inpher

August 2, 2019

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Re: Proposed Rulemaking: Amendments to Safeguards Rule (16 CFR Part 314)
Project No. P145407

Dear Commissioners:

Inpher appreciates the opportunity to comment on the Federal Trade Commission's ("FTC" or "Commission") notice of proposed rulemaking to amend the *Standards for Safeguarding Customer Information* ("Safeguards Rule").[1] The FTC is empowered by Subtitle A of Title V of the Gramm Leach Bliley Act of 1999 ("GLBA") to establish standards for financial institutions relating to administrative, technical, and physical safeguards for certain information, to "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[2] The Safeguards Rule became effective on May 23, 2003.

We submit these comments in response to the FTC's proposed modifications on the existing Safeguards Rule, which would provide covered financial institutions with more specific guidelines on how to develop, implement, and improve the accountability of their information security systems.[3] Inpher supports the Commission's decision to impose stronger security and privacy baselines for financial institutions that collect, transmit, and analyze sensitive customer information.

Increasing large-scale data breaches, underscored by this week's Capital One hacking that compromised over 100 million credit card customers' sensitive information,[4] confirms the urgent need for robust regulatory and technical standards for privacy-by-design. Therefore, we believe it is both timely and critical for the FTC to update the 2003 Safeguards Rule to reflect and embrace modern advances in Privacy-Enhancing Technologies ("PETs"). Design standards for privacy-preserving technologies will be necessary to mitigate financial data breaches, and to keep U.S. financial institutions competitive by harmonizing with extraterritorial privacy laws such as the General Data Protection Regulation ("GDPR").[5]

[1] *Standards for Safeguarding Customer Information*, 84 Fed. Reg. 13158 (proposed Apr. 4, 2019) (to be codified at 16 C.F.R. pt. 314), https://www.federalregister.gov/documents/2019/05/24/2019-10910/standards-for-safeguarding-customerinformation.

[2] 15 U.S.C. 6801(b), 6805(b)(2).

[3] *Supra* 1.

[4] *Capital One Reports Data Breach Affecting 100 Million Customers, Applicants*, The Wall Street Journal (Jul. 30, 2019), https://www.wsj.com/articles/capital-one-reports-data-breach-11564443355

[5] EU General Data Protection Regulation (GDPR) Article 25, Data protection by design and by default, http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm.

Notable international bodies including the United Nations ("UN"),[6] Organization for Economic Co-operation and Development ("OECD"),[7] and European Union Agency for Cybersecurity ("ENISA")[8] have all promoted the implementation of PETs to minimize risks to privacy and data protection.

Inpher Background

Inpher is a US-based cryptography and machine-learning company with the conviction that encryption and privacy are foundational to the future of computing and commerce. Inpher's customers include some of the world's largest multinational financial institutions that use its software platform for privacy-preserving analytics and computation 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.

Inpher's recent advances in PETs have brought years of academic research on Fully Homomorphic Encryption ("FHE") and secure Multi-Party Computation ("MPC") into commercially-ready applications that financial institutions are using in production today.[9] Our legal and public policy department facilitates public education on privacy-preserving technologies and advocates for data protection by design, global privacy, and algorithmic accountability.

1. Inadequacies of the Existing Safeguards Rule

Coming into effect in 2003, the Safeguards Rule was drafted as a technology-neutral guideline to allow flexibility for financial institutions of different sizes, operations, and types of data to develop an information security program that was appropriate for their particular practices. The Commission purposefully set broad goals that financial institutions could adapt to individualize their information security programs, and avoided prescriptive requirements that could quickly become outdated in an evolving technological landscape. The Safeguards Rule continues to rely on financial institutions to take "reasonable" precautions to protect the privacy and security of customer information—through employee training on information security, contractual terms with third party data processors, and risk assessments.[10]

a. Preventing Unauthorized Data Access

[6] United Nations, *UN Handbook on Privacy-Preserving Computation Techniques*, http://publications.officialstatistics.org/handbooks/privacy-preserving-techniques-handbook/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf

[7] OECD, *Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*: "The Joint Proposal also incorporates various recent data protection measures, including information management strategies, employee training, and appointment of individuals who are responsible for an organization's data protection practices, codes of practice, audits, privacy enhancing technologies, and privacy impact assessments." https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[8] European Union Agency for Cybersecurity (ENISA), *Privacy Enhancing Technologies 'Time to Adopt PETs'*, https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

[9] Inpher, *Case Studies*, https://www.inpher.io/case-studies-1#case-studies

[10] U.S. Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Although these guidelines remain as necessary touchstones to an information security plan, they alone are not sufficient *ex ante* safeguards to prevent or even mitigate the impact of data breaches and unauthorized access to customer information. The existing Safeguards Rule is outdated, because it does not institute systemic designs that can minimize the vulnerability of increasingly granular customer information held by financial institutions for a variety of operations. We believe that more specific guidelines are necessary to protect privacy and to prevent the occurrence of breaches or misuses of data.

Rapidly evolving cryptographic PETs such as FHE and MPC offer incorruptible *ex ante* privacy safeguards against unauthorized access by third parties, data processors, intermediaries, and internal employees.[11] The regulatory focus should now shift to implementing PETs that can keep data securely encrypted in storage, transit, and *in-use* (while being processed), so that sensitive plaintext information is not exposed to those who may violate their data-sharing agreement or fiduciary obligations to engage in misconduct. Cryptographic technologies that protect data during all stages of the processing lifecycle can safeguard privacy with mathematical certainty, whereas mere operational policies to monitor authorizations may fail to detect leaks in practice.

b. Inconsistent Information Security Programs

The frequency and impact of financial data breaches are rising every year,[12] yet consumer remedies and judicial recognition of information injuries remain stagnant. Therefore, we encourage the FTC to amend the Safeguards Rule to provide a more consistent framework of requirements-engineering[13] and privacy design standards that are empirically proven to minimize security risks, rather than allowing financial institutions to make qualitative judgements on what data practices are "reasonable" for their systems.

2. Recommendations

a. Privacy Impact Assessments

We strongly support the Commission's proposed amendment of §314.4(b) to add a requirement for financial institutions to "periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks." We agree with the Commission's assessment that an effective risk assessment must be subject to periodic review and validation.

We recommend the following additional requirements:

[11] 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/

[12] IBM, *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years* (Jul. 23, 2019), https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

[13] Mireille Hildebrandt & Laura Tielemans, *Data protection by design and technology neutral law*, 29 Computer Law & Security Review 509-521 (2013). See also Michael D. Birnhack, *Reverse Engineering Informational Privacy Law*, 15 Yale J. L. & Tech. 24 (2012).

(1) Require a Privacy Impact Assessment ("PIA") with specific guidelines to review internal data protection standards and adherence to fair information principles.[14] PIAs should be publicly available to inform customers of the financial institution's information security safeguards, and help facilitate regulatory communications with the FTC to clarify compliance with the Safeguards Rule.

(2) Require financial institutions to conduct a risk assessment of the technologies that are deployed by their information security systems, and evaluate the feasibility of adopting PETs that could better address vulnerabilities and thwart emerging threats to the security of those systems.

b. Additional Encryption Requirements

We strongly support the Commission's proposal to amend §314.2 to add a definition of "encryption" as "the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key." We agree with the Commission's assessment that "in most circumstances encryption is an appropriate and important way to protect customer information from unauthorized use and access," and support the proposed §314.4(c)(4) to require financial institutions to encrypt all customer information, both in transit and at rest.

However, as discussed above, customer information can also be exposed to privacy and security risks while it is being processed and shared with third parties for analysis. Advances in MPC and FHE allow functions to be performed on encrypted data without revealing the underlying information. Application of such privacy-preserving technologies obviate traditional tradeoffs in privacy and analytical precision (for example, with differential privacy methods), and allow secure collaboration across competing financial institutions to identify and address trends and outliers.

Therefore, we recommend the Commission to add a best practices standard for encryption of customer information *in-use* alongside encryption during transit and at rest.

Conclusion

Inpher supports robust privacy rules under the GLBA because we believe that concrete guidance from the FTC will: (1) raise compliance standards for data privacy and security, (2) create consistent security thresholds to guide enforcement, and (3) encourage the standardization of PETs that ensure customer privacy. Innovation and wider application of PETs in the financial services sector will benefit institutions, customers, and regulators by enabling secure analytics and information oversight without sacrificing data privacy for data utility, or vice versa.

Such reform is necessary to articulate privacy-preserving business practices, and to impose a common denominator of technical and organizational requirements that structurally embed strong data protection principles.[15]

[14] David Wright & Paul de Hert, *Privacy Impact Assessment* (2012), Springer, Law, Governance and Technology Series, Vol. 6.

[15] Mireille Hildebrandt & Laura Tielemans, *Data protection by design and technology neutral law*, 29 Computer Law & Security Review 509-521 (2013) at 518: "Perhaps the only way to achieve sustainability in this domain is to combine a general requirement stipulating that at the level of the technical design data protection obligations

Thank you for the opportunity to comment on this important proposal. 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.

must be met, if technically and economically feasible. This would incentivize technological innovation with regard to built-in data protection, because once such technology is state of the art it becomes the legal standard."