OLD NATIONAL BANCORP

Information Security Program Summary

Summary

Old National Bancorp and its subsidiaries (Old National) have an unwavering commitment to protecting customer personal and financial information. We are dedicated to the safe collection, handling and use of data, all while ensuring confidentiality, integrity and availability. Old National takes these responsibilities very seriously and has established a comprehensive information security program led by our Chief Information Security Officer.

Information Security Policy & Standards

Old National demonstrates its commitment to safeguarding information by maintaining a robust information security policy and standards that are designed to protect our clients. The information security policy, benefiting from Board of Director level oversight and annual approval, establishes the objectives of our information security program and sets the foundation for its importance within the company. Program visibility is maintained through ongoing updates within executive and senior management committees. As required by laws and regulation, we undergo regulatory oversight and examination related to information security and privacy practices, as well as work with independent auditors to conduct examinations of our organization to ensure compliance.

Old National leverages several standards as a basis for best practice, including ISO 27001/27002 International Standards, National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and Federal Financial Institutions Examination Council (FIECC) Cybersecurity Guidance. Our information security standards are designed to align with internal risk-based frameworks and experience ongoing maintenance, including review and approval by management and a designated Standards and Controls Committee. The Information Security Standards are communicated and available to all Old National team members.

Risk assessments are conducted annually to identify the threats and vulnerabilities related to the information security environment using categories as defined by the areas noted in ISO 27001/27002, NIST CSF Framework and FFIEC Cybersecurity Assessment. Old National identifies and assesses both internal and external threats that could cause the misuse, alteration, destruction or unauthorized disclosure of customer information. In addition, ongoing third-party due diligence is performed to ensure appropriate security and privacy controls are maintained.

Information Security Partnerships

Old National partners closely with industry associations such as the American Bankers Association (ABA), Mid-Size Bank Coalition of American (MBCA) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) to keep abreast of an ever-changing threat environment. Old National continuously monitors for emerging risks through threat feeds from the Federal Cybersecurity & Infrastructure Security Agency (CISA), SANS Institute and other technology partners. Our partnerships help proactively

identify, prevent and detect cybersecurity events and enable us to better protect our clients. To encourage independent opinions, audits and tests of our security posture are regularly conducted by third parties including security professionals, auditors and regulators.

Security and Employee Engagement

Old National has established a company focus on information security, including a dedicated Information Security Department. Under direction of the Chief Information Security Officer (CISO), the Information Security Department has been appointed to discharge these responsibilities, along with the responsibility for overseeing the technical implementation of our Information Security Policy objectives and standards.

Our Code of Conduct, privacy and information security standards necessitate due care in the treatment of data and reinforce our commitment to safeguarding our customers and their information. Individuals who access bank network and information are required annually to acknowledge our code of conduct information user acknowledgment, which describes expectations of the information security program, and participate in security awareness training and ongoing security testing. Additionally, Old National has established an anonymous incident hotline that is communicated and available to all associates 24 hours a day, 7 days a week.

Compliance

Internal Audit
Information Security and Network Security are subject to audits from Old National's dedicated Internal Audit Department and independent audits of department policies, standards, guidelines, risk assessment and control testing.

Regulatory Compliance
Internal and external audits are also conducted as Old National is subject to the Gramm Leach Bliley Act (GLBA), the Healthcare Information Portability and Accountability Act (HIPAA), the Fair and Accurate Credit Transaction Act (FACT Act), the Identity Theft Red Flag Rules and Guidelines, Sarbanes Oxley 404, SEC, OCC and FFIEC requirements, as well as other legal requirements.