



November 8, 2019

U.S. Consumer Financial Protection Bureau
1700 G St NW
Washington, DC 20552
ATTN: Timothy Lambert and Paul Watkins

Re: Request for Information Regarding Tech Sprints (CFPB-2019-0048)

Inpher appreciates the opportunity to advise the Consumer Financial Protection Bureau (“CFPB”) on the *Request for Information Regarding Tech Sprints*.¹ We believe this consultation is an important and timely opportunity for the Bureau to understand the obstacles that RegTech companies currently face in introducing their products and solutions to market due to the lack of education and regulatory support of emerging technologies in financial services. We urge the CFPB to promulgate policies that will alleviate the barriers to entry restricting privacy-focused startups from exploring use cases with institutional partners due to uncertainties on the potential regulatory risk of new data governance models. Supervised FinTech sandboxes can promote trust in privacy-enhancing technologies (“PETs”) and introduce consistent processes to evaluating compliance and adopting cutting-edge products that demonstrate value for both consumers and regulators.

There is a critical need for the standardization of PETs in the financial services industry, which operates on significant volumes of customer data and its derivatives. Technological solutions now exist to eliminate the traditional tradeoff between privacy and data utility. PETs benefit both financial institutions and regulators by instituting technological safeguards that allow parties to share data and facilitate collaboration for financial monitoring and effective enforcement. For example, advances in Fully Homomorphic Encryption (“FHE”) and Secure Multi-Party Computation (“MPC”) allow functions to be performed on encrypted data without revealing the sensitive underlying information. This keeps data securely encrypted in storage, transit, and *in-use* (while being processed)—creating an incorruptible *ex ante* privacy safeguard against unauthorized access by intermediaries and third parties.²

Cryptographic technologies thus preserve analytical precision (in contrast to differential privacy methods), and allow secure collaboration across data silos for greater coordination and scalability. Inpher is actively engaged in cryptographic privacy safeguards that can be applied (1) bank-to-bank, (2) bank-to-regulator, and (3) regulator-to-regulator to enable knowledge-sharing for anti-money laundering and fraud detection, without exposing the underlying personal information between parties.

¹ <https://www.regulations.gov/document?D=CFPB-2019-0048-0001>

² Yehuda Lindell & Benny Pinkas, *Secure Multiparty Computation for Privacy-Preserving Data Mining*, The Journal of Privacy and Confidentiality (2009), <http://jpc.cylab.cmu.edu>; ING Belgium Sees Opportunities for ‘Secret’ Sharing of Encrypted Data, The Wall Street Journal (Jun. 1, 2017), <https://blogs.wsj.com/cio/2017/06/01/ing-belgium-sees-opportunities-for-secret-sharing-of-encrypted-data/>

FHE and MPC are rapidly evolving from academic research into practical applications in multiple industries today, bolstered by quantifiable improvements in their computing power for large datasets. Inpher leverages these advanced PETs as a computing platform for privacy-preserving analytics with mathematical guarantees of data security and sovereignty. This ‘Secret Computing’ technology enables compliant data processing across siloed departments, cross-jurisdictional and cross-industry information sharing, and zero-knowledge cloud computing, as the host never ‘sees’ the data nor has access to the keys. We have made multiple order-of-magnitude advancements in the performance of both FHE and MPC without compromising accuracy—and have deployed this technology to solve real-world privacy and security challenges in banking, compliance, and financial inclusion.

Regulators should support the development of innovative approaches to protecting individuals’ privacy and increasing trust in financial products and services. The CFPB Tech Sprint has the potential to solve the following problems endemic to smaller FinTech companies:

- Difficulty getting the product to market.
- Difficulty staying competitive with incumbents.
- Difficulty clarifying compliance to commercial partners.

Public-private partnerships via hackathons, Tech Sprints, and regulatory sandboxes are integral to understanding, supporting, and applying these technologies with the appropriate safeguards for consumer protection and competition. These opportunities are particularly important for Inpher, whose core mission is to protect consumer data with privacy-preserving analytics. FinTech sandboxes allow us to prove our concept with the support of regulators, which legitimizes our solutions to the market and allows financial institutions to test the product without the fear of adverse regulatory action. Creating a defined space for financial institutions, technology companies, and regulators to come together to pair identified risks with innovative solutions is absolutely necessary to streamline ideas to production by enabling funding for PETs and fostering an ecosystem where startups can compete with incumbents.

At the international level, the UK Financial Conduct Authority (“FCA”)³ and Information Commissioner’s Office (“ICO”)⁴ have recently hosted sandbox sessions designed to support the development of products and services that aid compliance with data protection laws. Inpher participated in the FCA Tech Sprint to demonstrate the application of secure MPC to enable knowledge sharing between financial regulators to detect trade anomalies and monitor financial crimes whilst adhering to strict privacy law requirements.⁵

³ UK Financial Conduct Authority, *2019 Global AML and Financial Crime TechSprint* (Held on Jul. 29, 2019 to Aug. 2, 2019), <https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint>

⁴ Information Commissioner’s Office, *ICO opens Sandbox beta phase to enhance data protection and support innovation* (Mar. 29, 2019), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/03/ico-opens-sandbox-beta-phase-to-enhance-data-protection-and-support-innovation/>

⁵ Inpher, *Inpher Wins People’s Choice Award at FCA TechSprint* (Aug. 9, 2019), <https://www.inpher.io/news/2019/8/9/inpher-wins-peoples-choice-award-at-financial-conduct-authoritys-2019-tech-sprint>.



These partnerships create room for technologically-driven regulation and create demonstrable public value with responsible innovation. Therefore, it is incumbent on federal regulators to explore and support privacy-preserving, cryptographic technologies. In order for PETs to become a baseline standard for financial institutions, the technology must be incentivized and reinforced with hospitable market and regulatory climates. The CFPB must take a cohesive approach with other agencies to ensure that regulatory and legal measures are in place to create consistent privacy and security thresholds with PETs.

We support the CFPB's Tech Sprint initiative and submit these comments to foster PETs that empower transparent communications between banks and regulators, and moreover protect privacy with accountable data governance in financial services. In closing, we make the following recommendations to aid the Bureau's coordination of successful Tech Sprints.

- Selection criteria should ensure that Tech Sprint participants offer a novel product that benefits data privacy and security.
- Prevent anti-competitive abuses of sandboxes. Limit participation to independent companies and startups to ward off large incumbents that create subsidiaries to pass off as a smaller firm in the Tech Sprint.
- If participation is denied, give reasoned responses for the basis of the decision.
- Explain the overlapping jurisdiction of various U.S. financial regulators and how the CFPB no-action letter exempts or does not exempt certain activities from enforcement.
- Publish a guideline or white paper prior to the Tech Sprint to address the false dichotomy of sandbox enforcement waivers and consumer protection. Clarify that the Tech Sprint will facilitate transparency and supervision to harness solutions for privacy, and resolve regulatory ambiguity to promote responsible innovation.

Thank you for the opportunity to comment on this important consultation. If you have any questions regarding our comments, or if Inpher could be of any assistance, please do not hesitate to contact me at sunny@inpher.io.

Sincerely,

Sunny Seon Kang

Senior Privacy Counsel, Head of Policy

Inpher, Inc.