NORTHFIELD BANCORP, INC.
COMPLIANCE AND INFORMATION TECHNOLOGY COMMITTEE CHARTER

1. Purpose

The purpose of the Compliance and Information Technology Committee (the "Committee") of the Board of Directors (the "Board") of Northfield Bancorp, Inc. (the "Bancorp") and Northfield Bank (the "Bank"), collectively, the "Company" shall be to:

(i) provide oversight of compliance with consumer protection laws, regulations and guidance[1] ("Consumer Compliance"), the Community Reinvestment Act (CRA), the Bank Secrecy Act (BSA) /Anti Money Laundering (AML) and The Office of Foreign Assets Control (OFAC) laws, and the Gramm Leach Bliley Act (GLBA) information security provisions (collectively known as the "Compliance Program");

(ii) evaluate the performance of the Compliance Program;

(iii) provide oversight of the Company's Information Technology (IT) function and Information Security Program, serving as the central forum for information technology matters and cyber security projects;

(iv) provide oversight of the Company's corporate insurance and security functions; and

(v) report on the Committee's activities to the Board.

2. Committee Membership

The Committee shall be comprised of three or more directors who shall be appointed by the Board and shall serve until their successors are duly elected and qualified. The Chairperson of the Committee shall be elected by the Board. The Board shall appoint a new member or members in the event that there is a vacancy on the Committee that reduces the number of members below three, or in the event that the Board determines that the number of members on the Committee should be increased. The entire Committee and the individual Committee members shall serve at the pleasure of the Board of Directors. Any Committee member may resign effective upon giving written notice to the Chairperson of the Board or the Corporate Secretary.

3. Committee's Compliance Program Authority and Responsibilities

To fulfill its Consumer Compliance, CRA and BSA/AML, OFAC, and GLBA responsibilities and duties under this Charter, the Committee shall have the authority to:

- Review and recommend for approval the Compliance Program policies prepared by Management.

[1] See Exhibit A for a list of the consumer compliance laws and regulations monitored under the Compliance Management Program.

- Review and approve the Compliance Training Program (with Schedules) prepared by Management.
- Review and approve the BSA/AML Program.
- Review the BSA Risk Assessment prepared by Management.
- Review reports of the BSA Officer and Security Officer.
- Assess the adequacy of the Compliance Department and BSA Department staffing and make recommendations to the Board as a result of its assessment.
- Review annual performance evaluations and recommend appointment of the Compliance Officer and the Bank Secrecy Act Officer.
- Review and assess the adequacy of the Company's Consumer Compliance, CRA, and BSA, OFAC, and GLBA Programs.
- Review, approve and monitor the execution of the annual Compliance Monitoring Program.
- Review reports of Management's assessment of Policies & Procedures designed to comply with new or revised compliance laws, regulations and guidance.
- Review and recommend for approval the Company's CRA Policy Statement (with CRA Program).
- Review reports of Regulatory exams, Internal Audit and Compliance Monitoring Program Reviews and ensure that Management is taking necessary corrective actions.
- Review the selection, retention and termination of third-party vendors retained to support the Compliance, CRA, and BSA Officers.
- Retain outside counsel and any other advisors as the Committee may deem appropriate in fulfilling its responsibilities, with authority to approve related fees and retention terms. The Committee shall notify the Board prior to retaining any counsel or other advisors.
- Review the Company's non-deposit insurance and investment products program annually.
- Review Management's annual report of its identity theft prevention program.
- Report to the Board any actions taken for ratification by the Board as necessary.

- Perform an annual self-evaluation of the Committee and report such evaluation to the Nominating and Corporate Governance Committee or to the Board.

- Annually review this Charter and recommend changes to the Board as needed.

- Monitor enterprise risks assigned to the Committee by the Board under the Company's Enterprise Risk Management program and report thereon to the Board.

- Approve the hiring and termination of the Compliance Officer (CO). With input from the Chief Risk Officer, set objectives for CO, and prepare CO performance evaluation using Bank's performance standards. Determine the CO's annual compensation based on the Compensation Committee's philosophy, market data survey, and targeted increases for other similar level managers.

- Approve the hiring and termination of the BSA Officer (BSAO). With input from the Chief Risk Officer, set objectives for BSAO, and prepare BSAO performance evaluation using Bank's performance standards. Determine the BSAO's annual compensation based on the Compensation Committee's philosophy, market data survey, and targeted increases for other similar level managers.

- The CO and the BSAO will each have unrestricted access to the Committee, and the Committee will ensure executive sessions are scheduled with the CO and the BSAO, at least annually, and whenever necessary and appropriate.

4. Committee's Information Technology Oversight Authority and Responsibilities

To fulfill its Information Technology oversight responsibilities and duties under this Charter, the Committee shall have the authority to:

- Review and recommend for approval information technology and information security policies prepared by Management.

- Review annual performance evaluation and recommend appointment of the Chief Information Officer and the Chief Information Security Officer.

- Assess the adequacy of the IT Department staffing and make recommendations to the Board regarding its assessment.

- Assess the adequacy of the Information Security Department's staffing and make recommendations to the Board regarding its assessment.

- Review and approve the Information Security Program.

- Review, adopt and receive periodic reports of all capital projects with a significant information technology and/or information security component, and review the capital budgets thereof.

- Review, approve and monitor testing of the Company's Disaster Recovery Program.

- Review results of risk assessments relating to new information technology products.

- Review emerging information technology and information security threats.

- Review results of Management's cyber security risk assessments inclusive of any reviews or opinions on the results issued by independent risk management or internal audit functions regarding those results; and review and approve plans to address any risk management or control weaknesses.

- Review results of Management's ongoing monitoring of Company's exposure to and preparedness for cyber threats.

- Engage management in establishing the Company's vision, risk appetite and overall strategic direction in reference to cyber security and determine whether the Company's cyber security preparedness is aligned with its risk as determined by management

- Review emerging technologies applicable to financial institutions.

- Review strategic goals for information technology and information security to ensure that they support the Company's overall strategic goals.

- Review periodic audit reports of the Company's Information Technology and Information Security functions and ensure that Management is taking all necessary corrective action.

- Review the selection, retention and termination of critical[2] third-party information technology vendors and assess their performance except for Service Organization Controls (which is the responsibility of the Audit Committee).

- Retain outside counsel or any other advisors as the Committee may deem appropriate in fulfilling its responsibilities, with authority to approve related fees and retention terms. The Committee shall notify the Board prior to retaining any counsel or other advisors.

- The CISO will have unrestricted access to the Committee, and the Committee will ensure executive sessions are scheduled with the CISO at least annually, and whenever necessary and appropriate.

[2] As defined in the Third-Party Relationships Risk Management Policy & Program.

5. Committee's Additional Oversight Authority and Responsibilities

To fulfill its additional oversight responsibilities and duties under this Charter, the Committee shall have the authority to:

- Review no less than annually the report on the Company's Directors and Officers (D&O), fidelity bond, business interruption and cyber insurance policies.
- Recommend appointment of the Security Officer under Regulation H and the Bank Protection Act.
- Approve and oversee the adoption, implementation, and maintenance of a written security program for the main and branch offices.
- Review reports of the Company's compliance with Regulation H[3] and the Bank Protection Act.
- Review reports of consumer complaints lodged against the Company, including complaints alleging fair lending and unfair, deceptive, or abusive acts or practices activities.
- Review the annual report of the Privacy Officer.
- Review and recommend for approval the annual report of the Identity Theft Prevention Program Coordinator.
- Provide oversight of the Company's Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) and Fair Lending compliance efforts.

6. Meetings

The Committee shall meet at least four times annually, and may hold additional meetings as needed or appropriate. The Committee may ask members of management or others, including outside counsel, to attend meetings or to provide relevant information. A majority of Committee members shall constitute a quorum, and a majority of the members present at any meeting shall decide any questions brought before the Committee.

A meeting may be called by the Chairperson of the Committee or by a majority of the members of the Committee. Notice of any meeting shall be given by the person or persons calling the meeting to each member of the Committee at least 48 hours prior to the meeting. Notice may be given in the same fashion as permitted for notice of Board meetings pursuant to

[3] Regulation H: Membership of State Banking Institutions in the Federal Reserve System 12 CFR 208

the Company's Bylaws and applicable law. Notice may be waived by any member in attendance at the meeting.

When circumstances warrant, members may participate in any meeting by attendance in person or by means of a conference by telephone or other communications equipment in which all persons participating can hear each other. The Committee shall report its actions and recommendations to the Board after each Committee meeting. Minutes of each meeting shall be kept and shall be available to the Board, if requested. All other procedural matters shall be governed in the manner specified in the Company's or the Bank's Bylaws, as the case may be, for meetings of the Board.

* * * * *

Exhibit A

- Americans with Disabilities Act / NYS
- Community Reinvestment Act
- Controlling the Assault of Non-Solicited Pornography and Marketing Act
- Electronic Fund Transfers (Reg. E)
- Equal Credit Opportunity. Act (Reg. B)
- E-Sign Act
- Expedited Funds Availability (Reg. CC)
- Fair Credit Reporting Act
- Fair Debt Collection Practices (Bank Policy)
- Fair Housing Act
- Fair Lending Comparative File Review
- FDIC Membership
- Flood Disaster Protection Act, Biggert-Waters Flood Insurance Reform Act of 2012 & 2019 (Biggert-Waters Act), and the Homeowner Flood Insurance Affordability Act of 2014 (HFIAA)
- Garnishment of Accounts Receiving Federal Benefit Payments
- Home Mortgage Disclosure Act (Reg. C)
- Home Ownership and Equity Protection Act (HOEPA)
- Homeowners Protection Act (PMI)
- Homeownership Counseling
- Illegal Internet Gambling (Reg. GG)
- John Warner National Defense Authorization Act
- Loans to Executive Officers, Directors, and Principal Shareholders (Regulation O)
- Military Lending Act

- Non-Deposit Insured Products
- Protecting Tenants at Foreclosure State & Local Laws
- Real Estate Settlement Procedures Act (Reg. X)
- Reserve Requirements (Reg. D)
- Right to Financial Privacy Act
- Secure and Fair Enforcement for Mortgage Licensing (SAFE) Act
- Servicemembers Civil Relief Act
- Telephone Consumer Protection Act + Junk Fax Prevention Act
- Truth in Lending Act (TILA) / Real Estate Settlement Procedures Act (RESPA) Integrated Disclosures (TRID)
- Truth in Lending Act (Reg. Z)
- Truth in Savings Act (Reg. DD)
- Unfair, Deceptive, or Abusive Acts or Practices
- Websites & Other Audio / Visual Marketing