February 10, 2021

FIRST REPUBLIC BANK
DIRECTORS' INFORMATION SECURITY AND TECHNOLOGY COMMITTEE CHARTER

PURPOSE:

The purpose of the Directors' Information Security and Technology Committee ("Committee") of the Board of Directors (the "Board") of First Republic Bank (together with its subsidiaries, the "Bank") is to provide oversight of the information security and enterprise-wide technology ("IT") and cybersecurity functions of the Bank, including the strategies, policies, standards, procedures, and systems established by management to identify, assess, measure, and manage these areas. The Committee will assist the Board and management, including the Bank's Information Technology Steering Committee and Information Security Steering Committee, in managing, overseeing and addressing IT and cybersecurity issues and risks.

While the Committee has the authority and responsibilities set forth in this Charter, management is responsible for designing, implementing, monitoring, and maintaining effective IT functions.

MEMBERSHIP AND MEETINGS:

The Committee is comprised of a minimum of three Board members. Committee members are appointed by the Board on the recommendation of the Corporate Governance and Nominating Committee and may be replaced by the Board.

The Chair of the Committee shall be a director (other than the Bank's Chairman and Chief Executive Officer) that is "independent" under the rules of the New York Stock Exchange or any other applicable regulatory authority.

The Committee shall meet at least three times each year, and more frequently as determined to be necessary or appropriate by the Committee or the Board. The Chair, or at least two other members of the Committee, has the authority to call special meetings of the Committee. A majority of the members of the Committee present at a meeting shall constitute a quorum.

All determinations of the Committee shall be made by a majority of its members present at a duly convened meeting. In lieu of a meeting, the Committee may act by unanimous written consent. From time to time, the Board may designate one or more persons (who are not Board members) to act as (non-voting) Special Advisors to the Committee. Any such Special Advisor may attend meetings of the Committee and provide input to the Committee at such meetings. A Special Advisor's presence at a meeting shall not be counted for purposes of determining a quorum.

AUTHORITY AND RESPONSIBILITIES:

1. The Committee shall review the Bank's IT strategic plan, including the Bank's information security strategy for addressing ongoing and emerging IT and cybersecurity risks. The Committee shall review and, as appropriate, make recommendations to the Board regarding significant IT investments to support the Bank's IT strategic plan. The Committee shall review and receive updates on significant IT projects, IT budgets (and the adequacy and

allocation of IT resources for funding and personnel), IT priorities, and overall IT performance.

2. The Committee shall review and receive updates on policies and standards and shall review the ramifications of updates to policies and standards, in each case pertaining to IT and cybersecurity risks, including the Bank's framework to prevent, detect and respond to cyber-attacks or breaches.

3. The Committee shall review the Bank's significant IT and cybersecurity risk exposures and the steps management has taken to monitor and control such exposures.

4. The Committee shall establish policies and standards relating to escalating or reporting significant IT incidents to the Committee, the Board, any appropriate steering committees, government agencies, and law enforcement, as appropriate.

5. The Committee shall oversee the implementation and maintenance of (including assigning specific responsibility for its implementation and reviewing reports from management with respect to), and shall approve, the Bank's Information Security and Business Continuity Program and the IT Governance Program (collectively, the "IT Security Program"). The Committee shall review the following components of the IT Security Program, and any other as deemed necessary, at least annually, or more often as determined in the Committee's discretion or as directed by the Board:

    - Cybersecurity Risk Assessment;
    - Gramm-Leach Bliley Act (GLBA) Risk Assessment;
    - Information Security Enterprise Risk Assessment (ISERA) Report;
    - Information Assurance and Protection Program (IAPP);
    - Enterprise-level disaster recovery and business continuity;
    - Information Security Risk Management and Crisis Management Team plans, assessments, reports, tests, or exercises; and
    - IT and Information Security metrics including performance reporting.

6. Management shall report to the Committee at least annually on the overall status of the IT Security Program, the Bank's compliance with the IT Security Program and applicable law and regulation relating to the IT issues and management's recommendations for changes or updates to the IT Security Program.

7. The Committee shall establish processes and guidelines for approving and categorizing the Bank's third-party service providers to promote business continuity and to mitigate or prevent IT and cybersecurity risks.

8. The Committee shall receive reports from management regarding the Bank's business continuity planning.

9. The Committee shall oversee and receive updates on the risks, performance, development, security, and maintenance of the Bank's digital banking space and online banking systems, including any threats or other issues related thereto.

10. The Chief Information Security Officer shall report to the Chair of the Committee; provided, that the Chief Information Security Officer may report administratively to the EVP, Chief BSA Officer and Chief Security Officer.

11. The Committee shall perform such other duties and responsibilities as may be directed by the Board or required by applicable laws, rules, or regulations.

12. In performing its responsibilities, the Committee is authorized to obtain advice and assistance from internal or external legal, accounting, or other advisors at the Bank's expense without prior permission of the Board or management.

13. The Committee shall review and discuss with management significant audit and regulatory reports of the Bank, its subsidiaries, and technology service providers relating to information security, business continuity, and technology and any remediation plan related to any such report.

14. The Committee shall coordinate with the other committees of the Board on topics of common interest as the need arises.

15. The Committee shall make regular reports to the Board summarizing the actions taken at Committee meetings.

16. The Committee shall review its own performance and assess the adequacy of this Charter on annual basis. The Committee may recommend amendments to this Charter at any time and submit amendments for approval to the Board.

17. At its discretion, the Committee may form and delegate all or a portion of its authority to subcommittees.