognize the opportunities in reskilling the workforce to maintain a competitive and vibrant United States marketplace.

Upskilling and reskilling: AI is changing the nature of work in the financial services industry. As a result, financial institutions are working to upskill and reskill their workforces to ensure that they have the skills needed to succeed in a digital era that includes AI.

A resolute investment in reskilling and upskilling programs is not only an investment in human capital but an investment in the nation's competitive future. New skillsets are needed for AI research and development, opening a space for job creation and innovation in fields such as data science and analysis. The financial services sector is currently investing in its own labor force and encourages targeted investments in STEM education, vocational training programs, and diversity initiatives to maintain the United States competitive stance in this global marketplace.

Ensuring Adequate Competition in the AI Marketplace: The United States can ensure adequate competition in the marketplace for advanced AI systems by promoting transparency and fairness in the AI marketplace. For example, by fostering innovation through research and development incentives and encouraging consistency within the financial sector that both banks and non-banks are subject to the same regulations, rules, and expectations.

Conclusion

The Bank Policy Institute and its technology policy division, BITS, extends its sincere gratitude to OSTP for fostering an open and broad-reaching discourse on the national deployment of artificial intelligence. The financial sector, conscious of its pivotal role in the economy, fully grasps the monumental potential AI possesses to invigorate financial services, enrich customer experiences, and fortify financial and national security.

We are committed to collaborating with OSTP and other key stakeholders to harness the transformative power of AI. This commitment is underpinned by a conviction that AI, when integrated consistent with banks' robust governance, oversight, and risk management frameworks, can reap benefits for the industry, consumers, and society at large.

The guiding principles the banking industry will leverage in the era of widespread AI adoption are founded on decades of dedication to technological innovation, underpinned by stringent safety standards, unwavering focus on security, and a commitment to building trust through transparency and exemplary customer service. Mindful of historical leadership and cognizant of our obligations to our customers, employees, and society, we are committed to its responsible and transparent use in this new AI era.

We express our support for the effort underway via the National Institute of Standards and Technology (NIST) AI Risk Management Framework, recognizing it as a significant step in the right direction for AI governance and risk management. This framework offers an adaptable, flexible structure for the management of AI-related risks. The key principles guiding this framework include risk-based prioritization, transparency, accountability, fairness, and expectations of soundness practices. The

framework's adaptability and flexibility, accommodating for a range of AI systems across industries, diverse contexts and scales, make it an ideal candidate to harmonize global regulatory concepts.

Recognizing the significance of international cooperation, it's imperative to promote responsible, transparent AI development and usage, and distribute AI benefits equitably worldwide. These objectives can be achieved through international cooperation, wherein nations collaborate to formulate shared AI risk-based principles and frameworks.

We acknowledge that multiple challenges obstruct international cooperation on AI, including: a disparity of national interests that may not always align; the complexity of AI technology, making it tough to devise common standards and principles that are efficient and practical to enforce; and the rapid pace of technological evolution, rendering it challenging to stay up-to-date and establish standards that are not quickly outdated.

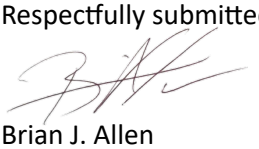
Despite these obstacles, there is an escalating consensus that international cooperation on AI is indispensable. As examined in this response, a principled, risk-based approach is an effective methodology for international AI cooperation. If nations adopt conflicting, prescriptive rules and regulations, it will hinder AI adoption, suppress innovation, and impose unnecessary costs on this burgeoning market.

The financial industry strongly believes that it is important to regulate AI outcomes rather than the technology itself. We endorse the notion that leveraging existing regulatory frameworks, which have evolved through decades of experience and are time-tested, is both efficient and imperative. The existing regulatory framework and robust risk management practices of banks have historically accommodated emerging technologies, and the same is true for banks' implementation of AI technologies. We support the responsible adoption of AI, fortified by strong governance, comprehensive risk management, and vigilant oversight, with focus on the core tenets of transparency, compliance, and social implications.

* * * * *

BPI appreciates the opportunity to respond to the request for information and to participate in this dialogue. If you have any questions, please contact the undersigned at 202-589-2441 or by email at Brian.Allen@bpi.com.

Respectfully submitted,



Brian J. Allen
SVP, Emerging Technology Risk Management
BITS/Bank Policy Institute