February 17, 2017

Via electronic submission to regs.comments@federalreserve.gov;
regs.comments@federalreserve.gov; Comments@fdic.gov

Mr. Robert deV. Frierson
Secretary
Board of Governors of the Federal Reserve System
20th Street & Constitution Avenue, N.W.
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, SW., Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219

Mr. Robert E. Feldman
Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

Re: Enhanced Cyber Risk Management Standards (Docket No. R-1550; RIN 7100-AE 61; Docket ID OCC-2016-0016; RIN 3064-AE45)

Dear Sirs and Madams;

Reprivata, a privately held cyber risk management company, appreciates the opportunity to provide comments on the advanced notice of proposed rulemaking (ANPR), Enhanced Cyber Risk Management Standards, jointly issued by the Board of Governors of the Federal Reserve System (Federal Reserve), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) (collectively, "the agencies").[1]

We commend the agencies for making an effort to describe a comprehensive cyber risk management protocol as a replacement or successor to the current "tool-based" or ad-hoc style system most organizations currently have in place. Organizations have traditionally addressed cybersecurity as an internal technology matter, rather than implementing a broader risk management strategy. Additionally, they have largely ignored the cyber health of their interconnected parties, which are often the weak link in cyber-attacks.

[1] Enhanced Cyber Risk Management Standards. 81 Fed. Reg. 74315 (Oct. 26, 2016). www.federalregister.gov/documents/2016/10/26/2016-25871/enhanced-cyber-risk-management-standards

***Reprivata's assessment is that* organizations are at heightened risk of a breach from cyber-attacks if they cannot define, document, enforce and monitor cyber policies and standards across ALL interconnected parties, including vendors, employees and customers.**

Background

Reprivata Corp (Reprivata) is submitting this response to the Board of Governors of the Federal Reserve System (Board), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) who invited comment on an advance notice of proposed rulemaking (ANPR) regarding enhanced cyber risk management standards (enhanced standards) for large and interconnected entities under their supervision and those entities' service providers.

Reprivata Corp. provides a suite of Standard Master Agreements that when implemented constitute a "Community of Trust" among participating organizations. The implementation of a Community of Trust provides the management of an organization with a simple Cyber Risk Management tool similar to tools currently used to manage credit risk within an organization or enterprise. Master Agreements, similar to those used in financial settlement mechanisms, are implemented to manage critical aspects of an organization's cyber risks.

Community of Trust provides a standard contract "Master" that is used for all Community of Trust owners and interconnected counterparties. Addenda to the Master requires Officer Certification of the NIST Cybersecurity Framework (CSF) maturity level required by the Community of Trust owner and each interconnected counterparty. Addenda to the Master is used to indicate the Cyber Insurance threshold requirements for each interconnected counterparty, required by the Community of Trust Owner. Addenda to the Master is used to name the Community of Trust Owner as additional insured by each interconnected counterparty with a threshold minimum as required by the Community of Trust Owner.

The implementation of this cyber risk management process initiates the flywheel effect to;

1. Require the Community of Trust owner and every interconnected counterparty to meet the requirements of the Master Agreement.
2. Require Community of Trust owners to consult with competing underwriters to guide the Community of Trust owner to shape the Master's Addenda enabling them to price the risk more efficiently and effectively.
3. Enable insurers to compete to originate and syndicate the risk that is defined by the Master agreement, governing the owner's Community of Trust.

The single defect preventing the development of accessible and efficiently priced cybersecurity insurance is the absence of a standard contract structure that would enable the efficient pricing of risk and ultimately broad adoption of prudent cybersecurity requirements. Due to the complexities of the systemic risks involved in cybersecurity,

underwriters safety load the policy premiums to contend with the theory that it is virtually impossible to perform a reasonable assessment of risk. This practice in and of itself is an accumulating hazard for underwriters and the insured. This practice is preventing underwriters from creating the velocity that is required to generate premiums and thus stagnates the development of accessible, effective and efficiently priced cybersecurity insurance. And most importantly, prevents underwriters from imposing meaningful underwriting requirements such as requiring a minimum level of cybersecurity maturity for the insured and all those connected to the insured.

Further, we assert that the defect is the absence of a standard contract structure that would enable the syndication of risk to natural financial counterparties. While there is no doubt that risk complexities require a significant premium, the absence of standardized contracts prevents the development of an efficient pricing mechanism to determine the significance of that premium as viewed by a diverse group of market participants.

To begin to solve this problem we have developed a suite of standardized contracts for the insured that will enable cybersecurity insurance providers to begin to uniformly mitigate risks in the underwriting process. By enabling cyber risk to become more transparent and creating liquidity by virtue of the standard contract structure, Community of Trust enables broad syndication of risk. And, ultimately market-driven adoption of requirements, such as all interconnected counterparties meeting NIST Cybersecurity Framework maturity thresholds and being reasonably insured themselves.

Reprivata also provides technology certified by Underwriter's Laboratory ("UL") Cyber Assurance Program 2900 to all Community of Trust participants that enables even small interconnected counterparties to cost effectively connect securely and enables monitoring of interconnection threats in real-time. Reprivata's secure transport technology is the only technology to date that has been certified by Underwriter's Laboratory ("UL") Cyber Assurance Program 2900.

Benefits for Financial Institutions

- Community of Trust enables a financial institution to proceed immediately with a market-based approach to measure, mitigate and manage systemic cyber risk using familiar financial risk management processes.
- Community of Trust enables financial institutions to access more effective and efficiently priced cybersecurity insurance.
- Community of Trust enables financial institutions to potentially unlock regulatory capital allocated to cyber risk.

Benefits for Insurers

- Community of Trust standard contracts enable fungibility and a frictionless, systematic syndication of risk.

- Community of Trust standard contracts enable the creation of financial instruments that enable the intermediation of risk by traditional financial market participants.
- Community of Trust requirements for interconnected counterparty compliance systemically improves cyber health and enables underwriting velocity, creating accelerated adoption of a prudent cybersecurity posture.

Our comments here do not address many of your questions. However, we believe that our approach begins to address many of the challenges we are facing as a nation to protect our critical infrastructure. Furthermore, we assert that many of the complexities of these challenges can be managed more efficiently by incentivizing financial participants to use standard processes and tools that they currently use in their day to day financial businesses to manage cyber risk and systemically improve the cyber health of our nation.

Accordingly, with respect to the agencies' proposal, the question then is, whether to impose enterprise risk management protocols on the financial industry through regulation; or, to strongly encourage engagement with market-based solutions like Reprivata that address all areas of concern and are already built and scalable. Together with UL, Reprivata has examined risk-based governance, transparency, counter-party risk and disclosure, third party compliance and risk measurement based largely on mandatory software testing (software integrity) modeled after the DHS group of the same name.

As a matter of record, the agencies' rule is proposing to implement what the UL CAP 2900 certification already requires.

We would like to work with the agencies on this important subject in the future and look forward to our next opportunity to comment.

Respectfully,

John B. Tripp Hardy
Chief Executive Officer, Reprivata, Corp.

David Cox
President, Reprivata, Corp.

Derek Jenkin
Executive Vice President, Reprivata, Corp.