



Filed electronically with Financial Stability Board (FSB)

DRAFT – August 20, 2018

Re: Comments on FSB’s Cyber Lexicon

To the Cyber Lexicon Committee:

The SPARK Institute, Inc. is pleased to submit comments on the Financial Stability Board (FSB)’s Cyber Lexicon for approval by the G20 Finance Ministers. Our comments offered below are a joint response from SPARK’s Data Security Oversight Board members.

The SPARK Institute represents the interests of a broad-based cross section of U.S. retirement plan service providers and investment managers, including banks, mutual fund companies, insurance companies, third-party administrators, trade clearing firms, and benefits consultants. Collectively, our members serve approximately 95 million American workers through their employer-sponsored retirement plans.

The SPARK Institute and its member firms recognize and applaud all efforts to improve the effectiveness and security of all commercial financial systems when transacting over the internet. We agree with the goal of developing a common lexicon to provide financial institutions with a shared language and to help establish international standards to address cyber security and cyber resilience in the financial sector. However, our members feel the FSB should consider the following:

1. **Cyber Fraud** – While we understand that this proposed lexicon is not intended for use in any legal interpretation of any international arrangement or agreement or any private contract, we do believe that the recognition of “*cyber fraud*”, or “*account take-over*” is important to the later definition of a Data Breach. A compromise of a client’s personal account using data or processes not within the authority and direct control of the financial institution that results in wrongful financial access or loss should not be considered a Data Breach. The commonly suggested example of this is if a client’s account is unlawfully accessed through the careless use of security passwords by the client, or through illegally obtained personally identifiable information from a third-party breach. In this example there was no breach of the financial firm’s firewalls or safeguards.
2. **Data Breach** – If the FSB agrees to include Cyber Fraud or Account Take-Over as an additionally defined term then the definition of a Data Breach should be adjusted accordingly. “A compromise of security *within the authority or direct control of the financial institution* that leads to the accidental or unlawful destruction, loss,

alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed.”

* * * * *

The SPARK Institute appreciates the opportunity to provide these comments to the FSB. If the Board has any questions or would like more information regarding these comments, please contact me at (508) 838-1919 or Tim@sparkinstitute.org.

Tim Rouse
Executive Director
SPARK Institute

Doug Peterson
Chair of SPARK’s
Data Security Oversight Board