



INFORMATION SECURITY PROGRAM POLICIES AND PROCEDURES

Schmidt Mortgage Corporation's ("Schmidt") Mortgage Loan applicants have provided us with nonpublic personal information that is protected by Regulations promulgated by the Federal Trade Commission under the federal Gramm-Leach-Bliley Act (the "Regulations"). Therefore, we have established an information security program (the "Program") setting forth standards for maintaining administrative, technical and physical safeguards to: (1) ensure the security and confidentiality of protected nonpublic personal information; (2) protect against any anticipated threats or hazards to the security of such information; and (3) protect against unauthorized access to or use of such information.

A. Information Security Program Administrator.

1. Schmidt designates Vincent R. Schmidt (Greenville office) and Tammy R. Youngblood (Charlotte office) as the person(s) responsible for administering the Program (the "Program Administrator(s)"). As required by the Regulations, the Program Administrator(s) are responsible for Schmidt's information security compliance efforts and, accordingly, all inquiries from and reports by Schmidt's personnel pertaining to Schmidt's information security should be directed to the Program Administrator(s).
2. The Program Administrator(s) will be responsible for: (a) assessing existing risks to nonpublic personal information; (b) developing ways to manage and control such risks; (c) monitoring third-party vendor arrangements to ensure information security; and (d) testing and revising the Program in light of relevant changes in technology and threats to client information.

B. Identification of Internal and External Risks to Customer Information.

The Program Administrator(s) will review all foreseeable internal and external risks to information security with key company operations, management and risk control personnel in all areas of Schmidt Mortgage Corporation's operations. The Program Administrator(s) will assess the likelihood and potential damage of these threats, the sufficiency of any safeguards in place to control such risks and, where appropriate, revise policies and procedures to address such risks.

1. The Program Administrator(s) will meet with all Schmidt personnel periodically to review and implement the Program. The Program Administrator(s) will be available for questions from Schmidt personnel as to the application of the Program. Based upon the information gathered by performing risk assessments, and as changes in the laws or Regulations require, the Program Administrator(s) will assess the need for, and arrange for, training of Schmidt personnel, and will provide policy and procedure updates as may be necessary to ensure that the Program is properly implemented.
2. The Program Administrator(s) will ensure that Schmidt: (a) takes reasonable steps in selecting, maintaining, upgrading and periodically testing the security protections of the Information Systems (including physical protection, network firewalls, relevant software, information processing, storage, transmission, and disposal systems and arrangements); and (b) employs appropriate password protection and encryption of electronic information where necessary, including while such information is in transit or stored on a network or system to which unauthorized persons may have access.
3. The Program Administrator(s) will ensure that all information systems and networks containing, or otherwise affecting, protected information have appropriate access controls, as well as detection, prevention, and response mechanisms against attacks, intrusions, or other system failures that might materially affect the security of protected information.

C. Design and Implementation Safeguards.

Based upon the policies and procedures provided under the Program, the Program Administrator(s) will design and/or arrange for the provision of all necessary and appropriate technical and administrative safeguards for protected information and will regularly test and monitor the effectiveness of such controls, systems and procedures.

D. Vendor Arrangements.

The Program Administrator(s) will review all current and prospective vendor arrangements with respect to persons who, through their service to Schmidt, will receive, maintain, process or otherwise be permitted to access protected information. In reviewing such arrangements, the Program Administrator(s) will attempt to ensure that:

1. Schmidt selects and retains service providers who are capable of maintaining appropriate safeguards on protected information.
2. All contracts with service providers provide that the vendor must maintain the confidentiality of protected information and that protected information only be used as necessary under the vendor contract.

E. Evaluation and Update of the Program.

The Program Administrator(s) will periodically, as necessary or appropriate, revise or update the Program based on: (a) results of testing and monitoring pursuant to the Program; and (b) material changes to the business and operation of Schmidt.