Federal Deposit Insurance Corporation
New York Regional Office
350 Fifth Avenue, Suite 1200, New York, NY 10118

NEW YORK STATE DEPARTMENT of FINANCIAL SERVICES
One State Street, New York, NY 10004

March 25, 2021

Board of Directors
Apple Bank for Savings
122 East 42nd Street
New York, NY 10168

Subject: Update on Ongoing Monitoring Activities as of December 31, 2020

Dear Board Members:

This letter summarizes Ongoing Monitoring (OGM) activities conducted by the FDIC and New York State Department of Financial Services (NYSDFS) during the fourth quarter of 2020 (4Q2020). Supervisory activities included the completion of offsite monitoring, follow-up of previously issued supervisory recommendations, and follow-up on a previously cited apparent violation of the Gramm-Leach-Bliley Act (GLBA). This letter and its contents (including attachments) are confidential and intended only for the Bank's internal use. The disclosure of such confidential supervisory information is governed by Part 309 of the FDIC Rules and Regulations and Section 36.10 of the New York Banking Law.

Closure - GLBA Apparent Violation

In 2017, examiners cited a nonconformance with interagency guidelines (Appendix B to Part 364 of the FDIC Rules and Regulations - Interagency Guidelines Establishing Information Security Standards). The apparent violation remained outstanding at the 2020 Information Technology Target Review, with examiners noting that continued work was needed on the risk assessment component of the GLBA, Section III C-3, which mandates that the bank:

> *Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the institution's risk assessment. Tests should be conducted or reviewed by independent third parties, or staff independent of those that develop or maintain the security programs.*

Examiners followed up on this issue during 4Q2020 OGM activities and noted that Chief Technology Officer Debi Gupta had completed an IT Risk and Control Self-Assessment (RCSA) with assistance from a third-party specialist (ITA Partners) using the bank's internal RCSA framework. Subsequently, Chief Risk Officer (CRO) Steven Eckert and Chief Information Security Officer (CISO)

Maksim Tumarinson engaged ITA Partners to complete a GLBA Risk Assessment Program. Examiners concluded that the GLBA risk assessment program is comprehensive and adequately covers the IT environment. Additionally, management adequately identified key controls and performed control testing. CISO Tumarinson identified several control weaknesses and developed project plans to address the weaknesses. The GLBA Risk Assessment was presented to the Board Risk Committee on October 28, 2020. See Appendix A *Summary of Closed Supervisory Recommendations* for additional information.

If you have any questions or concerns regarding the content of this letter, please contact FDIC Senior Case Manager Amanda Dubuque at (917) 320-2802 or NYSDFS Supervising Bank Examiner Maxine Turner at (212) 709-3837.

Sincerely,

/S/ Yolanda Ford

Yolanda Ford	Steven P. Slovinski
Deputy Superintendent of Banks	Assistant Regional Director
New York State Department of Financial Services	Federal Deposit Insurance Corporation

Appendix A – Summary of Closed Supervisory Recommendations

cc: Federal Reserve Bank of New York

Appendix A
Summary of Closed Supervisory Recommendations

Issue Type and Number	Target Letter	Issue Description	Status
MRBA IT #04/2016	SL #06-2016	IT Enterprise-Wide Risk Management Program (IT-ERMP)	Closed
Corrective Action: Enhance the IT risk assessment and fully develop the IT risk management framework needed to support the IT-ERMP. **Supporting Comments:** Examiners reviewed the IT Risk and Control Self-Assessment (RCSA) that was developed with assistance from a third-party specialist (ITA Partners) using the bank's internal RCSA framework. Examiners noted that the RCSA is comprehensive and adequately covers the IT environment. Management adequately identified key controls and performed control testing. Management identified several control weaknesses and developed project plans to address the weaknesses. The RCSA will continue to be refined in subsequent reviews to mature the process.			
SR IT #07/2016	SL #06-2016	Identification and Documentation of Key Controls	Closed
Corrective Action: Identify and document the appropriate controls that are in place within the Bank's environment. These documented controls should be used for reporting and testing across the three lines of defense: Operations, Risk Management, and Audit. **Supporting Comments:** Examiners found management's remedial action satisfactory. As noted above, the IT RCSA is comprehensive and key controls have been identified and tested.			

Interagency Guidelines Establishing Information Security Standards
Appendix B to Part 364 of the FDIC Rules and Regulations

Issue Type and Number	Target Letter	Issue Description	Status
Apparent Violation of GLBA	SL #03-2017	GLBA Risk Assessment	Corrected
CTO Gupta completed a satisfactory IT RCSA. Subsequent to the completion of the IT RCSA, CRO Eckert and CISO Tumarinson engaged ITA Partners to complete a GLBA Risk Assessment Program. The GLBA Risk Assessment process assessed the bank's business lines using the following categories: Finance & Treasury, Consumer Banking, IT, and Legal & Compliance. The GLBA Risk Assessment identified 31 applications, 20 IT systems, 24 physical repositories that process customers' non-public information. Management's process of testing key controls identified 21 issues. Management completed project plans to address the identified issues. Examiners found the GLBA Risk Assessment Program and the process of key control testing to be comprehensive and in conformance with the information security standards of the GLBA.			