Independent Bankers Association of Texas

Bradley H. Tidwell
IBAT Chairman
VeraBank, Henderson

Thomas C. Sellers
IBAT Chairman-Elect
Alliance Bank, Sulphur Springs

K. Kyle Irwin
IBAT Secretary-Treasurer
Western Bank, Gruver

Peter Smith
Leadership Division Chairman
American Momentum Bank, Lubbock

Hazem A. Ahmed
IBAT Education Foundation Chairman
Independent Financial, Houston

Richard F. Scanio
Immediate Past Chairman
American Bank, Corpus Christi

Christopher L. Williston VI, CAE
President and CEO
IBAT, Austin

Ursula L. Jimenez, CAE
Chief Operating Officer
IBAT, Austin

Stephen Y. Scurlock
Director of Government Relations
IBAT, Austin

Curt Nelson
Director of Membership
IBAT, Austin

Christy Bussey
Director of Growth and Development
IBAT, Austin

Julie Courtney, CAE, CMP
IBAT Services Inc. President
IBAT, Austin

Esmeralda Gonzalez, CAE
IBAT Education Foundation President
IBAT, Austin

Karen Neeley
General Counsel
IBAT, Austin

April 12, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street SW, Suite 3E–218
Washington, DC 20219

Ann E. Misback,
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Hames P. Sheesley
Assistant Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Via Regulations.gov

Re: OCC Docket ID OCC–2020–0038; FDIC RIN 3064–AF59; FRB No. R–1736 RIN 7100–AG0

Greetings,

The following comments are submitted on behalf of the Independent Bankers Association of Texas ("IBAT"), a trade association representing more than 350 independent, community banks domiciled in Texas.

1. How should the definition of ''computer-security incident'' be modified, if at all? For example, should it include only occurrences that result in actual harm to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits? Should it include only occurrences that constitute an actual violation of security policies, security procedures, or acceptable use policies?

Generally speaking, this is the definition adopted by the National Institute of Standards and Technology (NIST) and should be adopted for the sake of uniformity. While broad enough for banks, the agencies should clarify that this definition includes incidents occurring at third-party information systems and their sub-contractors (fourth-party providers) that collect banking related information.

2. How should the definition of ''notification incident'' be modified, if at all?

For example, instead of ''computer security incident,'' should the definition of ''notification incident'' refer to other NIST terms and definitions, or another recognized source of terms and definitions? Should the standard for materially disrupt, degrade, or impair be altered to reduce potential redundancy between the terms or to consider different types of impact on the banking organization? Should the definition not include language that is consistent with the ''core business line'' and ''critical operation'' definitions included in the resolution-planning rule? Should those elements of the definition only apply to banking organizations that have resolution planning requirements?

The term 'notification incident' should be crafted to include incidents occurring at third-party service provider information systems and the sub-contractors (fourth-party providers) of those third-party service providers that collect banking related information. Sub-contractors of third-party service providers with access to the information or systems that contain covered information of banking organization customers should be held to the same standard as third-party service providers that contract directly with the banking organizations.

3. How should the 36-hour timeframe for notification be modified, if at all, and why? Should it be made shorter or longer? Should it start at a different time? Should the timeframe be modified for certain types of notification incidents or banking organizations (for example, should banks with total assets of less than $10 billion have a different timeframe)?

The proposed rule would require such notification upon the occurrence of a notification incident as soon as possible and no later than 36-hours after the banking organization customer believes in good faith that the incident occurred. That should be revised to not exceed 48-hours after the banking organization customer believes in good faith that the incident occurred. Community banks in particular need the additional 12 hours to evaluate the situation and implement an appropriate incident response plan.

9. Do existing contracts between banking organizations and bank service providers already have provisions that would allow banking organizations to meet the proposed notification incident requirements?

No doubt most will, but some will not. The proposed rule should clarify specific contract expectations for both bank service providers and bank organizations. Contract expectations should include sub-contractors of bank service providers as well.

11. Should the proposed rule for bank service providers require bank service providers to notify all banking organization customers or only those affected by a computer-security incident under the proposed rule?

Bank service providers should only notify those customers affected by the computer-service incident. To notify all banking organization customers will not doubt cause the banking organization customers and the bank service provider to respond to questions and concerns from banking organization customers not affected by the computer-security incident. When a 'computer-security incident' under the proposed rule has occurred, time is a valuable resource and to have to expend it on banking organization customers not impacted will tax that valuable resource without providing any benefit to banking organization customers not impacted.

12. Within what timeframe should bank service providers provide notification to banking organizations? Is immediate notification after experiencing a disruption in services provided to affected banking organization customers and to report to those organizations reasonable? If not, what is the appropriate amount of time for a bank service provider to determine it has experienced a material disruption in service that impacts its banking organization customers, and why?

Unlike a 'computer-security incident' which requires time to identify and evaluate, a disruption in service is instantaneously apparent and bank service providers can immediately notify banking organizations of the disruption in service. Customers of those banking organization customers will no doubt contact their bank when the disruption of service is noticed and not the bank service provider, so immediate notification to the banking organization customers is appropriate to handle bank customer concerns in a timely and thorough manner.

Texas community bankers are dedicated to ensuring customer information is protected when shared with bank service providers. Any proposed rule, if carefully crafted, could be the cornerstone for ensuring that bank organizations and bank service providers have a clear and reasonable standard for the notification of primary regulators.

Thank you for this opportunity comment.

Sincerely,

Christopher L. Williston, CAE
President and CEO