LAWDESK

COMPLIANCE PROGRAM AND POLICY MANUAL

TABLE OF CONTENTS

REVISION CONTROL

VERSION NUMBER	CHANGE DESCRIPTION	AUTHOR	DATE
1.0	Original Manual	Allan Shutt	
1.1			
1.2			

COMPLIANCE PROGRAM AND POLICY

PURPOSE

Lawdesk ("Company") is committed to maintaining a high level of compliance with all consumer protection statutes and regulations, civil rights, fair lending laws, *Office of Foreign Assets Control* ("OFAC"), the *Bank Secrecy Act* ("BSA"), and avoiding *Unfair, Deceptive, or Abusive Acts or Practices* ("UDAAP"). Company believes keeping customers informed and treating them fairly is good business. Company also recognizes that failure to comply with laws and regulations can expose Company to substantial risks and penalties.

Company's policies, procedures and practices shall not in any way discourage persons from applying for credit, or discriminate against any person on the basis of age (providing the applicant has the capacity to enter into a legal contract), race, color, religion, national origin, sex, marital status, receipt of income from public assistance or maintenance programs, or a consumer's exercise of his or her rights under the *Consumer Credit Protection Act*.

Company's policy of nondiscrimination shall cover all aspects of Company's services, including requests and inquiries; taking and processing applications; the consideration, granting, servicing, and collection of extensions of credit; underwriting standards; and fixing loan and service rates, terms and conditions.

Company's application forms shall request only information permitted by law. Procedures shall be established and adhered to by all staff to ensure credit applications are processed promptly in accordance with regulations, and all appropriate disclosures for credit are accurate and provided within required time frames.

RESPONSIBILITY OF ALL PERSONNEL

It is Company's policy to fully comply with federal and state laws and regulations covering all aspects of its operation. Each officer and employee of Company shall ensure they familiarize themselves with Company's policies and procedures and the requirements of all laws and regulations affecting his or her job responsibilities. Each employee is expected to carry out his/her responsibilities, at all times, in a manner that complies with applicable regulatory requirements, and Company's policies and procedures, as amended from time to time.

All personnel shall report any known or suspected compliance violations to the Chief Compliance Officer, Compliance Department, and/or BSA Officer if it is BSA related.

AUTHORITY AND RESPONSIBILITIES OF CHIEF COMPLIANCE OFFICER

The Board of Directors of Company shall appoint a Chief Compliance Officer who is charged with implementing the Compliance Program outlined in this policy. The Compliance Program shall include developing compliance training materials to assist departmental training needs, monitoring compliance exceptions, and reviewing internal and external compliance audits to determine additional training needs. The Compliance Program also includes Compliance review

and approval of all marketing material for Company's products and third-party products, and Compliance Department participation in all aspects of new product design, existing product changes, marketing and fulfillment channels, including direct mail campaigns, website design, telemarketing and fulfillment scripts, IT product development/changes, etc. Other processes designed to ensure compliance with consumer laws regulations will also be included in the Compliance Program portion of this document.

This Compliance Policy and Compliance Program will be reviewed and approved by Executive Management and submitted to the Board for approval on an annual basis. Modifications to the Compliance Program may be recommended by the Chief Compliance Officer from time to time, as deemed appropriate based on the needs of Company, provided that the Program continues to include the minimum standards identified in this document.

The Compliance Department staff shall have access to all departments and documentation that may be necessary to carry out their responsibilities. The Compliance Department shall have the authority to implement corrective action upon discovering actual or possible violations. Any actions will be discussed with Executive Management and the Board of Directors, as applicable.

RESPONSIBILITIES OF DEPARTMENT HEADS

Procedure Manuals

All Department Heads will be responsible for ensuring their department staff is educated in any regulatory requirements relating to their job functions. In addition, they are also responsible for:

- Updating procedure manuals.

- Ensuring new personnel receive compliance training appropriate to their job functions, appropriate existing personnel receive compliance training when regulations change or when new regulations are added, when audit and examinations reveal non-compliance or compliance weaknesses, and when compliance-related functions are transferred to different personnel or different units within their departments. (See "Compliance Training" section).

- Compliance training can be accomplished through internal departmental training programs or through targeted training conducted by the Compliance Department. Compliance will assist in the training process to the extent the Compliance Department and the Department Head deem appropriate or necessary.

- All Compliance training is to be documented and provided to the Compliance Department for inclusion in training records and provided to regulatory examiners or auditors upon request.

COMPLIANCE PROGRAM

The Chief Compliance Officer is responsible for coordinating and administering the Compliance Program. While he/she is responsible for its coordination and oversight, each department or function manager will be accountable for compliance in his/her own area of responsibility. Likewise, each employee will be responsible and accountable for ensuring that his/her own work complies with all applicable rules and regulations, and that all applicable policies and procedures are followed.

Company's Compliance Program, which shall include review of internal and external audit reports, focusing on violations of applicable consumer protection laws and regulations and/or exceptions to Company's policies and procedures affecting compliance with such laws and regulations. Information regarding violations and exceptions in these reports will be used to determine training needs. The Compliance Department will coordinate additional training with the Department Head to determine appropriate action, as discussed below under "Compliance Training."

Internal Controls

All Department Heads should ensure similar or enhanced internal controls covering all regulatory issues affecting their departmental functions are implemented and enforced to minimize risk of violation, regulatory criticism, or enforcement action, and legal risk.

Compliance Committee

A Compliance Committee, consisting of Executive Management and their Department Head designees, will meet at least quarterly and will be chaired by the Chief Compliance Officer. The Chief Compliance Officer will present for review the status of corrective action on errors/issues identified in internal or external audits or covered in working memos that have regulatory impact. Members of the Committee shall also report any errors/issues they are aware of that have not yet been reported to the Compliance Department. Discussion of these items will include corrective action taken or to be taken to prevent recurrence and estimated implementation dates. Compliance issues that have not been corrected may require more frequent follow-up meetings. Regulatory bulletins or other notices regarding new or changing regulations affecting Company will also be covered in these Committee meetings. This forum will also be used to address compliance questions or compliance related issues that require clarification. Minutes will be recorded and disbursed to Compliance Committee members and made available for discussion at Board meetings.

Internal/External Compliance Resources

The Compliance Department will provide guidance as necessary or upon request to all departments of Company regarding consumer regulatory issues, and as necessary, will obtain the assistance/opinions of Company's Chief Legal Officer and/or outside legal counsel to resolve compliance questions. The Compliance Department will maintain adequate resource materials to research compliance issues, such as an updated regulatory service covering federal banking

regulations and access to electronic versions of regulatory bulletins and notices, and is responsible for ensuring that Department Heads are informed of regulatory changes and/or new regulations affecting Company's operations.

Communications Review and Approval

All communications to be provided to consumers and customers, in connection with any credit product must be reviewed and approved by appropriate Department Heads, and must be submitted to the Compliance Department for review and approval. Communications requiring approval include (but are not limited to) application language, disclosures, loan agreements, letters informing customers of approval, denial or incompleteness of an account application, change in terms notices, website pages, phone scripts, and all other such communications.

If a communication is determined to be in noncompliance, Department Heads shall be responsible for ensuring that corrections are made promptly, and shall also be responsible for ensuring that any obsolete communications are removed from circulation and destroyed.

Regulatory Liaison

The Chief Compliance Officer will coordinate with regulatory examiners during compliance exams, furnish them with requested information, and shall act as the primary examination contact.

Internal and External Compliance Audit Liaison

The Chief Compliance Officer will coordinate with internal or external auditors during internal or external compliance audits, provide external auditors with requested information, and shall act as the primary audit contact.

Legal Counsel Liaison

As deemed necessary or appropriate, the Chief Compliance Officer shall seek the advice of Chief Legal Officer and/or outside counsel regarding regulatory or legal matters, which cannot be resolved. As appropriate, the Chief Compliance Officer will communicate information received from the Chief Legal Officer and/or outside counsel to executive management and Department Heads.

COMPLIANCE TRAINING

New Hire and Required Annual Training – The Compliance Department has identified specific regulatory issues that need to be addressed during New Hire Orientation, such as Bank Secrecy Act, Privacy, and Information Security. Each Department will have minimum training requirements within their given area of responsibilities. The Human Resources Director, Bank Secrecy Officer, and the Information Security Officer are responsible for ensuring that Compliance Department approved material is presented and reviewed with new employees during New Hire Orientation.

In addition, annual Bank Secrecy Act and Information Security training is required for all staff. Updated policies may be provided to Department Heads every year by the Compliance Department. The Department Head is responsible for ensuring all department staff receive and acknowledge receipt of the new policies, and the documents are reviewed in a training session. Compliance will assist in presenting this annual training or training will be conducted by the department's designated trainer, as deemed appropriate by the Department Head. The Department Head is responsible for requesting assistance from the Compliance Department in conducting training if needed.

General Compliance Training – Department Heads are responsible for ensuring that all staff in their departments are properly trained regarding compliance with consumer laws and regulations affecting their departmental functions. Department Heads are responsible for ensuring that policies and procedures covering their departments include all applicable compliance issues in accordance with Guidelines provided by the Compliance Department. Compliance training can be conducted using the departmental policies and procedures, or targeted training conducted by the department-designed trainer or Compliance Department staff, as deemed appropriate by the Department Head. The Department Head is responsible for requesting assistance from the Compliance Department with respect to conducting training, training the department-designated trainer, or developing a departmental training program.

Additional Training Needs Evidenced by Audit Results – The Compliance Department will assess additional or enhanced training needs based on review of violations or exceptions noted in internal or external audit reports. Compliance will coordinate implementation of additional training with the Department Head to determine the best course of action to meet the department's training needs. All such training discussions and decisions will be documented for reporting to the Compliance Committee and the Board of Directors Audit Committee, and to regulatory examiners upon request. Training may be conducted by Compliance staff, department designated trainer, or external trainer and/or training tools, as deemed appropriate by the Department Head and Compliance staff. If appropriate, the Compliance staff will conduct training with the department-designated trainer (train-the-trainer), who will, in turn, conduct training with the department staff.

Training Recordkeeping – All Compliance training is to be documented and provided to the Compliance Department for inclusion in training records and provided to regulatory examiners or auditors upon request. Training status report will also be disbursed and discussed at all Board meetings.

WEB SITES

Company's Compliance Policies and Guidelines shall also apply to all Web Sites. The applicable laws and regulations include, but are not limited to, the following:

- Truth-in-Lending Act, Regulation Z ("TILA")
- Dodd-Frank Act's Unfair, Deceptive or Abusive Acts or Practices

- Sections 5 and 12 of the Federal Trade Commission Act ("FTCA")
- Equal Credit Opportunity Act, Regulation B ("ECOA")
- Fair Credit Reporting Act, Regulation V ("FCRA")
- Gramm-Leach-Bliley Act, Regulation P ("GLBA")
- Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act")
- Bank Secrecy Act/Customer Identification Program ("BSA"/"CIP")
- Office of Foreign Assets Control ("OFAC")

Links to Third-Party Web Sites

If Company provides links to third-party web sites, Company's Web Sites shall include the following or substantially similar language recommended by the OCC Bulletin 2003-15:

- Company is not endorsing or guaranteeing the products, information, or recommendations provided by linked web sites.

- Company is not liable for any failure of products or services advertised on those linked web sites.

- Each third-party web site may have a privacy policy different than that of Company.

- The linked third-party web sites may provide less security than Company's web site.

Website Record Retention

Company's retention policy shall be to retain the web site content in electronic media files or hard copy for a period of three years. The retention process shall enable the Company to easily retrieve the web sites' content if requested.

MARKETING REVIEW

All employees involved in the development of new products or making changes to existing products and/or marketing and fulfillment channels are responsible for ensuring that any regulatory requirements and compliance issues for those products and marketing and fulfillment channels are addressed. All new products and changes to existing products and marketing and fulfillment channels must be submitted to Compliance for review and approval prior to implementation.

Final documentation for all new products, changes to existing products, and new or changed marketing and fulfillment channels, including but not limited to, Company's Web Sites, direct mail, telemarketing and telephone fulfillment scripts must be submitted through the Compliance Approval process and receive approval prior to use.

The Compliance Approval process also applies to marketing of third-party products or services offered to Company customers via telephone, website advertising, statement messages, statement or solicitation inserts, etc.

The Chief Compliance Officer is authorized to waive the sign-off of the Compliance Approval process if he/she determines that changes to existing product documentation is minor and is not significant enough to warrant submission to the Compliance Approval process.

COMPLIANCE AUDITS

Company is responsible for developing a Compliance Audit schedule, approved by the Board of Directors, each year. The schedule will include the below listed consumer regulations, as appropriate to Company's products and services, and audit frequency will be annually. Audits will be conducted by the internal Compliance staff or outsourced to external auditors, as deemed appropriate by the Chief Compliance Officer. Compliance Committee meetings and quarterly Compliance Reports to the Audit Committee will include a recap of compliance audit findings and the status of any corrective action.

If compliance audit findings indicate a need for additional compliance training, Compliance will coordinate additional training plans with the Department Head to determine appropriate steps to provide additional staff training as discussed in this document under "Compliance Training."

Consumer Regulations that may be included in the Audit Schedule:

- Bank Secrecy Act ("BSA")
- Office of Foreign Assets Control ("OFAC")
- Federal Right to Financial Privacy Act ("RFPA")
- Equal Credit Opportunity Act, Regulation B ("ECOA")
- Fair Credit Reporting Act, Regulation V ("FCRA")
- Privacy of Consumer Financial Information, Regulation P ("Privacy Rule")
- Servicemembers Civil Relief Act Policy ("SCRA")
- Truth in Lending Act ("TILA")
- Telephone Consumer Protection Act ("TCPA")
- Unfair, Deceptive or Abusive Acts or Practices ("UDAAP")
- CAN-SPAM Act
- Electronic Signatures in Global and National Commerce ("E-SIGN")
- Social Media
- Vendor Management Program
- Fair Debt Collections Practices Act, Regulation F ("FDCPA")
- Identity Theft Protection Program

POLICIES AND PROCEDURES

Department Heads are required to provide the Compliance Department with a copy of any proposed new or revised policy or procedure impacting regulatory compliance prior to implementation of such new or changed policy or procedure.

Company's Board of Directors must approve all new and revised policies. The Board of Directors authorizes Company's Chief Compliance Officer to review and approve Guidelines implementing policies.

General procedures may be implemented or revised by Department Heads without review and approval by the Board of Directors. For example, a Department Head may implement or revise written procedures that outline the steps necessary to perform transactions in the computer system. However, any procedure that impacts compliance with regulatory requirements, such as changing terms and conditions of an account, changing fees or rates applicable to credit, or changing the timing or content of customer notices, requires the prior review and approval of the Chief Compliance Officer.

BANK SECRECY ACT OFFICER

The Board shall annually review and approve Company's Bank Secrecy Act ("BSA") Policy and appoint a Bank Secrecy Act Officer ("BSA Officer") for Company.

All loans originated through Company's platform will be made by County Bank, a Delaware state-chartered bank who is also regulated by the FDIC (the "Bank"). Company provides services to the Bank in connection with the origination of such loans (the "Loan Account Program" or "Program") and Company services loans made to the Bank consumers on behalf of registered loan buyers who purchase such loans. In connection with the Program, Company will develop, administer, and maintain the following policies for compliance with the BSA, including record keeping and reporting requirements.

The BSA officer will report any Suspicious Activity Report ("SAR") notices submitted to the Bank for further investigation, at the next regular Board meeting after such notices are submitted to the Bank. The BSA officer will also provide the Board with an annual report of BSA activities and training.

INFORMATION SECURITY OFFICER

The Board shall appoint an Information Security Officer for Company, who shall be responsible for security procedures under Company's Security Program. The Information Security Officer will report annually to the Board on the implementation, administration, and effectiveness of the Security Program.

COMMUNITY REINVESTMENT ACT

While not required, the Board may appoint a Community Reinvestment Act ("CRA") Officer, who will be responsible for developing and administering a CRA plan in accordance with Company's desire to engage in community development services, provide technical assistance on financial matters to nonprofits, or provide other community services.

ADDITIONAL RESPONSIBILITIES OF THE COMPLIANCE DEPARTMENT UNDER THIS PROGRAM

Customer Complaints

The Compliance Department will review complaint reports to determine if there are complaint trends that indicate a need for targeted compliance training or procedural changes. Compliance will also participate in weekly meetings with departments, during which specific complaints received from or through a federal or state regulatory agency, Company, the Better Business Bureau ("BBB"), or state law enforcement agencies will be reviewed. The purpose of these meetings is to determine if any of the complaints indicate a need for procedural changes, or represent potential violation of consumer regulations requiring corrective action.

Suspicious Activity Report ("SAR")

The BSA Officer is responsible for the notification of suspicious activity to the Bank under the BSA. All employees are instructed to advise the BSA Officer, Chief Compliance Officer, or one of the Compliance staff in the event they detect suspicious activity in accordance with the BSA Policy. The BSA Officer is responsible for reviewing the reports and determining if a SAR Notice to the Bank for regulatory filing is necessary or appropriate. If so, the reporting of the SAR Notices will be processed by the BSA Officer. Compliance will provide a recap of SAR Notices that were provided to the Bank to the Board quarterly. *See* the BSA Policy.

USA PATRIOT Act, Section 314a Reporting

The Compliance Department is aware of a Bank's responsibility for establishing a system to monitor Section 314a lists of potential terrorists and reporting to FinCEN if a positive match is identified. Company understands that this information is required to be kept strictly confidential. Thus, Company does not do the request for information and reporting, it is done by County Bank. *See* the BSA Policy.

OFAC Compliance

The Compliance Department is responsible for establishing a system to monitor OFAC lists of potential terrorists, drug traffickers, blocked persons, etc., and communicating with OFAC when a positive match is identified. *See* the OFAC Policy.

Bank Secrecy Act

The Compliance Department is responsible for ensuring a BSA policy is developed and implemented that includes all requirements of the Act, including SAR, OFAC and section 314a reporting, anti-money laundering policy, etc. The BSA Policy will be reviewed and approved by the Board annually, and annual training will be conducted for all employees. *See* the BSA Policy.

Privacy Policy and Privacy Notice

The Compliance Department is responsible for ensuring Company's Privacy Policy and Privacy Notice to customers is reviewed, amended as necessary, approved by the Board, and provided to Company's customers at least annually.

Disclosure Statements and Notices

The Compliance Department is responsible for developing, disclosure statements, loan agreements, arbitration agreements, privacy notices, change in terms notices, and any other notices or legal documentation for Company's credit products. As necessary, such documents will be reviewed by the Chief Legal Officer or outside legal counsel.

BANK SECRECY ACT POLICY

PURPOSE

The provisions of the Bank Secrecy Act Policy are in adherence to the *Currency and Foreign Transactions Reporting Act of 1970*, which legislative framework is commonly referred to as the "Bank Secrecy Act" or "BSA." The BSA requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the BSA requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. The BSA is sometimes referred to as an "anti-money laundering" law ("AML") or jointly as "BSA/AML."

Several AML acts, including provisions in Title III of the USA PATRIOT Act of 2001, have been enacted up to the present to amend the BSA.

SCOPE

The BSA imposes reporting requirements for large currency and foreign transactions, customer identification, and record keeping requirements for transactions involving the cash purchase of monetary instruments. BSA requires that procedures be in place to detect suspicious transactions and report such transactions to law enforcement agencies. BSA violations can result in civil, monetary and criminal penalties. Real or personal property traceable to illegal drug sales or purchased with laundered money is subject to government seizure and forfeit, including property held by Company as collateral.

Company provides a consumer-lending platform that facilitates loans between consumers and loan buyers. Company is committed to complying with all applicable provisions of the AML regulations and BSA.

As previously mentioned, all loans originated through Company's platform will be made by a Bank (the "Bank"). Company provides services to the Bank in connection with the origination of the Loan Account Program and Company services the loans made to the Bank consumers on behalf of registered loan buyers who purchase such loans. In connection with the Program, Company will develop, administer, and maintain the following policies for compliance with the BSA, including record keeping and reporting requirements.

POLICY

Under the BSA, banks and other institutions that are vulnerable to money laundering are required to take several precautions against financial crime. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 in daily aggregate amounts, and to report suspicious activity that may indicate that money laundering, tax evasion, or other criminal activities are taking place.

Reports from financial institutions are submitted to the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). FinCEN collects and analyzes the information submitted to support law enforcement investigations and provide U.S. policy makers with strategic analyses of domestic worldwide money laundering developments, trends, and patterns.

Currency Transaction Reports

Under the BSA, a Currency Transaction Report ("CTR") must be completed and filed any time a financial institution engages in a "transaction in currency" that exceeds $10,000. According to the law, a "transaction in currency" occurs every time a person or a business deposits, withdraws or exchanges more than $10,000 in cash.

The meaning of "currency" in this context is the coin and/or paper money of any country that is designated as legal tender by the country of issuance. The definition is specifically limited to physical transfers of cash, either in or out of a financial institution. The transaction must involve actual currency to be reportable. Deposits or withdrawals by check and other non-cash transactions are not subject to CTR filing requirements.

In addition, CTRs are only required when a physical transfer or exchange occurs. As such, mere transfers between accounts, wire transfers, and other operational transactions that do not involve the physical transfer of cash are not subject to CTR filing requirements.

Company does not deal with cash. Company uses the Automated Clearing House ("ACH") network, wire transfers, checks, or bank drafts for all transmissions of funds into and out of its accounts and the accounts of its consumers and loan buyers. Therefore, Company does not participate in physical transfers or exchanges of funds and as a result is not required to submit CTRs.

CUSTOMER IDENTIFICATION

In response to the terrorist attacks that took place on September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"). Title III of the PATRIOT Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.

Among other things, Section 326 of the PATRIOT Act supplements the existing BSA framework by firming up customer identification procedures and establishing minimum procedures for identification verification for all new accounts.

Definitions

The following terms in this Policy shall have the same meanings as the meanings found in the Department of Treasury's Customer Identification Program ("CIP") Regulations.

Account - Account means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services.

Account does not include - a product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order; an account that Company acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or an account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

Customer - A customer is (A) A person that opens a new account; and (B) An individual who opens a new account for: (i) An individual who lacks legal capacity, such as a minor; or (ii) An entity that is not a legal person, such as a civic club. For purposes of this definition, a customer can be an individual, corporation, partnership, trust, estate, joint stock company, association, syndicate, joint venture, other unincorporated group, certain Indian Tribes, or any recognized legal entity. A customer does not include a person that has an existing account with the financial institution, provided the institution has a reasonable belief that it knows the true identity of the person.

Under this definition, Company has two types of customers: consumers and loan buyers. Borrowers can be any person who is a U.S. resident in a state where the Bank, is licensed or otherwise authorized or permitted to lend. Loan buyers can be any Accredited Investor as that term is defined under the Securities Act of 1933.

Customer Identification

When a consumer registers for an individual account (i.e. when a consumer applies for a loan via the Company loan application process), he or she provides Company with his/her name, Social Security Number or Individual Taxpayer Identification Number, date of birth, primary physical street address (either residential or military), contact phone number, email address, and bank account number and routing number.

Verification of Customer Identity

Company uses a variety of documentary and non-documentary methods during the account set-up process, and prior to the loan account being established, to verify the identity of our customers.

At the time a consumer applies for a loan:

Email Verification - First, Company sends an email to the consumer at the email address he/she enters in the loan application. This email contains a link that must be clicked-through to activate the account. The only consumers who can open an account are those who have received this

email and clicked-through on the link in its body. In certain circumstances a manual verification of the email address may be required.

Verification of Personally Identifiable Information - Company verifies Personally Identifiable Information ("PII") provided by the consumer against data on file with credit reporting agencies and other identity and anti-fraud verification databases, including OFAC. In order to successfully pass this verification, the consumer's PII must be able to match a high degree of such information as it is presented.

Knowledge-Based Authentication - Each consumer may also be verified through Knowledge-Based Authentication. Each consumer is asked a series of personal questions supplied from data sources, which could include their credit profile, public records, and possibly other sources. These questions are designed so that only the actual individual to whom they pertain would know the appropriate responses—they are often referred to as "out of wallet questions."

Company uses a risk-based approach to the level of verification a consumer undergoes, as additional verification measures are taken depending on the accuracy of the information the consumer provides and the data we collect on the consumer throughout the loan application process.

At the time a consumer applies for a loan, the following additional verification steps *may* be requested:

Address Verification - a security postcard containing an address verification code may be sent to the consumer's input mailing address. To receive a loan, the consumer must retrieve the postcard and enter the code prior to loan origination. Additional steps are taken when the address provided by the applicant is different than the address shown on the photo identification. A copy of the applicant's current utility bill or other relevant document may be requested which reflects the applicant's name and current address. An applicant's verbal acknowledgement of an address variation may be sufficient when other evidence corroborates the stated address.

Bank Account Ownership Verification - Company takes reasonable steps to verify that the consumer is an authorized owner of the bank account to which loan funds will be transferred. Depending on the bank the consumer uses, Company will either:

- Verify that the consumer is an authorized owner of the bank account,
- Request a check or bank statement from the consumer that lists them as the named owner of the account; or
- Initiate small (less than $1.00), offsetting debit and credit transactions in the bank account and ask the consumer to provide the amount of the transaction.

Employment Verification - Based on risk characteristics of the loan request, some consumers are flagged for employment verification. If the account is flagged for employment verification,

Company will attempt to confirm the consumer's employment status by contacting the employer named by the consumer. Some consumers may also be asked to provide documented employment verification such as paystubs or a letter.

Income Verification - Based on risk characteristics of the loan request, some consumers requesting a loan are flagged for income verification. Income verification is completed by document verification and may require the consumer to provide a copy of their paystub(s) or previous year's W2. Alternatively, Company may require the consumer to submit one or more federal income tax returns, or complete a form authorizing Company to obtain a copy of their electronic IRS 1040 transcripts.

Phone Verification/Fraud Screen - Based on risk characteristics of the loan request, some accounts requesting a loan may be flagged for phone verification and/or fraud screening. Additional fraud screening may be employed when the consumer is on the phone.

A consumer's failure to pass any of the above verification procedures will result in:

- Escalation of document verification procedures; and/or
- Denial of the loan request.

Verification of Borrower Identity via Documentary Methods

At any time during the loan application process, a consumer could be flagged for document verification based on various pre-determined risk factors.

In the event an account is flagged, Company may request that the consumer provide the following documents:

- **Driver's License or Government-Issued Identity Card** - A close-up picture of the photo identification is also requested to enable required recordkeeping of the photo identification, which includes state of issuance, issue date, and expiration date.
- **Voided check or bank statement.**
- **Additional Information -** Depending on the level of verification and the risk associated with the transaction, the consumer may be asked to supply the following:
    - Social Security card
    - Authorization to retrieve IRS Electronic Transcripts
    - Current pay stub and their most recent W2
    - Utility bills or bank statements showing primary address
    - U.S. Passport or Green Card
    - Military ID card and Orders of Deployment

- **Due diligence for U.S. Resident Aliens –** If the applicant may be a permanent resident alien in the United States, as indicated by the applicant's admission, by consumer database records, or by risk alerts, the following documentary evidence will be requested to determine the applicant's immigration status:

    - Social Security card
    - U.S. Passport, U.S. Birth Certificate, Green Card, or U.S. Naturalization Certificate

Recordkeeping

A record for each Customer that includes all identifying information must be made and maintained for **five years** *after* the Customer's Account is closed. A record for each Customer includes:

- A description of any document used for verification of identity, including any identification number, place of issuance and, if any, the date of issuance and the expiration date;

- A description of the methods and results of any non-documentary measures undertaken to verify the identity of the customer; and

- A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained from a customer must be made and maintained for five years after the record was made.

- The amount of the loan applied for, as well as an address, IP geolocation, or notations indicating Company's understanding of the applicant's physical location. Together, these elements provide a capability to determine whether an application greater than $10,000 was received from a person outside the U.S.

Customer Notice

Pursuant to Section 326 of the PATRIOT Act, financial institutions are required to provide customers with adequate notice that the information being requested is being used to verify their identities.

Company's verification process requires consumers who are submitting loan applications to expressly authorize Company, on behalf of the Bank, to obtain information from the consumer's credit profile with a credit reporting agency to confirm the consumer's identity and avoid fraudulent transactions in the consumer's name.

Moreover, Company provides a notice of *Important Information about Procedures for Opening a New Account* in accordance with the regulations implemented by Section 326. This notice is provided as part of the application process. See the below notice language:

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To assist the government in fighting the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account with us.

This means that when you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. In addition, we may also ask to see your driver's license or other identifying documents.

OFFICE OF FOREIGN ASSETS CONTROL POLICY

The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under US jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

In general, these regulations:

- Require blocking of accounts and other assets of specified countries, entities, and persons; and

- Prohibit unlicensed trade and financial transactions with specified countries, entities, and persons.

Company, on behalf of the Bank, submits all new loan application information to TransUnion's Identity Manager System, which will flag any new loan application that contains a possible match to the OFAC Specially Designated Nationals ("SDN") List and OFAC Consolidated Non-SDN Lists. TransUnion provides this service as part of its contract with Company. Possible matches to the list are flagged for manual review by a verification agent. If manual verification *confirms* the match, Company, on behalf of the Bank, will deny the loan application.

All full and accurate records of each rejected transaction are kept for a period of at least **five years** after the date of the transaction and, for blocked property (including blocked transactions) records will be maintained for the period the property is blocked and for five years after the date the property is unblocked.

See the specific *OFAC Policy* within this Compliance Program and Policy Manual.

KNOW YOUR CUSTOMER POLICY

Company, on behalf of the Bank, employs a risk-based approach to the customer identity diligence process. These procedures allow Company to form a reasonable belief that it knows the true and accurate identity of its customers. Any consumer that fails any stage of the outlined verification procedures, or that is flagged for other risk factors, is manually reviewed by Company's Loan Operations team. This team has the ability and authority to request additional information and/or documentation on a case-by-case basis. In addition, all loan buyers are verified as part of Company's loan buyer registration process, which requests sufficient data to develop an understanding of normal and expected activity for the loan buyer's business operations. The individuals performing these reviews will be trained to recognize key risk factors for money laundering.

The following risk factors are assessed for consumers requesting a loan:

- Identity Verification Results (Match to Data and Answers to Out of Wallet Questions)
- Credit Profile Data
- Loan Size

Much of the Customer Due Diligence ("CDD") information is confirmed through a credit reporting agency, bank verification, and correspondence and telephone conversations with the consumer. Company may take additional measures such as obtaining third-party references or researching public information (i.e., internet or commercial databases).

Pursuant to Federal law, CDD policies and procedures should be commensurate with the institution's BSA/AML risk profile, with special attention to high-risk customers. Pursuant to Federal Financial Institutions Examination Council ("FFIEC") guidelines, Company's AML risk is relatively low because it offers limited products and services, loans are made to individuals only, and loans are only made to residents of the United States.

SUSPICIOUS ACTIVITY MONITORING AND REPORTING

Banks are required to report suspicious activity that may involve BSA violations, terrorist financing, money laundering, and certain other crimes above certain dollar amount thresholds.

Any consumer that fails any stage of Company's verification procedures, or that possesses other risk factors, is manually reviewed by Company's Loan Operations team. If Company knows, suspects, or has reason to suspect, (1) insider abuse (in any amount), (2) any suspicious transaction involving a violation or attempted violation of federal law of $5,000 or more when a suspect can be identified, (3) any suspicious transactions involving a violation or attempted violation of federal law aggregating $25,000 or more regardless of a potential suspect, then Company will aid the Bank in filing its Suspicious Activity Report ("SAR") by providing sufficient information for the Bank to complete its FinCEN SAR.

Company will create and maintain sufficient operational Guidelines and procedures to allow its employees to identify red flags for suspicious activity, including when transactions are:

- Intended or manufactured to hide or disguise funds or assets derived from illegal activity,
- Obtained from illegal activity,
- Transacted with no business or lawful purpose,
- Transacted with no reasonable explanation for the transaction after examining available facts including the purpose and background of the transaction,
- Designed to eschew any reporting requirements of the BSA,
- Not the kind the customer normally engages in,
- Actual or attempted identity theft; or
- Fraudulent information submitted on an application.

If any suspicious activity is detected, a referral will be made promptly to the Bank to enable a timely FinCEN SAR to be filed. SARs are required to be electronically filed through the BSA E-Filing System no later than **30 calendar days** from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time for filing a SAR is **extended to 60 days**.

If there is continued activity on a previously reported SAR, a continuing SAR must be filed within **90 to 120 days**. Company will report any continuing activity to the Bank to facilitate a continuing SAR filing, if applicable.

As required by law and subject to penalty, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR. Company, its officers, directors, employees, and agents will not notify any person involved in the suspicious transaction that information has been provided to the Bank for purposes of filing a SAR, or that a SAR has been reported. Company will ensure confidentiality of all such reports to the Bank and will limit knowledge of such referrals on a business-need-to-know basis.

All supporting documentation provided to the Bank for purposes of filing a SAR shall be retained by Company for five years from the date the information was reported.

FINCEN INFORMATION REQUESTS

Section 314(a) of the PATRIOT Act allows law enforcement agencies to work in conjunction with the Financial Crimes Enforcement Network ("FinCEN") to require a financial institution to search its records to determine whether it maintains or has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

When the Bank receives an information request, the Bank (not Company) will conduct a one-time search of its records to identify accounts or transactions of a named suspect.

The Bank will search its records for current accounts, accounts maintained during the preceding 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. The Bank must report any positive matches to FinCEN within **14 days**.

TRAINING

The BSA Officer is to ensure Company associates are trained in the AML compliance requirements that affect their job functions. The training also includes Company's own internal BSA policies and procedures, including the CIP, required recordkeeping, suspicious activity referrals to the funding bank, and any other anti-money laundering policies and procedures. Training will be conducted at least annually and basic training within 10 days of hiring for employees with BSA/AML/OFAC responsibilities.

Training records will be maintained of all participants to document compliance with this requirement.

INDEPENDENT TESTING OF COMPLIANCE

Company will implement a system of independent testing for compliance with applicable law at least annually. This testing may be done by internal or external personnel, or a combination of both, if it is conducted by persons independent of the area being tested.

At a minimum, the testing will include the following elements:

- Attest to the overall integrity and effectiveness of management systems and controls, and BSA technical compliance.
- Test transactions in all areas of Company with emphasis on high-risk areas to ensure Company is following prescribed regulations.
- Assess employees' knowledge of regulations and procedures.
- Assess adequacy, accuracy, and completeness of training programs.
- Assess adequacy of the CIP and the process for identifying suspicious activity.

The findings of the testing are to be reported promptly to Company management and Company's Board of Directors and, as appropriate, the funding bank. In areas in which deficiencies are found, follow-up testing will be conducted to ensure the deficiencies are corrected.

BSA/AML OVERSIGHT

The Chief Compliance Officer is designated with primary oversight of Company's BSA/AML compliance responsibilities related to Company's partnership with the Bank. Personnel with day-to-day compliance responsibilities are designated by the BSA Officer and clearly communicated to them as part of their ongoing position responsibilities.

OFFICE OF FOREIGN ASSETS CONTROL POLICY

PURPOSE

The provisions of the Office of Foreign Assets Control Policy are in adherence to the *Office of Foreign Assets Control* ("OFAC") the laws and regulations. OFAC is part of the United States Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

SCOPE

Financial institutions (as well as all U.S. persons and entities) must monitor all financial transactions performed by or through them to detect those that involve any entity or person subject to the OFAC laws and regulations. In most situations, a financial institution should accept deposits and funds subject to OFAC regulations, but freeze the funds and accounts, so that absolutely no funds can be withdrawn. There are a few situations that require the financial institution to reject the transaction or funds instead of accepting and blocking them.

POLICY

The Chief Compliance Officer is designated with primary oversight of Company's OFAC compliance responsibilities. Personnel with day-to-day compliance responsibilities are designated by the BSA Officer and the compliance responsibilities are clearly communicated to them as part of their ongoing position responsibilities.

The policy of Company is to comply with economic sanctions and embargo programs administered by OFAC. The rules require blocking of accounts and assets of countries identified as being a threat to national security, including accounts and assets of the sanctioned countries' governments, and sometimes involve nationals of the sanctioned countries. The rules also prohibit unlicensed trade and financial transactions with such countries. Treasury has identified certain individuals and entities located around the world that are acting on behalf of sanctioned country governments who must be treated as if they were part of the sanctioned governments (also known as Politically Exposed Persons or PEPs).

Company must block funds transfers that are remitted by or on behalf of a blocked individual or entity, are remitted to or through a blocked entity, or are remitted in connection with a transaction in which a blocked individual or entity has an interest. A payment order cannot be cancelled or amended. Company is required to execute the payment order and place the funds in a blocked account, which may be released only by specific authorization from Treasury.

Payments or transfers that are received and blocked or rejected by Company are required to be reported to OFAC within 10 business days from the date that property becomes blocked. A comprehensive report on all blocked party held as of **June 30** of the current year must be filed annually by **September 30** and OFAC requires the retention of all reports and blocked or rejected transaction records for **five years**.

The BSA officer is responsible for ensuring updated OFAC lists of "Specially Designated Nationals and Blocked Persons" and "Country Sanctions Programs" are reviewed as changes are issued by OFAC. The BSA officer is also responsible for monitoring when a name match is detected on loan applications. If a name match cannot be eliminated based on other identification criteria, the BSA Officer is responsible for OFAC compliance are required to report the match to OFAC and/or obtain OFAC guidance on what actions to take on the account, and documenting such guidance.

Customer names of all new loan applicants and new hires are verified against the OFAC list as outlined in OFAC Guidelines. Company performs periodic verifications of the customer database against the OFAC list on behalf of loan buyers.

In the event, any employee identifies a positive match on an existing account, new account request, or wire transfer affiliated with any person or entity on the listing, the BSA officer is to be notified immediately for appropriate contact with the OFAC Compliance Hotline. The OFAC Compliance Hotline will provide instructions for proper account disposition: reject, block, or continue with the account relationship.

OFAC PENALTIES

Severe civil and criminal penalties, which may be imposed for non-compliance with the various OFAC laws and regulations. For example, penalties may be imposed up to the following for each occurrence:

Most fines historically imposed by OFAC have been civil penalties related to failure to block illicit wire transfers. However, non-compliance with any requirement under Company's OFAC compliance program subjects us to penalties by OFAC, as well as reputation risks. See below chart for a list of civil and criminal penalties:

LAW/COUNTRY	IMPRISONMENT	CORPORATE FINE	INDIVIDUAL FINE	CIVIL PENALTY
Trading with the Enemy Act – North Korea	10 Years	$1,000,000	$250,000	$65,000
Economic Powers Act – Sudan, Iran, Syria, Burma, Balkans, Zimbabwe	20 Years	$500,000	$250,000	$50,000
Iraqi Sanctions Act	12 Years	$1,000,000	$1,000,000	$325,000
Foreign Narcotics Act	30 Years	$10,000,000	$5,000,000	$1,075,000

FEDERAL RIGHT TO FINANCIAL PRIVACY ACT POLICY

PURPOSE

The provisions of the Federal Right to Financial Privacy Act Policy are in adherence to the *Federal Right to Financial Privacy Act* ("FRFPA"), which was enacted in 1979 in order to provide customers of financial institutions with a reasonable amount of privacy from federal government scrutiny.

SCOPE

FRFPA applies *only* to requests made by government agencies, and requires government agencies to follow specific procedures when seeking information about a customer's financial records. It also imposes duties on financial institutions prior to the release of information to government agencies. Prior to enactment of the FRFPA, customers could not challenge government access to their financial records, and had no way of knowing that personal records were being turned over to a government agency. Except in limited circumstances, such as Grand Jury investigations, customers now must be informed of the information request and given an opportunity to file an objection to release of the information through motion to quash the information request.

POLICY

The confidential relationship between Company and its customers is built on trust and must be preserved and protected. It is the policy of Company to protect the rights of our customers, and to comply with all applicable laws that relate to the release of customer information. It shall be the responsibility of all Company employees to maintain the confidentiality of all customer information. Information relating to customers, and financial information of Bank customers, is not to be discussed outside Company. Customer information may not be discussed with, or released to, outside parties without proper authorization and/or documentation.

Compliance Guidelines covering the FRFPA, including the permissible methods of requesting information, have been prepared by Company's Chief Compliance Officer and are to be incorporated into appropriate procedures at Company covering release of financial information. Financial privacy rules covering civil actions, State Tax Board, and other matters falling under Florida law will be covered under a separate document.

Responding to Requests

All information requests must be in writing. No information is to be released to any party in response to a verbal request, including in-person requests by police officers, FBI agents, or Treasury Agents. Anyone requesting information verbally must be told that Company's policy is to require that requests be provided in writing, in the form of a subpoena or other legal process, and that Company will respond to such requests in writing only.

All subpoenas and other requests for Information shall be handled by one or more designated persons.

Company shall review each request (subpoena, summons, or other formal Request for Information) to determine that the requesting party has a legal right to the information, and that the requesting party has complied with all of its duties under the FRFPA, as outlined in Company's Compliance Guidelines. Company shall determine the nature of the information being requested and shall forward a request to the appropriate department(s) to gather specified information. In cases where the request for information is very broad, Company shall communicate with the requesting party to narrow the request as much as possible. In addition, if the response time provided in the subpoena or information request cannot be met, Company will communicate with the requesting party to obtain an extension of time. All such communications must be documented.

Release of Documents

Information shall not be released until the requesting party has provided evidence of compliance with the Act's requirements, and Company shall not forward the documents until expiration of the time-period allowed for the customer to file a motion with the court to quash the subpoena or other information request. Documents being released shall be sent in a double sealed envelope. The outer envelope is to be addressed to the requesting party, and the inner envelope containing the documents is to be sealed and marked with the customer's name, account number and subpoena identification name or number. The purpose of the double envelope is to prevent release of information if notice of the customer's filing of a motion to quash is received by Company after it has mailed out the information. The requesting party is not allowed to open the inner envelope until authorized to do so by the court with whom the motion to quash has been filed.

In most cases, customers have the right to obtain copies of records supplied to government agencies or others in response to permissible information requests (subpoena, summons, etc.). However, if the request is in connection with a criminal investigation, Company may be required by law or court order to keep the existence of the information request confidential. For example, Grand Jury subpoenas are confidential and Company is prohibited from providing any information about, or acknowledging the existence of, the subpoena. To do so would subject Company to criminal penalties and fines.

Customer requests for confirmation of the existence of a subpoena or other request for information, or for copies of the documents provided under such legal process, must be in writing and shall be forwarded to the person or department designated to handle such requests. No information is to be provided to customers in response to verbal inquiries.

Record Retention

Company shall establish a file for each subpoena or information request, and the file shall contain documentation of all verbal or written communications with the requesting party, copies

of the subpoena or other information request, and copies of all documents provided to the requesting party. All files shall be retained for a period of **7 years**.

Special Information Sharing under the USA PATRIOT Act

As discussed under Company Bank Secrecy Act Policy, special regulations have been issued encouraging the sharing of information between the government and financial institutions and among financial institutions themselves to combat terrorism and money laundering. This information-sharing program is not mandatory, and may still subject Company to legal risks under Privacy Laws. The Compliance Department is to be consulted before releasing any information requested under the USA PATRIOT Act. If necessary, Compliance will consult with the Chief Legal Officer or outside legal counsel in determining whether the information being requested can be released.

EQUAL CREDIT OPPORTUNITY ACT POLICY

PURPOSE

The provisions of the Equal Credit Opportunity Act Policy are in adherence to the *Equal Credit Opportunity Act* ("ECOA") and *Regulation B* ("Reg. B"), which implements the ECOA (hereafter, collectively referred to as the "Law" through the remainder of this Policy). The purpose of the Law is to ensure that all persons have an equal chance to obtain credit and to prohibit lenders from engaging in discriminatory lending practices.

The Law covers all aspects of a credit transaction, including evaluation of credit applications, the administration and collection of accounts, advertising and credit reporting practices, and limits the information that can be asked in a credit application. Both consumer (personal) and business loans are covered.

The purpose of this policy is to promote the availability of unsecured loans to all eligible and creditworthy applicants with underwriting standards and lending procedures that are applied consistently and fairly.

POLICY

Company is an equal opportunity lender. Company's policy shall be to comply with all the requirements of the Law. All potential consumers are encouraged to apply for a loan and Company will make every attempt to review all applications to determine if they can qualify for any of loan programs. All potential Applicants for any of Company's available products will be granted or denied based on legally permissible criteria only. Company shall not engage in discriminatory practices with regard to extensions of credit, application procedures, criteria used to evaluate creditworthiness, administration of accounts, or the treatment of delinquent accounts.

Company shall not engage in practices that discriminate on the basis of age (provided the Applicant has the capacity to enter into a binding contract), sex, marital status, race, color, religion, national origin, receipt of public assistance benefits, or if the Applicant has in good faith exercised any of his or her rights under the Consumer Credit Protection Act or any other state law upon which an exemption has been granted by the federal Consumer Financial Protection Bureau. Further, Company will not engage in any practice that would discourage, on prohibited basis, anyone from making application for a loan.

Company's credit scoring system has been developed based in accordance with the Law and fair lending principles.

Any Special Purpose Credit Program, as defined in the Law, offered by Company shall be established and administered in accordance with requirements specified in the Law.

Company shall not require the signature of an Applicant's spouse on any document in violation of the Law.

Company shall not request any information prohibited under the Law. Inquiries regarding marital status will be made only when permitted, and in the format permitted under the Law. Any such information obtained will not be considered in evaluating the credit application.

Applicants will be provided with notice on the application form that income from alimony, child support, or separate maintenance payments need not be disclosed.

Company shall not consider whether an Applicant does not have a telephone listing in his or her name for credit. However, an Applicant must provide at least one telephone number in the application.

If credit history is considered in evaluating an application, it will be applied uniformly to all Applicants for the particular type and amount of credit. For each credit product offered by Company, Management shall determine whether to report Company's credit experience with customers to Consumer Reporting Agencies. If credit is reported, Company shall report in the names of the Primary Accountholder, all Joint Accountholders (if applicable). Company shall keep account records in a format that allows retrieval under either the name of the Primary Accountholder or any Joint Accountholders (if applicable).

Company shall allow customers to open loan accounts in their own names. The account may be opened in the customer's birth-given surname, a combination of birth-given surname and spouse's birth-given surname, or just the spouse's surname (if applicable).

Management shall be mindful of the Law's rules regarding disparate treatment and disparate impact in establishing its policies and procedures, and shall take steps to ensure that a policy or practice that is neutral on its face does not result in an unjustified, disproportionate, or negative effect on a protected class.

Company shall determine whether an application is approved, denied, or incomplete within 30 days of receipt of the application, and a written notice of the determination shall be provided to the Applicant. If a credit score pulled from a credit report is the basis for denial, the written notice shall disclose the credit score. Notice to the customer of the action taken will be provided. The rules regarding notice of action taken on an application cover all forms of applications, and cover initial and subsequent credit requests. Generally, notice need only be given to the primary Applicant. However, the FCRA requires that if information from a credit report is the basis, or in part, for denial of the request for credit, adverse action notices will be provided to the Primary and any Joint Applicants (if applicable) separately.

In some cases, a counteroffer, denying the original request and offering credit in a different amount or under different terms, may be appropriate. The counteroffer may be given in writing. Written counteroffers will be designed as a combination counteroffer and denial notice to avoid having to take further action if an Applicant or customer does not accept the counteroffer. The denial notice shall contain the reason or reasons the original request for credit was not granted, and shall include any applicable denial reasons under the FCRA.

Applicable adverse action notices will be provided to customers when any request for credit is denied (except as described above regarding a counter offer), including applications for a new account. The adverse action notice shall include the disclosure of credit scores pulled from a credit report, and information relating to credit scores if a credit score is used in taking adverse action.

Changes to the interest rate or fees are not adverse actions if the changes affect all or a substantial portion of Company's accounts. In such cases, Company would be required to provide a Change-in-Terms Notice to all the affected customers.

RECORD RETENTION

All written or record information in connection with a covered account or an application for a covered account will be retained for at least **25 months** or the minimum state licensing agency requirements, after the date on which a program representative informed an applicant of:

- An action taken on the application; or
- The incompleteness of an application.

Although the Law specifies minimum retention periods for applications and other documents evidencing compliance, other factors such as various statutes of limitation must be considered when determining the retention period for documents. The ECOA Guidelines reference specific retention timeframes. An electronic image of an application may be retained instead of the original paper application form.

FAIR CREDIT REPORTING ACT ("FCRA") POLICY

PURPOSE

The provisions of the Fair Credit Reporting Act Policy are in adherence to the *Fair Credit Reporting Act*, as amended and inclusive of the *Fair and Accurate Credit Transactions Act* and *Regulation V* ("Reg. V") (hereinafter collectively referred to as "FCRA" for the remainder of this Policy). The FCRA was enacted to ensure the "accuracy and fairness of credit reporting." The FCRA contains various sections with which Company must comply as a user and a furnisher of consumer information, including identity theft prevention and credit history restoration, consumer access to credit information, and enhancing the accuracy of consumer report information.

In the regular course of its business activities, Company uses information from a credit reporting agency ("CRA"), and may furnish information to a CRA about its applicants and customers, (hereinafter collectively referred to as "customer" for the remainder of this Policy).

POLICY

Company will comply with all requirements of the FCRA governing its activities as a user or furnisher of consumer information. Company will:

- Ensure that Consumer Reports are used only for *permissible purposes* as authorized by the FCRA. Company will prohibit ordering Consumer Reports for any other purpose, and limit access to the ability to order reports. Company must have a permissible purpose to request a Consumer Report on behalf of the Bank.

- Obtain written authorization for Consumer Reports from all credit and employment applicants.

- Ensure that Adverse Action Notice forms in use in all departments comply with FCRA requirements if Consumer Reports are used in making credit or employment decisions (these requirements are incorporated in Company's *Equal Credit Opportunity Act and Regulation B Policy*.)

- Provide the appropriate Adverse Action Notice to any consumer who has been denied credit or employment, or when adverse action is taken on an existing account (if applicable), based, in whole or in part, on information from a CRA. Company will also disclose a credit score and information relating to that credit score, if pulled from a CRA Consumer Report, in Adverse Action Notices when taking adverse action based on the use of a credit score.

- As applicable, report the month and year of delinquency for those accounts reported as assigned for collection, charge off or similar action, in accordance with the FCRA's timing requirements.

- As applicable, under the FCRA and the Metro 2 format for credit reporting, Company will report the account status.
- Respond to all fraud and active duty alerts, and prior to taking any credit actions communicate with the consumer before establishing a relationship. There are three types of alerts:
  - **Initial Fraud Alert**: 90 days.
  - **Extended Fraud Alert**: 7 years.
  - **Active Duty Alert**: 12 months to 2 years.
- Ensure that a written Identity Theft Prevention program is in place to comply with the Red Flag regulations and requirements for change of address for high risk transactions.
- Provide information to victims of identity theft and law enforcement, related to alleged fraud in response to victim's request.
- Respond to any notification received from or submitted to a CRA relating to information resulting from identity theft, to prevent refurnishing blocked information (i.e. Re-pollution). Also, Company will not sell, transfer or place for collections after notified of blocked information.
- Respond to all notifications from debt collectors that any information related to a debt that is attempted to be collected may be fraudulent or may be the result of identity theft.
- Provide opt-out notice of prescreened list solicitations in a format, type size and manner that is simple and easy to understand.
- Ensure that information received or shared from an Affiliate is not used to make a marketing solicitation unless the consumer has been given notice and an opportunity to opt out.
- Ensure that information derived from Consumer Reports is properly destroyed.
- Provide written notice to consumers that negative information may be reported to a CRA in the loan terms and conditions.
- Ensure that procedures are in place to respond to direct disputes from consumers or customers.
- Ensure that procedures are in place to respond to disputes from Consumer Reporting Agencies.

- Ensure that procedures are in place to enhance the accuracy and integrity of information furnished to CRAs, and reinvestigate disputes concerning the accuracy of information contained in a Consumer Report, based on a direct request by the consumer.

- If, after any reinvestigation Company finds that a disputed item by a consumer is inaccurate or incomplete or cannot be verified, Company will ensure its CRA reports are modified upon the completion of reinvestigation.

- Ensure that reasonable policies and procedures are in place regarding notices of address discrepancies received from CRAs to reduce identity theft.

- Ensure that medical information is not obtained or used in connection with any determination of a consumer's eligibility, or continued eligibility, for credit, outside of the prescribed regulatory exceptions.

- Ensure that if Risk-Based Pricing is used that either: (1) Company will provide a *Credit Score Disclosure Exception Notice,* which represents Model Form H-4; or (2) Company will provide a *Risk-Based Pricing Notice,* which represents Model form H-6 that explains that the Annual Percentage Rate ("APR") terms offered are materially less favorable than the most favorable APR terms available to a substantial portion of consumers. Company will also disclose a credit score and information relating to that credit score in Risk-Based Pricing Notice when Company uses a credit score when setting the material terms of credit.

Company is not classified as a CRA, but it is considered a user of consumer reports and may also be a furnisher of information, if it reports account payment history to a CRA. Thus, it is the policy of Company to comply with all the responsibilities under the FCRA regarding users of consumer reports and furnishers of information, as applicable.

PRIVACY OF CONSUMER FINANCIAL INFORMATION POLICY

PURPOSE

The provisions of the Privacy of Consumer Financial Information Policy are in adherence to the *Privacy of Consumer Financial Information Rule ("*Privacy Rule*")* of the *Gramm-Leach-Bliley Act* (GLBA") and *Regulation P* ("Reg. P"), which implements the Privacy Rule (hereafter, collectively referred to as the "Law" through the remainder of this Policy).

SCOPE

The GLBA seeks to protect consumer financial privacy. Its provisions limit when a "financial institution" may disclose a consumer's "nonpublic personal information" to nonaffiliated third parties. The law covers a broad range of financial institutions, including many companies not traditionally considered to be financial institutions because they engage in certain "financial activities." For the purpose of this Policy, Company is a financial institution.

Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they don't want their information shared with certain nonaffiliated third parties. In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and redisclosure of that information.

The GLBA requires the Federal Trade Commission ("FTC") and other government agencies that regulate financial institutions to implement regulations to carry out the GLBA's financial privacy provisions. The FTC is responsible for enforcing its Privacy Rule. The regulations required all covered businesses to be in full compliance by July 1, 2001.

DEFINITIONS

As it relates to the Law, the terms "consumer" and "customer" are defined as follows:

- **Consumer** – is an individual who requests, obtains or has obtained a financial product or service from Company that is used primarily for personal, family, or household purposes. For example, an individual that applies for a credit card for personal family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

- **Customer** – is a type of consumer that has a continuing relationship with Company whereby Company provides one or more financial products or services to the consumer. For example, a consumer is a customer that has an account or relationship with Company.

CUSTOMER PRIVACY POLICY STATEMENT

Trust and confidence are essential in the relationship with customers. It is the duty and responsibility of every employee of Company to protect and maintain the confidentiality and accuracy of all customer information. To protect customer privacy, the Board of Directors has approved this Policy and implemented procedures to formalize Company's commitment to safeguard customers' personal information, transactions and bank records while providing guidance to employees in carrying out their responsibilities. References in this Policy to "customer information" and "nonpublic personal information" refer to information pertaining to existing customers, former customers, and applicants.

Sharing of information with third parties, as discussed below, must be approved by the Compliance Department prior to release of such information.

PRIVACY PRINCIPLES

Information We Collect - Company collects, retains and uses nonpublic personal information about individual customers, allowed by law, to provide products and services to our customers.

We may collect nonpublic personal information such as:

- Social Security number and income.
- Credit history and credit score.
- Payment history and transaction history.

We may collect nonpublic personal information from such sources as:

- Applications and other forms.
- Information about customer's transactions with us, our affiliates or others.
- Information we receive from a consumer reporting agency.
- Information we receive directly or indirectly from customers, such as income information, telephone numbers, and e-mail addresses.

Information We Share and the Reasons We Can Share - Company may share any nonpublic personal information we collect. Any nonpublic personal information shared is conducted in strict adherence to applicable law. Listed below are the reasons we can share our customers' nonpublic personal information:

- **For our everyday business purposes** - such as to process customer transactions, maintain our customers account(s), respond to court orders and legal investigations, or report to credit bureaus.
- **For our marketing purposes** - to offer our products and services to our customers.
- **For joint marketing with other financial institutions.**

- **For our affiliates' everyday business** purposes - information about customers' transactions and experiences.
- **For our affiliates' everyday business purposes** - information about our customers' creditworthiness.
- **For our affiliates to market to our customers**.
- **For our nonaffiliates to market to our customers**.

How to Limit Our Sharing – If applicable, Company may share information regarding our experience and transactions with our customers with a parent company and other financial service providers in our corporate family, such as other financial institutions, so that they may offer or provide additional services to our customers. We also may share other information we obtain about our customers with those companies and others including service providers and companies with which we have established marketing agreements to provide products and services we feel our customers may find useful (e.g., information from applications and credit reports), unless customers call us and direct us not to share that information with them. Federal law gives customers the right to limit only the following:

- Sharing for affiliates' everyday business purposes - information about their creditworthiness.
- Affiliates from using their information to market to them.
- Sharing for nonaffiliates to market to them.

If a customer has more than one account, he/she will need to provide us with each account number to which they want the opt-out to apply. If they have a joint account, an opt-out received from one party on the account will apply to all parties on the account.

Who Receives Information and Why - If applicable, Company may share any information we collect with affiliates and nonaffiliated third parties including service providers, members of our corporate family and companies we have established marketing agreements with who provide products and services we feel our consumers and customers may find useful. Such information shared includes:

- Information provided to a data processing company that provides account maintenance, payment processing or statement printing services.
- Information provided to companies that assist us in collecting payments.
- Information provided to marketing companies that market Company's products and services on our behalf, and other companies and financial institutions with whom we have joint marketing agreements.
- Information we receive from customers on applications, and other forms, such as name and address and social security number.
- Information about customer transactions with us, our affiliates or others, such as account balance, payment history and credit card usage.
- Information we receive from a credit reporting agency, such as information relating to creditworthiness and credit history.

Service Providers and Companies with Joint Marketing Agreements – To provide our customers with products or services that they may find useful, Company may share nonpublic personal information about our customers with companies that conduct marketing services on our behalf. Such information shared may include:

- Information we receive from customers on applications or other forms, such as name, address, social security number, assets, and income.
- Information about customers' transactions with us, our affiliates or others, such as account balance, payment history, parties to transactions and credit card usage.
- Information we receive from a consumer reporting agency, such as information relating to customers' creditworthiness and credit history.

Company will require a contract or agreement with all third-party service providers and companies with which we jointly market prior to sharing any information. All contracts or agreements will contain a confidentiality clause, whereby the third-party promises to keep all information provided to it confidential, and prohibits the vendor from using the information for any purpose other than the purposes set forth in the contract or agreement.

How We Protect Customer Information - Company understands that the protection of customer nonpublic personal information is of the utmost importance. Guarding our customer's privacy is our obligation. Company maintains this Policy to safeguard customer nonpublic personal information. Employee access to customer information is restricted to those that have a business reason to know such information and we educate our employees about the importance of confidentiality and consumer privacy.

Employees are required to adhere to procedures for safeguarding customer information, including:

- When telephone calls are received, or made, employees must strictly follow verification procedures to ensure the customer is the party to whom we are speaking.
- To prevent sensitive information from being left unattended on computer screens, employees should log off the system before leaving their work areas.
- The IT Department adheres to strict information security policies including security software, network intrusion monitoring, access restrictions, security and customer privacy training as well as other safeguards to protect our customers' privacy.
- When disposing of documents containing customer information, such as account statements, the documents must be placed in the shredder bins only.
- Documents containing customer information may not be left on desktops where others can view the information.
- All documents containing customer information must be stored in cabinets when not in use, and cabinets must be locked after-hours. Access to locked cabinets and secure areas will be limited to authorized personnel only.
- The IT and HR Departments will ensure that building and system access is immediately removed for any person who leaves Company's employment.

Accuracy of Customers' Records - All customers expect and deserve that their records will be correct and accurate. The way records are established and maintained reflects on the control structure and professionalism of Company. Employees will investigate claims of inaccurate or incomplete information in a timely manner, and promptly correct any information determined to be inaccurate or incomplete.

Confidentiality of All Customer Information - The following confidentiality rules will be observed by all employees, except to the extent release of information is allowed by law, authorized by the customer, or provided in response to a valid subpoena, formal request for information, or other legal process:

- All customer bank records, documents, data and other information in any form is strictly confidential and may not be disclosed, copied or provided to any unauthorized person.
- Employees may not discuss customer accounts, transactions, or confidential information with other employees, customers or any other person who requests such information.
- Any request for confidential information about customers must be referred to a supervisor or manager.
- Company does not permit any document, data, records or other information in any form to leave Company premises without approval of a member of Executive Management.

Unauthorized Computer Access

- 18 U.S.C. Section 1030(a)(5) prohibits any person from intentionally accessing a computer used by a financial institution without authority, or in excess of authority granted, or improperly obtaining any customer information or records. The financial institution must report any violation of this law to the appropriate authorities.

- Any employee who detects a breach or misuse of any computer used by Company must report such breach or misuse to Company's Information Security Officer and the Chief Compliance Officer immediately.

Disposal of Records

Paper Reports: All paper reports that identify customer names, account balances, or any other customer information must be must be placed in the shredder bins for disposal.

Data Stored on Computers and Magnetic Media: If a computer is to be removed from service or transferred to another department or user, the internal disk drive must have the data destroyed by the IT Department before the status of the computer is changed. If data stored on portable media, such as magnetic tapes, data cartridges and removable disks is to be removed from service, the media must be physically destroyed before discarding.

Customer Requests for Name, Address or Other Record Changes - Customer requests for name, address or other record changes will be processed in accordance with applicable

policies and procedures, which require either that the request be submitted in writing or that proper verification of the caller's identity is obtained, if the request is accepted verbally.

Telephone Requests for Customer Information - Requests for customer information received via the telephone will be honored only after following applicable policies and procedures to verify that the calling party is the customer. No information will be given to a third-party unless specifically authorized in writing by the customer using a valid Power of Attorney ("POA").

Pretext Phone Calling: Pretext phone calling is a means of gaining access to a customer's confidential account information by organizations and individuals. Such organizations or individuals use surreptitious or fraudulent means to try to induce employees into providing customer account information. For example, the individual may pose as a customer who has misplaced his or her account number and may repeatedly call until the individual finds an employee who is willing to divulge confidential account information. The individual may use information about the customer, such as the customer's social security number, that has been obtained from other sources to convince the employee that the caller is legitimate.

Company employees should be cognizant of this practice and always follow the verification policies and procedures to determine that the caller is the customer. If an employee suspects there are illicit attempts to obtain confidential customer information, this fact should be reported immediately to a supervisor or manager.

Employee Training - All Department Heads are to ensure that this Policy is presented to and reviewed by each departmental employee.

Privacy Notice Delivery - The Compliance Department shall prepare an annual Privacy Notice that will be delivered to all existing customers each calendar year.

SERVICEMEMBERS CIVIL RELIEF ACT POLICY

PURPOSE

The provisions of the Servicemembers Civil Relief Act Policy are in adherence to the *Servicemembers Civil Relief Act* ("SCRA"). The SCRA establishes a maximum allowable interest rate charge during Military Service, and prohibits Company from taking certain actions against Servicemembers for the sole reason that they are a Servicemember. The SCRA does not relieve Servicemembers from their obligations; it only suspends enforcement until the ability to meet them is no longer materially affected by Military Service. Contracts entered into, and fees and charges incurred *after* the period of Military Service has begun, are not covered by the SCRA.

SCOPE OF APPLICATION

It is the policy of Company to comply with all *applicable* requirements under the SCRA. Company shall apply SCRA protection to the following Servicemembers:

- Active duty members of the:
  - **Army**
  - **Navy**
  - **Air force**
  - **Marine Corps**
  - **Coast Guard**
- Members of the **Public Health Service Commissioned Corps** in active service.
- Members of the **National Oceanic and Atmospheric Administration Commissioned Corps** in active service.
- **Reservists,** upon notice of being called to active duty.
- **Individuals ordered to report for induction** (i.e. individuals drafted into Military Service).
- **National Guard members**, when called to a period of active service by the President or the Secretary of Defense for a period of more than 30 consecutive days.

APPLICATION TO THE COMPANY PLATFORM

Company is committed to honoring the protections afforded under the SCRA. A servicemember may request relief and have the interest rate (the term "interest" includes service charges, renewal charges, fees, or any other charges (except bona fide insurance) with respect to an obligation or liability) on the loan capped at 6%, effective retroactively to the first day of active duty, for the duration of the servicemember's service.

Interest above 6% will be permanently forgiven and will not become due once the servicemember leaves active duty. Monthly payments on any effected loans will be re-amortized and reduced by the amount of interest saved during the covered period.

Company's ability to take action on a Servicemember's account in the event of default is limited under the SCRA. Company shall not take the following actions against a Servicemember based on the *sole reason* that they are a Servicemember:

- Make a determination that a Servicemember is unable to make payments on an account according to its terms.
- Deny or revoke credit.
- Change the terms of an account.
- Refuse to grant credit or terms as requested.
- Make an adverse report relating to creditworthiness.
- Refuse to insure.
- When assembling or evaluating consumer credit information, annotate a Servicemember's record identifying them as a member of the National Guard or the Reserves.
- Change the terms offered or the conditions required for the issuance of insurance.

The SCRA does not prohibit Company from reporting factual information as to payment histories or debts to Consumer Reporting Agencies (CRAs) on a Servicemember's account; such conditions may be reported to CRAs or others during the period of Military Service. Nevertheless, Company, at its discretion, may choose not to report delinquent information to CRAs or others during the period of Military Service.

NOTICE OF ACTIVE DUTY

In order for servicemembers to be entitled to SCRA interest rate protections, the SCRA provides that the servicemembers must submit a request for relief, provide a copy of their military orders calling them to military service and any orders further extending military service, **no later than 180 days** after the date of the servicemember's termination or release from military service.

Notwithstanding the technical requirements of the SCRA, Company may decide to ***not*** require a servicemember to provide his or her military orders in order to obtain relief, unless the terms of Company's servicing agreement for the noteholder require adherence to the letter of the law.

Rather, if an employee is informed that a customer may qualify for SCRA benefits, he or she may verify the applicant's status by accessing the information available at https://www.dmdc.osd.mil/appj/scra/single_record.xhtml (the "SCRA Website"). Searches require the service member's last name, Social Security Number, date of birth, and Active Duty Status Date. Website verification should be treated as the equivalent of receipt of the member's orders.

QUALIFYING LOANS

For reserve members, loans executed prior to notice of going on active duty are qualified for the **6% interest rate cap**. For all other servicemembers, only loans executed prior to active duty are qualified for the 6% interest rate cap. Loans entered into after going on active duty are not protected under the SCRA.

NOTICE OF THE END OF SCRA BENEFIT

While not required, Company may send the servicemember a written notice, at least **45 days before** SCRA benefits are scheduled to end, informing him or her of the date the SCRA benefits are scheduled to end and the interest rate to which loan will revert on that date. This letter will inform the servicemember that if he or she is eligible for continued SCRA benefits, to please contact Company. If a customer informs Company that his or her military service has been extended, Company will extend the SCRA benefits through the new date, subject to confirmation of the customer's information through a review of military orders or the SCRA Website.

CODE OF ETHICS POLICY

PURPOSE

Compliance with the *Code of Ethics* is the responsibility of every officers, directors and employees of Company. The reputation and successful business operation of Company is built upon the principles of fair dealing and ethical conduct of its officers, directors and employees. The success and continuance of Company industry and related financial institutions are heavily dependent upon the public's trust. Company is dedicated to the preservation of that trust and its reputation for integrity and excellence requires careful observance of the spirit and letter of all applicable laws and regulations, as well as scrupulous regard for the highest standard of conduct and personal integrity.

Company conducts its business in accordance with the highest ethical standards. Company will comply with all applicable laws and regulations and expects its directors, officers, and employees to conduct their personal business in accordance with the letter, spirit, and intent of all relevant laws and to refrain from any form of illegal, dishonest, or unethical conduct.

SCOPE

Directors, officers, and employees owe a duty to Company and its customers to act in all matters in a way, which will merit the continued trust and confidence of the public. In general, the use of good judgment, based on high ethical principles, will guide directors, officers, and employees with respect to lines of acceptable conduct. In the event a situation arises in which it is difficult to determine the proper course of action, the matter should be discussed openly with supervisory staff and, if necessary, higher levels of management.

POLICY

Confidential Information

Officers, directors and employees, during performance of their duties, acquire a great deal of information about Company and its customers and suppliers. This information is privileged and must be held in the strictest confidence and used solely for the purposes of Company. No information should be divulged to persons outside of Company except with respect to routine credit inquiries and disclosures required by legal process.

Confidentiality is also required with respect to certain privileged information regarding Company. Financial information regarding Company should not be released to any outside person or organization unless it has been published and reported or otherwise made available to the public through authorized news release. Any news media inquiries, particularly in emergencies, or on highly controversial or very sensitive issues, must be referred to the Chief Legal Officer or a member of Executive Management.

On a periodic basis, Company may be examined by representatives of various regulatory agencies and both internal and external auditors. The reports, which they furnish, remain, by

law, the property of the issuing agency and are strictly confidential. The information contained in the reports may not be communicated to anyone not needing the information, or to anyone not officially connected with Company.

Conflict of Interest

It is the policy of Company that all employees conduct their personal business affairs completely independent from those of Company. A conflict of interest is defined as an involvement in outside interests, which might either conflict with your duty to Company, or adversely affect your judgment in the performance of work and responsibilities. For example, any direct or indirect financial interest in a customer, supplier or competitor by you or your immediate family, which might reasonably be construed to affect decisions you make on behalf of Company, is a conflict of interest. You must avoid situations where your personal interests conflict with, or appear to conflict with, the interests of Company. It is sometimes difficult to determine whether an actual conflict of interest does exist. If you have a question, you should consult your supervisor or senior management.

Lending Practices

It is the policy of Company that its lending service is available to serve the legitimate and deserving credit needs of customers on an equitable basis.

Acceptance of Gratuities

Employees may not accept money or gifts from customers, vendors or service providers of Company, including commissions, special discounts, or other forms of compensation from agencies, attorneys, insurance and real estate agents, salesmen, or others who offer such gratuities. The only exception is small value (not to exceed $50) promotional, and holiday items from vendors/service providers, given to employees such as pens, coffee mugs, t-shirts, key chains, etc. Gifts more than $50 may only be accepted with the permission of Executive Management of Company (*exception: business meals, meetings, and conferences*).

Administration of Code of Ethics

It is the responsibility of each officer, director and employee to be familiar with Company's Code of Ethics Policy and to abide by the letter and spirit of its provisions and principles at all times. You are encouraged to discuss questions of interpretation and applicability of the code with your supervisor or management.

TRUTH-IN-LENDING ACT POLICY

PURPOSE

The provisions of the *Truth-in-Lending Act* Policy are in adherence to the *Truth-in-Lending Act* ("TILA"), Regulation Z issued by the Consumer Financial Protection Bureau ("CFPB"), which requires lenders to provide certain uniform disclosures to consumers concerning the terms of consumer loans they will issue. These disclosures include the annual percentage rate ("APR"), the finance charge, the amount financed, the number of payments and the amount of the monthly payment. The purpose of TILA is to promote informed use of credit.

As required by TILA, Company provides these disclosures before loans are closed by providing consumers with TILA disclosure during the loan application process. If a subsequent event renders a previous TILA disclosure inaccurate, we will provide an updated disclosure as required by Regulation Z.

POLICY

Finance Charge Definition

The finance charge is a measure of the cost of consumer credit represented in dollars and cents. Along with APR disclosures, the disclosure of the finance charge is central to the uniform credit cost disclosure envisioned by the TILA.

The finance charge does not include any charge of a type payable in a comparable cash transaction. Examples of charges payable in a comparable cash transaction may include taxes, title, license fees, or registration fees paid in connection with an automobile purchase.

Finance charges include any charges or fees payable directly or indirectly by the consumer and imposed directly or indirectly by Company either as an incident to or as a condition of an extension of consumer credit. The finance charge on a loan always includes any interest charges and often, other charges. Regulation Z includes examples, applicable both to open-end and closed-end credit transactions, of what must, must not, or need not be included in the disclosed finance charge

Annual Percentage Rate Definition – Closed-End Credit

Credit costs may vary depending on the interest rate, the amount of the loan and other charges, the timing and amounts of advances, and the repayment schedule. The APR, which must be disclosed in nearly all consumer credit transactions, is designed to take into account all relevant factors and to provide a uniform measure for comparing the cost of various credit transactions.

The APR is a measure of the cost of credit, expressed as a nominal yearly rate. It relates the amount and timing of value received by the consumer to the amount and timing of payments made. The disclosure of the APR is central to the uniform credit cost disclosure envisioned by the TILA.

The value of a closed-end credit APR must be disclosed as a single rate only, whether the loan has a single interest rate, a variable interest rate, a discounted variable interest rate, or graduated payments based on separate interest rates (step rates), and it must appear with the segregated disclosures. Segregated disclosures are grouped together and do not contain any information not directly related to the disclosures required under section 12 C.F.R.1026.18.

Company uses an automated process by which to calculate finance charges and APRs and populate required disclosures. Calculations are executed in accordance with Part 1026, Appendix J: Annual Percentage Rate Computations for Closed-End Credit Transactions.

Accuracy Tolerances – Closed-End Credit

Regulation Z provides finance charge tolerances for legal accuracy that should not be confused with those provided in the TILA for reimbursement under regulatory agency orders. As with disclosed APRs, if a disclosed finance charge were legally accurate, it would not be subject to reimbursement.

TILA and Regulation Z permit various finance charge accuracy tolerances for closed-end credit. Tolerances for the finance charge in a closed-end transaction, other than a mortgage loan, are generally $5 if the amount financed is less than or equal to $1,000 and $10 if the amount financed exceeds $1,000.

The APR will be considered accurate if it is within 1/8 of 1% above or below the actual APR in a regular transaction, or within 1/4 of 1 % above or below the actual APR in an irregular transaction. Irregular transactions include one or more of the following features: multiple advances, irregular payment periods, or irregular payment amounts (other than an irregular first period or irregular first or final payment).

Company aims to comply with TILA requirements related to advertising of credit, the treatment of consumer credit balances, and the servicing of loans. All advertising copy will include information that complies with TILA and Regulation Z. Advertisements for the program may state those specific credit terms that actually are or will be arranged or offered in connection with the program.

If an advertisement states:

- The amount or percentage of any down payment;
- The number of payments or period of repayment;
- The amount of any payment; or
- The amount of any finance charge:

  Then the advertisement must also include the following terms, as applicable (an example of one or more typical extensions of credit with a statement of all the terms applicable to each may be used):
  - The amount or percentage of the down payment;

- The terms of repayment, which reflect the repayment obligations over the full term of the loan; and
- The "annual percentage rate," using that term, and, if the rate may be increased after consummation, that fact.

If the "trigger" terms are displayed in electronic advertising, a table or schedule with the additional terms must be included. If "trigger" terms are used in television or radio advertisements, each additional term must be stated clearly and conspicuously.

Company will make the disclosures required by Regulation Z when using "trigger" terms in all advertisements for covered accounts.

All content used in advertising and marketing the loan program will be reviewed by Company's Compliance department.

Company will on a periodic basis a sample loan accounts to ensure loan disclosures and other communications with consumers and customers are compliant.

We will retain copies of TILA disclosures for a period of at least two years from the date on which disclosure was required to be made or other action was required to be taken.

TELEPHONE CONSUMER PROTECTION ACT POLICY

PURPOSE

The provisions of the Telephone Consumer Protection Act Policy are in adherence to the *Telephone Consumer Protection Act of 1991* (as amended) and corresponding Federal Communications Commission ("FCC") Regulations (hereafter, collectively referred to as the "TCPA" through the remainder of this Policy).

POLICY

It is the policy of Company to comply with all *applicable* requirements of the TCPA. Company shall establish Guidelines to ensure compliance with all applicable provisions of the TCPA affecting Company.

Company, and if applicable it's outbound calling vendors, when initiating outbound *non-telemarketing* calls to consumers or customers for account purposes, will obtain prior express consent when calling cellular and/or wireless telephone numbers.

Company and its outbound calling vendors (if any) will:

- Provide a copy of this Policy to all employees that make outbound calls on Company's behalf; and

- Provide adequate training to its supervisors in the administration and implementation of this Policy.

Company does not currently engage in outbound telemarketing. If Company decides to do so in the future, it will adhere to and abide by the provisions of the TCPA outlined herein:

- Company and its outbound telemarketing vendors will not call a consumer or customer who previously has requested not to receive calls from Company.

- Company and its outbound telemarketing vendors are responsible for maintaining "Do Not Call" lists of those consumers or customers who have requested not to receive calls.

- Company and its outbound telemarketing vendors are further bound by the jurisdictions of certain states whose statutes specifically identify restrictions.

- Company and its outbound telemarketing vendors will obtain prior express written consent for autodialed or prerecorded telemarketing calls to wireless numbers and for prerecorded telemarketing calls to residential lines. Further, prior express written consent cannot be conditioned on the issuance of credit.

- Company and its outside telemarketing vendors will ensure a prerecorded telemarketing message provide the consumer or customer, will have an automated way to opt out of receiving further telemarking calls.

- Company and its outside telemarketing vendors will ensure adherence to the required three percent call abandonment rate calculation for each calling campaign.

- All other requirements of the TCPA as applicable.

UNFAIR, DECEPTIVE, OR ABUSIVE ACTS OR PRACTICES POLICY

PURPOSE

The provisions of the Unfair, Deceptive or Abusive Acts or Practices Policy are in adherence to Title X of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* and Section 5 of the *Federal Trade Commission Act.*

The purpose of Title X of the *Dodd-Frank Wall Street Reform and Consumer Protection Act* ("Dodd-Frank Act") is to prevent a covered person or service provider from committing or engaging in an unfair, deceptive, or abusive acts or practices ("UDAAP") under Federal law in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service. The Consumer Financial Protection Bureau ("CFPB") is empowered with rule-making authority and, with respect to entities within its jurisdiction, enforcement authority over UDAAPs.

Section 5 of the *Federal Trade Commission Act*, 15 USC § 45(a) ("FTC Act"), broadly prohibits unfair, deceptive acts or practices ("UDAP") in or affecting commerce. Collectively, the Dodd-Frank Act and the FTC Act will be referred to as the "Act."

The federal regulators for financial institutions are empowered by the *FDIC Improvement Act* to take appropriate enforcement actions against their respective banks for violations of law or regulation.

SCOPE

This Policy provides general guidance on the principles of unfairness, deception, and abuse in the context of offering and providing consumer products and outlines the methods by which Company limits risk of UDAP and UDAAP violations by employees and third-party service providers. Because of the significant harm that could result from a violation of these statutes, strict compliance with this Policy and related statutes and regulations are a matter of utmost importance. Thus, all employees are required to comply with this Policy.

RESPONSIBILITY

Company's Chief Compliance Officer, with support from the operational management team, has the responsibility to ensure all activities and communications with consumers (which term includes customers) in connection with the Company Loan Program are handled in accordance with this Policy. Certain responsibilities may be transferred to a responsible designated representative if deemed appropriate; however, the Chief Compliance Officer retains ultimate responsibility for compliance.

POLICY

It is never the intention of Company to engage in UDAAPs in any part of its business. Policies and Guidelines are in place to review various aspects of Company's operations to ensure we are treating consumers fairly; communications will not be misleading, deceptive, or unclear; and the net effect of any communication or dealings with consumers will not have a negative impact.

Guidelines for managing the risks identified are provided below. Company will utilize these guidelines to improve customer information, communication, and service. Company will take the following definitions into account in its communications and dealing with consumers.

A. Unfair Acts or Practices

A practice may be found to be *unfair* if the following factors are present:

- **The act or practice must cause or be likely to cause substantial injury to consumers**. Substantial injury usually involves monetary harm. Monetary harm includes, for example, costs or fees paid by consumers as a result of an unfair practice. An act or practice that causes a small amount of harm to a large number of people may be deemed to cause substantial injury. Actual injury is not required in every case. A significant risk of concrete harm is also sufficient. However, trivial or merely speculative harms are typically insufficient for a finding of substantial injury. Emotional impact and other more subjective types of harm also will not ordinarily amount to substantial injury. Nevertheless, in certain circumstances, such as unreasonable debt collection harassment, emotional impacts may amount to or contribute to substantial injury.

- **The Consumers must not be reasonably able to avoid the injury.** An act or practice is not considered unfair if consumers may reasonably avoid injury. Consumers cannot reasonably avoid injury if the act or practice interferes with their ability to effectively make decisions or to take action to avoid injury. Normally the marketplace is selfcorrecting; it is governed by consumer choice and the ability of individual consumers to make their own private decisions without regulatory intervention. If material information about a product, such as pricing, is modified after, or withheld until after, the consumer has committed to purchasing the product; however, the consumer cannot reasonably avoid the injury. Moreover, consumers cannot avoid injury if they are coerced into purchasing unwanted products or services or if a transaction occurs without their knowledge or consent.

  A key question is not whether a consumer could have made a better choice. Rather, the question is whether an act or practice hinders a consumer's decision-making. For example, not having access to important information could prevent consumers from comparing available alternatives, choosing those that are most desirable to them, and avoiding those that are inadequate or unsatisfactory. In addition, if almost all market participants engage in a practice, a consumer's incentive to search elsewhere for better terms is reduced, and the practice may not be reasonably avoidable.

The actions that a consumer is expected to take to avoid injury must be reasonable. While a consumer might avoid harm by hiring independent experts to test products in advance or by bringing legal claims for damages in every case of harm, these actions generally would be too expensive to be practical for individual consumers and, therefore, are not reasonable.

- **The injury must not be outweighed by countervailing benefits to consumers or competition.** To be unfair, the act or practice must be injurious in its net effects — that is, the injury must not be outweighed by any offsetting consumer or competitive benefits that also are produced by the act or practice. Offsetting consumer or competitive benefits of an act or practice may include lower prices to the consumer or a wider availability of products and services resulting from competition.

  Costs that would be incurred for measures to prevent the injury also are taken into account in determining whether an act or practice is unfair. These costs may include the costs to the institution in taking preventive measures and the costs to society as a whole of any increased burden and similar matters.

  Public policy, as established by statute, regulation, judicial decision, or agency determination, may be considered with all other evidence to determine whether an act or practice is unfair.

B. Deceptive Acts or Practices

Practices or acts may be determined to be *deceptive* if the following factors are present:

- **There must be a representation, omission, act, or practice that misleads or is likely to mislead the consumer.** Deception is not limited to situations in which a consumer has already been misled. Instead, an act or practice may be deceptive if it is likely to mislead consumers.

  It is necessary to evaluate an individual statement, representation, or omission not in isolation, but rather in the context of the entire advertisement, transaction, or course of dealing, to determine whether the overall net impression is misleading or deceptive. A representation may be an express or implied claim or promise, and it may be written or oral. If material information is necessary to prevent a consumer from being misled, it may be deceptive to omit that information.

  Written disclosures may be insufficient to correct a misleading statement or representation, particularly where the consumer is directed away from qualifying limitations in the text or is counseled that reading the disclosures is unnecessary. Likewise, oral or fine print disclosures or contract disclosures may be insufficient to cure a misleading headline or a prominent written representation. Similarly, a deceptive act or practice may not be cured by subsequent accurate disclosures.

Acts or practices that may be deceptive include: making misleading cost or price claims; offering to provide a product or service that is not in fact available; using bait-and-switch techniques; omitting material limitations or conditions from an offer; or failing to provide the promised services.

The Federal Trade Commission's "four Ps" test can assist in the evaluation of whether a potentially misleading representative, omission, act, or practice is likely to mislead:

1. Is the statement **prominent** enough for the consumer or customer to notice?

2. Is the information **presented** in an easy-to-understand form that does not contradict other information in the materials and at a time when the consumer's or customer's attention is not distracted elsewhere?

3. Is the **placement** of the information in a location where consumers and customers can be expected to look or hear?

4. Is the information in close **proximity** to the claim it qualifies?

- **The representation, omission, act, or practice must be considered from the perspective of the reasonable consumer.** In determining whether an act or practice is misleading, one also must consider whether the consumer's interpretation of or reaction to the representation, omission, act, or practice is reasonable under the circumstances. In other words, whether an act or practice is deceptive depends on how a reasonable member of the target audience would interpret the representation. When representations or marketing practices target a specific audience, such as older Americans, young people, or financially distressed consumers, the communication must be reviewed from the point of view of a reasonable member of that group.

  Moreover, a representation may be deceptive if the majority of consumers in the target class do not share the consumer's interpretation, so long as a significant minority of such consumers is misled. When a seller's representation conveys more than one meaning to reasonable consumers, one of which is false, the seller is liable for the misleading interpretation.

  Exaggerated claims or "puffery," however, are not deceptive if the claims would not be taken seriously by a reasonable consumer.

- **The representation, omission, or practice must be material.** A representation, omission, act, or practice is material if it is likely to affect a consumer's choice of, or conduct regarding, the product or service. Information that is important to consumers is material.

  Certain categories of information are presumed to be material. In general, information about the central characteristics of a product or service – such as costs, benefits, or restrictions on the use or availability – is presumed to be material. Express claims made with respect to a

financial product or service, are presumed material. Implied claims are presumed to be material when evidence shows that the institution intended to make the claim (even though intent to deceive is not necessary for deception to exist).

Claims made with knowledge that they are false are presumed to be material. Omissions will be presumed to be material when the financial institution knew or should have known that the consumer needed the omitted information to evaluate the product or service.

If a representation or claim is not presumed to be material, it still would be considered material if there is evidence that it is likely to be considered important by consumers**.**

C. Abusive Acts or Practices

An act or practice may be found to be *abusive* if the following factors are present:

- Materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service.

- Takes unreasonable advantage of:

  - A lack of understanding on the part of the consumer or customer of the material risk, costs, or conditions of the product or service;

  - The inability of the consumer to protect its interest in selecting or using a consumer financial product or service; or

  - The reasonable reliance by the consumer on a covered person to act in the interest of the consumer.

Although abusive acts also may be unfair or deceptive, examiners should be aware that the legal standards for abusive, unfair, and deceptive each are separate.

The Role of Consumer Complaints in Identifying Unfair, Deceptive, or Abusive Acts or Practices

Consumer complaints play a key role in the detection of unfair, deceptive, or abusive practices. Consumer complaints are an essential source of information for examinations, enforcement, and rule-making for regulators. As a general matter, consumer complaints can indicate weaknesses in elements of Company's Compliance Management System, such as training, internal controls, or monitoring.

While the absence of complaints does not ensure that unfair, deceptive, or abusive practices are not occurring, complaints may be one indication of UDAAPs. For example, the presence of complaints alleging that consumers did not understand the terms of a product or service may be a red flag indicating a potential issue for review. This is especially true when numerous consumers

make similar complaints about the same product or service. Because the perspective of a reasonable consumer is one of the tests for evaluating whether a representation, omission, act, or practice is potentially deceptive, consumer complaints alleging misrepresentations or misunderstanding may provide a window into the perspective of the reasonable consumer.

Consumers can file complaints with several different entities, such as: Company itself, credit reporting agencies, the Better Business Bureau ("BBB"), State Attorneys General, the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), the Federal Communications Commission ("FCC"), the Department of Justice ("DOJ"), other Federal and State agencies.

Analyzing Complaints

Company will review and analyze consumer complaints to assist in the identification of potential unfair, deceptive, or abusive practices. Company will consider the context and reliability of complaints; because every complaint does not indicate violation of law. When consumers repeatedly complain about a Company's product or service, Company will flag the issue for possible further review.

Company will also consider complaints lodged against any of its affiliates, vendors, and third parties regarding the products and services offered through Company or using Company's name. Company will monitor and respond to complaints filed against such parties.

Relationship to Other Laws

Company understands that an unfair, deceptive, or abusive act or practice may also violate other federal or state laws. For example, pursuant to the TILA, creditors must "clearly and conspicuously" disclose the costs and terms of credit. An act or practice that does not comply with these provisions of TILA may also be unfair, deceptive, or abusive.

Conversely, Company understands that a transaction that is in technical compliance with other federal or state laws may nevertheless violate the prohibition against UDAAPs. For example, an advertisement may comply with TILA's requirements, but contain additional statements that are untrue or misleading, and compliance with TILA's disclosure requirements does not insulate the rest of the advertisement from the possibility of being deceptive.

CAN-SPAM ACT POLICY

PURPOSE

The provisions of the CAN-SPAM Act Policy are in adherence to the federal law, *Controlling the Assault of the Non-Solicited Pornography and Marketing Act of 2003*, more commonly known as "The CAN-SPAM Act of 2003" (the "Act"). Act allows consumers to opt-out of receiving commercial emails, and gives Federal civil and criminal enforcement authorities new ways to combat commercial email that is unwanted by the recipient and/or deceptive.

The Federal Trade Commission ("FTC") published regulations implementing the Act on January 19, 2005, which included adding criterion for determining the primary purpose of an email message. The Act regulates both commercial messages and transactional or relationship messages.

The Act has created a national standard in the United States for the regulation of marketing by email by preempting 38 state laws. However, the Act permits states to continue to regulate fraudulent and deceptive email practices.

The goals of the Act are:

- To reduce spam and unsolicited pornography by prohibiting senders of unsolicited commercial email messages from disguising the source and content of their messages; and

- To give consumers the choice to cease receiving a sender's unsolicited commercial email messages

SCOPE

The Act does not prohibit the sending of legitimate email solicitations. Rather, all commercial email messages, whether to existing customers or not, must include a means for the recipient to opt-out of further commercial email messages.

The Act allows the use of a list of choices whereby the recipient may choose to receive or not receive certain commercial emails from the sender, if the list includes the option not to receive any further commercial emails.

POLICY

It is the policy of Company to comply with all requirements under the Act. Company may send email solicitations to customers and non-customers. Company may provide email notifications about customer accounts to those customers who have elected to receive such notifications (i.e., reminders that a bill is due, notice that a payment has posted, etc.). All emails covered by CAN-SPAM will contain a link to click on to opt-out of future notifications.

To ensure compliance with the Act and implementing regulations, management is responsible for ensuring that new or expanded email programs are reviewed and approved by the Compliance Department before implementation.

ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT POLICY

PURPOSE

The provisions of the Electronic Signatures in Global and National Commerce Act Policy are in adherence to the *Electronic Signatures in Global and National Commerce Act* ("E-SIGN Act"). The E-SIGN Act allows the use of electronic communications to satisfy any statute, regulation or rule of law requiring that such information be provided in writing, if the consumer has affirmatively consented to such use and has not withdrawn such consent. The E-SIGN Act provides a general rule of validity for electronic communications and signatures for transactions.

The E-SIGN Act provides that electronic signatures and records cannot be denied legal effect solely because they are electronic as compared to being on paper. The E-SIGN Act states two general rules:

- Signatures, contracts, or other records may not be denied legal effect, validity, or enforceability solely because they are in electronic form; and

- A contract may not be denied effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

The E-SIGN Act contains specific requirements with regard to obtaining a consumer's consent to receiving disclosures electronically. If a statute, regulation or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing provided the E-SIGN Act's consumer consent requirements are met.

POLICY

It is Company's policy to comply with the requirements of the E-SIGN Act.

With the customer's affirmative consent, Company may provide access to certain disclosures, notices, and communications (hereinafter collectively referred to as "Communications"), in an electronic format, such as HTML webpages and PDF files.

Company will provide customers with a clear and conspicuous disclosure before it obtains their consent to provide electronic Communications. The disclosure will include the following:

- Scope of Communications included with consent.

- The hardware and software requirements to access and retain electronic Communications, and a statement that Company will provide at least 45 days' electronic notice before a change is made to the hardware or software requirements.

- Requirement that the customer demonstrate their ability to view Company's electronic Communications, as applicable.

- How to request paper copies of Communications after consent is given and any associated fees.

- Procedures to withdraw consent.

Company shall retain electronic copies of the E-SIGN agreement and electronic Communications in a form that is capable of being reproduced in according to the applicable statutes. The retention process shall enable Company to easily retrieve the electronic content upon request.

SOCIAL MEDIA POLICY

PURPOSE

The provisions of the Social Media Policy are in adherence to the *Social Media: Consumer Compliance Risk Management Guidance* ("Guidance") published by the Federal Financial Institutions Examination Council ("FFIEC"). This Guidance will assist Company in addressing the applicability of federal consumer protection and compliance laws, regulations and policies regarding activities conducted on Social Media sites (e.g., Facebook, YouTube, Flickr, LinkedIn, etc.). While the Guidance does not impose any new requirements on Company, it helps Company understand and manage potential consumer and customer compliance and legal risks, including reputation and operational risks, associated with the use of social media.

For the purposes of this Policy, "Social Media" is defined as a form of interactive online communication in which users can generate and share content through messages, text, images, audio, and or video. Messages sent via email or text message, standing alone, do not constitute social media. Such emails and text messages may, however, be subject to other laws and regulations not discussed in the Guidance or this Policy.

Some uses of social media includes marketing, providing incentives to consumers and customers, facilitating applications for new accounts, inviting feedback from the public, and engaging with existing and potential customers by responding to complaints or providing pricing.

POLICY

For activities conducted on social media sites, Company implements the following as applicable:

- Company will have a risk management program to identify, measure, monitor, and control the risks related to its social media usage. The size and complexity of that program will commensurate with the breadth of Company's involvement in social media. The program will be designed with participation from Compliance, IT, Information Security, Legal, Human Resources, and Marketing departments.

- If Company uses social media to engage in lending, account creation, payment activities, etc., it will comply with the applicable laws and regulations as when it engages in those activities through other media (e.g. Equal Credit Opportunity Act and Regulation B, Truth in Lending Act and Regulation Z, Electronic Fund Transfer Act and Regulation E, etc.).

- If Company uses or conduct activities in Social Media, it will comply with all applicable Laws, and Regulations regarding the privacy of Consumer information (e.g. Gramm-Leach-Bliley Act, Telephone Consumer Protection Act, Children's Online Privacy Protection Act, etc.).
- If Company uses or conducts activities in Social Media it will be sensitive to, and properly manage, the reputational risks that arise from those activities (e.g. Fraud in the Company's name, Brand identity protection, etc.).

- If Company allows employees to officially communicate on behalf of the Company through Social Media, it will provide those employees with training and direction concerning those activities.

EMPLOYEE GUIDELINES

This Policy also provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

The following principles apply to professional use of social media on behalf of Company as well as personal use of social media when referencing Company

- Employees need to know and adhere to the Company's Code of Conduct, Employee Handbook, and other policies when using social media in reference to Company

- Employees should be aware of the effect their actions may have on their images, as well as Company's image. The information that employees post or publish may be public information for a long time.

- Employees should be aware Company may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Company, its employees, or customers.

- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment.

- Employees are not to publish, post, or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department and/or supervisor.

- Social media networks, blogs, and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to authorized Company spokespersons.

- If employees find encounter a situation while using social media that threatens to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of a supervisor.

- Employees should get appropriate permission before you refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get

appropriate permission to use a third-party's copyrights, copyrighted material, trademarks, service marks, or other intellectual property.

- Social media use should not interfere with employee's responsibilities at Company. Company's computer systems are to be used for business purposes only. When using the Company's computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, Company blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.

- Subject to applicable law, after-hours online activity that violates Company's Code of Conduct or any other policy may subject an employee to disciplinary action or termination.

- If employees publish content after-hours that involves work or subjects associated with Company, a disclaimer should be used, such as this: "The postings on this site are my own and may not represent Company's positions, strategies, or opinions."

- It is highly recommended that employees keep Company-related social media accounts separate from personal accounts, if practical.

VENDOR MANAGEMENT POLICY

PURPOSE

The provisions of the Vendor Management Policy are in scope with adherence to the *Gramm Leach Bliley Act* ("GLBA") regulation section (b) protecting personal information, and financial industry regulatory guidance.

Given the specialized expertise or proprietary processes within the lending industry needed to design, implement, and service new technologies and products, vendors may provide a valuable means to acquire expertise and resources that Company cannot, or chooses not to, provide on its own. In planning whether and how to contract for these needs, Company will assess how it will manage the risks associated with these new relationships.

Company will establish written procedures that contain adequate controls to limit the risks associated with the use of vendors to perform operational functions. Vendors may be used to support new Company technologies, systems, and products. While Company can outsource many functions, management remains responsible for the performance and actions of its vendors while the vendors are performing work for Company.

Managers are required to handle requests to do business with vendors, through a vendor management review process. The process assigns a risk level based on the amount of risk presented to Company by employing the vendor's services.

It is management's responsibility to review and approve all vendor activities and performance and to know their competencies. If a vendor cannot meet contractual commitments, Company must be able to exercise a contingency plan and secure those services elsewhere. The risks associated with non-compliance, credit risk, operational risk, reputation risk, compliance risk, and strategic risk – will be borne by Company, not the vendor.

RISK MANAGEMENT LIFE CYCLE

Company will have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and the Company's organizational structures. Company will also ensure comprehensive risk management and oversight of third-party relationships involving ***critical activities*** — significant functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology), or other activities that:

- could cause Company to face significant risk if the third- Company party fails to meet expectations.
- could have significant customer impacts.
- require significant investment in resources to implement the third-party relationship and manage the risk.

- could have a major impact on Company's operations if it must find an alternate third-party or if the outsourced activity must be brought in-house.

Company will follow an effective third-party risk management process, which follows a continuous life cycle for all relationships and incorporates the following phases:

- **Planning:** Developing a plan to manage the relationship is often the first step in the third-party risk management process. This step is helpful for many situations but is necessary when Company is considering contracts with third parties that involve critical activities.

- **Due diligence and third-party selection:** Conducting a review of a potential third-party before signing a contract helps ensure that the bank selects an appropriate third-party and understands and controls the risks posed by the relationship, consistent with the bank's risk appetite.

- **Contract negotiation:** Developing a contract that clearly defines expectations and responsibilities of the third-party helps to ensure the contract's enforceability, limit the bank's liability, and mitigate disputes about performance.

- **Ongoing monitoring:** Performing ongoing monitoring of the third-party relationship once the contract is in place is essential to Company's ability to manage risk of the third-party relationship.

- **Termination:** Developing a contingency plan to ensure that Company can transition the activities to another third-party, bring the activities in-house, or discontinue the activities when a contract expires, the terms of the contract have been satisfied, in response to contract default, or in response to changes to Company's or third-party's business strategy.

In addition, Company should perform the following <u>throughout</u> the life cycle of the relationship as part of its risk management process:

- **Oversight and accountability:** Assigning clear roles and responsibilities for managing third-party relationships and integrating Company's third-party risk management process with its enterprise risk management framework enables continuous oversight and accountability.

- **Documentation and reporting:** Proper documentation and reporting facilitates oversight, accountability, monitoring, and risk management associated with third-party relationships.

- **Independent reviews:** Conducting periodic independent reviews of the risk management process enables management to assess whether the process aligns with Company's strategy and effectively manages risk posed by third-party relationships.

MANAGEMENT WHITE PAPER PLANNING

Outsourcing can be used to accomplish a great number of services needed by Company. The types of services can vary in complexity and risk to the institution. Management shall maintain processes to determine the level of risk a particular service may have on Company and prescribe a required amount of analysis prior to engagement. Whether it's outsourcing high risk or critical processes, upgrading existing systems or creating a new system internally, management will undertake a pragmatic planning process that will assess risk and performance gains within the context of Company's overall strategic goals and existing competencies. An assessment document should be included in the vendor management approval file. This document should be maintained within the executive contract file and may include:

- A cost/benefit analysis;
- An overview of the vendors operation including a critique of the proposed process;
- A written overview outlining the vendors operations to identify and determine the specific risk exposure to Company as well as the adequacy of the vendors internal controls to ensure limitation of that risk;
- The ability to initiate a COB ("Continuity of Business") plan to resume operations swiftly and with data intact in the event of vendor system failure or inability to process;
- Service Level Agreements designed to monitor vendor performance;
- A review and evaluation of vendor information systems and MIS necessary to monitor adherence to the established objectives and properly supervise the relationship;
- A review and evaluation of their security controls in place necessary to protect the sensitive information of Company and adhere to GLBA regulations; and
- A comparative analysis of similar vendors and or products to ensure competitive product and pricing.

Contracts and/or agreements should ensure the expectations and obligations of each party are clearly defined, understood and otherwise enforceable.

It is the policy of Company to comply with all regulations for any transactions and dealings with outside vendors. Company's management shall ensure vendors serve Company's best interests and perform the services in a safe and sound manner.

CONTRACTS AND AGREEMENTS

Contracts will be reviewed by management and the Chief legal and Compliance Officer, as appropriate, to ensure the following subject matter is incorporated in the written agreement:

- Scope
- Responsibilities of both parties, and description of product or services to be provided including subcontractors, if applicable
- Performance Measurements or Benchmarks that can be used to ensure performance of the product or service
- Compliance with applicable laws and regulations
- Compliance with regulation and policy standards governing vendor relationships
- Default and Termination
- Cost and Compensation
- Ownership and Licensing
- Confidentiality
- Notification of Network Compromise
- Consumer Complaint Handling
- Contingency Plans
- Indemnification
- Insurance certifications
- Training and Dispute Resolution
- Limits of Liability
- Right to Audit

POLICY STANDARDS

Oversight - All vendor relationships must be documented and approved by the appropriate Executive Officer. Management shall ensure Company does not relinquish strategic control of any functions or activities outsourced to a vendor, and that vendor management approval and ongoing review procedures are followed.

Fees - The vendor's fees should be fair, equitable and representative of, and have a direct relationship to, the service provided.

Information Sharing - Executive Management shall ensure sharing of customer information with vendors is restricted to sharing permitted by law, written agreement to maintain the confidentiality and adequate security procedures are maintained. Executive Management approval is required prior to the commencement of an information sharing relationship.

MAINTENANCE DUE DILIGENCE

Vendor Selection - Management shall ensure proper due diligence is performed in selecting a vendor, including, but not limited to, consideration of business reputation, financial condition,

and qualifications. Written procedures shall address the steps to be taken to determine the amount of due diligence needed based on the level and complexity of services performed.

Critical Vendors - A list of vendors critical to Company will be maintained and updated as defined in the Vendor Management procedures.

REVIEWS

Annual Vendor Reviews - Management shall ensure each vendor considered to be critical to Company's operation and/or processes and stores any Company account number or social security number will have an annual review performed to validate compliance and be subjected to an annual due diligence review, including financials, audits and security assessment and other areas as deemed necessary based on the level of risk associated with that vendor, as well as an optional on-site (at management's discretion) review of the vendors operations.

Executive Summary Report - An Executive Summary report will be prepared on the annual vendor management review of critical service providers and presented to the Executive Committee and Board of Directors for review. Quarterly updates will be provided if there are status updates from vendor management.

FAIR DEBT COLLECTION PRACTICES ACT POLICY

POLICY STATEMENT

The provisions of the Fair Debt Collection Practices Act Policy are in scope with adherence to the *applicable* provisions of the *Fair Debt Collection Practices Act* ("FDCPA") found at 15 U.S.C. 1692. The provisions of the FDCPA Policy are in adherence to the FDCPA.

The FDCPA only applies to a "debt collector." A debt collector is any organization that regularly collects debts for a third-party or in a name other than its own. Company is not considered a debt collector under the statute because it is considered a creditor collecting in its own name. Further, Company's principal business purpose is not the collection of debts.

Nevertheless, as a best practice, Company employees will comply with the *applicable* provisions of the FDCPA whenever they collect consumer debts owed to Company.

DEFINITIONS

As used in this Policy:

- The term "**Commission**" means the Federal Trade Commission ("FTC").

- The term "**communication**" means the conveying of information regarding a debt directly or indirectly to any person through any medium.

- The term "**consumer**" means any natural person obligated or allegedly obligated to pay any debt.

- The term "**creditor**" means any person who offers or extends credit creating a debt or to whom a debt is owed, but such term does not include any person to the extent that he receives an assignment or transfer of a debt in default solely for the purpose of facilitating collection of such debt for another. In this Policy, Company is considered the "creditor."

- The term "**debt**" means any obligation or alleged obligation of a consumer to pay money arising out of a transaction in which the money, property, insurance, or services which are the subject of the transaction are primarily for personal, family, or household purposes, whether or not such obligation has been reduced to judgment.

- The term "**debt collector**" means any person who uses any instrumentality of interstate commerce or the mails in any business the principal purpose of which is the collection of any debts, or who regularly collects or attempts to collect, directly **or** indirectly, debts owed or due or asserted to be owed or due another.

  Notwithstanding the exclusion provided in this definition below, the term includes any creditor who, in the process of collecting his own debts, uses any name other than his own

which would indicate that a third person is collecting or attempting to collect such debts. For the purpose of the "Unfair Practices" section hereafter, such term also includes any person who uses any instrumentality of interstate commerce or the mails in any business the principal purpose of which is the enforcement of security interests.

The term does not include:

- any officer or employee of a creditor (i.e. Company) while, in the name of the creditor, collecting debts for such creditor;
- any person while acting as a debt collector for another person, both of whom are related by common ownership or affiliated by corporate control, if the person acting as a debt collector does so only for persons to whom it is so related or affiliated and if the principal business of such person is not the collection of debts;
- any officer or employee of the United States or any State to the extent that collecting or attempting to collect any debt is in the performance of his official duties;
- any person while serving or attempting to serve legal process on any other person in connection with the judicial enforcement of any debt;
- any nonprofit organization which, at the request of consumers, performs bona fide consumer credit counseling and assists consumers in the liquidation of their debts by receiving payments from such consumers and distributing such amounts to creditors; and
- any person collecting or attempting to collect any debt owed or due or asserted to be owed or due another to the extent such activity:
  - is incidental to a bona fide fiduciary obligation or a bona fide escrow arrangement;
  - concerns a debt which was originated by such person;
  - concerns a debt which was not in default at the time it was obtained by such person; or
  - concerns a debt obtained by such person as a secured party in a commercial credit transaction involving the creditor.

- The term "**location information**" means a consumer's place of abode and his telephone number at such place, or his place of employment.
- The term "**State**" means any State, territory, or possession of the United States, the District of Columbia, the Commonwealth of Puerto Rico, or any political subdivision of any of the foregoing.

ACQUISITION OF LOCATION INFORMATION

Company or the debt collector communicating with any person other than the consumer for the purpose of acquiring location information about the consumer shall:

- identify himself, state that he is confirming or correcting location information concerning the consumer, and, only if expressly requested, identify his employer;
- not state that such consumer owes any debt;
- not communicate with any such person more than once unless requested to do so by such person or unless Company or the debt collector reasonably believes that the earlier response of such person is erroneous or incomplete and that such person now has correct or complete location information;
- not communicate by post card;
- not use any language or symbol on any envelope or in the contents of any communication effected by the mails or telegram that indicates that Company or the debt collector is in the debt collection business or that the communication relates to the collection of a debt; and
- after the Company or the debt collector knows the consumer is represented by an attorney with regard to the subject debt and has knowledge of, or can readily ascertain, such attorney's name and address, not communicate with any person other than that attorney, unless the attorney fails to respond within a reasonable period of time to communication from Company or the debt collector.

COMMUNICATION IN CONNECTION WITH DEBT COLLECTION

(a) Communication with the Consumer Generally - Without the prior consent of the consumer given directly to Company or the debt collector or the express permission of a court of competent jurisdiction, Company or the debt collector may not communicate with a consumer in connection with the collection of any debt:

- at any unusual time or place or a time or place known or which should be known to be inconvenient to the consumer. In the absence of knowledge of circumstances to the contrary, Company or the debt collector shall assume that the convenient time for communicating with a consumer is after 8 o'clock antemeridian and before 9 o'clock postmeridian, local time at the consumer's location;
- if Company or the debt collector knows the consumer is represented by an attorney with respect to such debt and has knowledge of, or can readily ascertain, such attorney's name and address, unless the attorney fails to respond within a reasonable period of time to a communication from Company or the debt collector, or unless the attorney consents to direct communication with the consumer; or

- at the consumer's place of employment if Company or the debt collector knows or has reason to know that the consumer's employer prohibits the consumer from receiving such communication.

(b) Communication with Third Parties - Except as provided in section 1692b of this title, without the prior consent of the consumer given directly to Company or the debt collector, or the express permission of a court of competent jurisdiction, or as reasonably necessary to effectuate a post-judgment judicial remedy, Company or the debt collector may not communicate, in connection with the collection of any debt, with any person other than the consumer, his attorney, a consumer reporting agency if otherwise permitted by law, the creditor, the attorney of the creditor, or the attorney of the debt collector.

(c) Ceasing Communication - If a consumer notifies Company or the debt collector in writing that the consumer refuses to pay a debt or that the consumer wishes Company or the debt collector to cease further communication with the consumer, Company or the debt collector shall not communicate further with the consumer with respect to such debt, except:

- to advise the consumer that Company or the debt collector's further efforts are being terminated;

- to notify the consumer that Company or the debt collector may invoke specified remedies which are ordinarily invoked by Company or the debt collector; or

- where applicable, to notify the consumer that Company or the debt collector intends to invoke a specified remedy.

If such notice from the consumer is made by mail, notification shall be complete upon receipt.

(d) "Consumer" Defined - For the purpose of this section, the term "consumer" includes the consumer's spouse, parent (if the consumer is a minor), guardian, executor, or administrator.

HARASSMENT OR ABUSE

Company or the debt collector may not engage in any conduct the natural consequence of which is to harass, oppress, or abuse any person in connection with the collection of a debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:

- The use or threat of use of violence or other criminal means to harm the physical person, reputation, or property of any person.

- The use of obscene or profane language or language the natural consequence of which is to abuse the hearer or reader.

- The publication of a list of consumers who allegedly refuse to pay debts, except to a consumer reporting agency or to persons meeting the requirements of section 1681a (f) or 1681b (3) [1] of this title.

- The advertisement for sale of any debt to coerce payment of the debt.

- Causing a telephone to ring or engaging any person in telephone conversation repeatedly or continuously with intent to annoy, abuse, or harass any person at the called number.

- Except as provided in the Acquisition of Location Information section above, the placement of telephone calls without meaningful disclosure of the caller's identity

FALSE OR MISLEADING REPRESENTATIONS

Company or the debt collector may not use any false, deceptive, or misleading representation or means in connection with the collection of any debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:

- The false representation or implication that Company or the debt collector is vouched for, bonded by, or affiliated with the United States or any State, including the use of any badge, uniform, or facsimile thereof.

- The false representation of:

    - the character, amount, or legal status of any debt; or

    - any services rendered or compensation which may be lawfully received by any debt collector for the collection of a debt.

- The false representation or implication that any individual is an attorney or that any communication is from an attorney.

- The representation or implication that nonpayment of any debt will result in the arrest or imprisonment of any person or the seizure, garnishment, attachment, or sale of any property or wages of any person unless such action is lawful and Company or the debt collector intends to take such action.

- The threat to take any action that cannot legally be taken or that is not intended to be taken.

- The false representation or implication that a sale, referral, or other transfer of any interest in a debt shall cause the consumer to:

    - lose any claim or defense to payment of the debt; or

    - become subject to any practice prohibited by this subchapter.

- The false representation or implication that the consumer committed any crime or other conduct in order to disgrace the consumer.

- Communicating or threatening to communicate to any person credit information which is known or which should be known to be false, including the failure to communicate that a disputed debt is disputed.

- The use or distribution of any written communication which simulates or is falsely represented to be a document authorized, issued, or approved by any court, official, or agency of the United States or any State, or which creates a false impression as to its source, authorization, or approval.

- The use of any false representation or deceptive means to collect or attempt to collect any debt or to obtain information concerning a consumer.

- The failure to disclose in the initial written communication with the consumer and, in addition, if the initial communication with the consumer is oral, in that initial oral communication, that the debt collector is attempting to collect a debt and that any information obtained will be used for that purpose, and the failure to disclose in subsequent communications that the communication is from a debt collector, except that this paragraph shall not apply to a formal pleading made in connection with a legal action.

- The false representation or implication that accounts have been turned over to innocent purchasers for value.

- The false representation or implication that documents are legal process.

- The use of any business, company, or organization name other than the true name of the debt collector's business, company, or organization.

- The false representation or implication that documents are not legal process forms or do not require action by the consumer.

- The false representation or implication that Company or the debt collector operates or is employed by a consumer reporting agency as defined by section 1681a (f) of this title.

UNFAIR PRACTICES

Company or the debt collector may not use unfair or unconscionable means to collect or attempt to collect any debt. Without limiting the general application of the foregoing, the following conduct is a violation of this section:

- The collection of any amount (including any interest, fee, charge, or expense incidental to the principal obligation) unless such amount is expressly authorized by the agreement creating the debt or permitted by law.

- The acceptance by Company or the debt collector from any person of a check or other payment instrument postdated by more than five days unless such person is notified in writing of Company or the debt collector's intent to deposit such check or instrument not more than ten nor less than three business days prior to such deposit.

- The solicitation by Company or the debt collector of any postdated check or other postdated payment instrument for the purpose of threatening or instituting criminal prosecution.

- Depositing or threatening to deposit any postdated check or other postdated payment instrument prior to the date on such check or instrument.

- Causing charges to be made to any person for communications by concealment of the true purpose of the communication. Such charges include, but are not limited to, collect telephone calls and telegram fees.

- Taking or threatening to take any nonjudicial action to effect dispossession or disablement of property if:

    - there is no present right to possession of the property claimed as collateral through an enforceable security interest;

    - there is no present intention to take possession of the property; or

    - the property is exempt by law from such dispossession or disablement.

- Communicating with a consumer regarding a debt by post card.

- Using any language or symbol, other than Company or the debt collector's address, on any envelope when communicating with a consumer by use of the mails or by telegram, except that Company or the debt collector may use the business name if such name does not indicate that it is in the debt collection business.

NOTICE OF DEBT

Within five days after the initial communication with a consumer in connection with the collection of any debt, a debt collector shall, unless the following information is contained in the initial communication or the consumer has paid the debt, send the consumer a written notice containing:

- the amount of the debt;
- the name of the Company (to whom the debt is owed);
- a statement that unless the consumer, within thirty days after receipt of the notice, disputes the validity of the debt, or any portion thereof, the debt will be assumed to be valid by the debt collector;
- a statement that if the consumer notifies the debt collector in writing within the thirty-day period that the debt, or any portion thereof, is disputed, the debt collector will obtain verification of the debt or a copy of a judgment against the consumer and a copy of such verification or judgment will be mailed to the consumer by the debt collector; and
- a statement that, upon the consumer's written request within the thirty-day period, the debt collector will provide the consumer with the name and address of the original creditor, if different from the current creditor.

These above notices are not applicable to Company when collecting the debt in its own name because it is the original creditor. However, the notices are applicable to its debt collection vendor(s).

DISPUTED DEBTS

If the consumer notifies Company or the debt collector in writing within the thirty-day period described above that the debt, or any portion thereof, is disputed, or that the consumer requests the name and address of the original creditor, the debt collector shall cease collection of the debt, or any disputed portion thereof, until the debt collector obtains verification of the debt or a copy of a judgment, or the name and address of the original creditor, and a copy of such verification or judgment, or name and address of the original creditor, is mailed to the consumer by Company or the debt collector.

MULTIPLE DEBTS

If any consumer owes multiple debts and makes any single payment to Company or the debt collector with respect to such debts, Company or the debt collector may not apply such payment to any debt which is disputed by the consumer and, where applicable, shall apply such payment in accordance with the consumer's directions.

LEGAL ACTIONS

Venue - Company or the debt collector who brings any legal action on a debt against any consumer shall:

- bring such action only in the judicial district or similar legal entity:
    - in which such consumer signed the contract sued upon; or
    - in which such consumer resides at the commencement of the action.

FURNISHING CERTAIN DECEPTIVE FORMS

- It is unlawful to design, compile, and furnish any form knowing that such form would be used to create the false belief in a consumer that a person other than Company is participating in the collection of or in an attempt to collect a debt such consumer allegedly owes Company, when in fact such person is not so participating.

- Any person who violates this section shall be liable to the same extent and in the same manner as a debt collector is liable under the FDCPA for failure to comply with this section.

RELATION TO STATE LAWS

The FDCPA does not annul, alter, or affect, or exempt any person subject to the provisions of this subchapter from complying with the laws of any State with respect to debt collection practices, except to the extent that those laws are inconsistent with any provision of the FDCPA, and then only to the extent of the inconsistency. For purposes of the FDCPA, a State law is not inconsistent if the protection such law affords any consumer is greater than the protection provided by the FDCPA.

IDENTITY THEFT PREVENTION POLICY

POLICY

The provisions of the Identity Theft Prevention Policy are in scope with adherence to the Federal Trade Commission ("FTC") Red Flags Rule. This Policy provides employees with guidance on how to protect our customers from identity theft as required by the Red Flags Rule. The Policy is appropriate to Company's size and complexity and the nature and scope of our activities. The Policy addresses:

- Identifying relevant identity theft Red Flags for Company
- Detecting those Red Flags
- Responding appropriately to any that are detected to prevent and mitigate identity theft
- Updating this Policy periodically, no less than annually, to reflect changes in risks

Our identity theft policies, procedures, and internal controls will be reviewed and updated periodically to ensure they reflect changes both in regulations and in our business.

RISK ASSESSMENT

Company will conduct a Risk Assessment identifying identity theft risk factors related to loan products, the process used to originate and fund loans, the way that customer information can be accessed, and its experience with identity theft. The Policy is based on information obtained during the Risk Assessment.

Company will review this Policy annually and update the Policy whenever there is a material change to operations, structure, business, or location or if we experience an increase or change in our experience with identity theft.

On an ongoing basis, Compliance will review new methods of identity theft, evaluate the risk they pose to Company, and make recommendations to Management regarding identity theft prevention and changes to this Policy as needed.

POLICY ADMINISTRATION

The BSA Officer is responsible for the oversight, development, implementation and administration (including employee training and oversight of third-party service providers) of this Policy.

OTHER GUIDANCE

The Company BSA Policy, privacy policy, and data security policy including protection of customer information overlap with considerations addressed in this Policy and can be reviewed by employees for additional guidance.

TRAINING

Compliance will perform mandatory annual Red Flags training for all loan operations staff, and will train all new operations staff regarding Red Flags within 90 days of their start date.

IDENTIFYING RELEVANT RED FLAGS

Company will use information learned in its initial Risk Assessment to identify identity theft Red Flags and will revise these Red Flags from time to time based on changes to risk factors, changes to identity theft techniques and supervisory guidance. Company reviewed these risk factors:

- Types of loan products offered
- Methods used to open or access these loan products and customer information
- Previous experience with identity theft

Company used its experience and its industry's experience and the Red Flags contained in the FTC's Red Flags Rule deemed relevant to its business to develop its Red Flags:

1. Alerts, notifications or warnings from a credit reporting agency and the results from Company's use of customer authentication and fraud analytics supplied by specialized data providers;
2. Suspicious documents;
3. Suspicious identifying information, such as suspicious address
4. Suspicious account activity; and
5. Notices from other sources (customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts)

DETECTING RED FLAGS

Red Flags are detected during the application process when identifying information is obtained about new customers and the identity of new customers is verified. Red Flags are detected for funded loans when customers are authenticated for access to their loans, customer activity is monitored, and change requests (name, address, authorized users) are verified.

PREVENTING AND MITIGATING IDENTITY THEFT

Company will use information obtained in its initial Risk Assessment to develop procedures to respond to detected identity theft Red Flags. These procedures will be reviewed from time to time and revised as needed.

Procedures to Prevent and Mitigate Identity Theft

When Company receives notice of an actual or suspected data breach or its detection procedures show evidence of a Red Flag, these steps will be taken, as appropriate to the type and seriousness of the threat:

1. **Applicants** – For Red Flags raised when processing a loan application:

    a. ***Review the Application*** – The BSA Officer or a member of the Fraud Team will review the applicant's information collected pursuant to our Know Your Customer ("KYC") requirements under our AML ACT Program (e.g., name, date of birth, physical address, and an identification number such as a Social Security Number or Taxpayer Identification Number).

    b. ***Seek Additional Verification*** – The BSA Officer or a member of the Fraud Team determines the potential risk of identity theft indicated by the Red Flag is probable, the customer's identity will be verified through non-documentary methods, including:
    - Contacting the customer;
    - Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database or other third-party data sources;
    - Checking banking account references with other financial institutions, via direct call or other online resources; or
    - Obtaining a tax return, birth certificate, or other documentation.

    c. ***Deny the Application*** – If the BSA Officer or a member of the Fraud Team determines the customer is using an identity other than his or her own, we will deny the application.

    d. ***Report*** – If the BSA Officer or a member of the Fraud Team has determined the customer is using an identity other than his or her own, it will be reported to our Bank partner.

    e. ***Notification*** – If the BSA Officer or a member of the Fraud Team determines personally identifiable information has been accessed, Company will prepare any specific notice to customer.

2. **Access Seekers** – For Red Flags raised by someone seeking to access an existing customer's loan information such as a change in address:

    a. ***Check with the Customer*** – Company will contact the customer using our information for them, describe what we have found and verify with them that there has been an attempt at identity theft.

b. ***Heightened Risk*** – Company will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a data security incident, or the customer's giving account information to an imposter pretending to represent Company or to a fraudulent web site.

c. ***Check Similar Accounts*** – Company will review other customer loans to determine if there have been attempts to access them without authorization.

d. ***Report*** – If the BSA Officer or a member of the Fraud Team has determined the customer is using an identity other than his or her own, it will be reported to our Bank partner.

e. ***Notification*** – If the BSA Officer or a member of the Fraud Team has determined personally identifiable information has been accessed, Company will prepare any specific notice to customer.

f. ***Assist the Customer*** – Company will work with our customers to minimize the impact of identity theft by taking the following actions, as applicable:
- Offering to change the password, security codes or other ways to access the threatened account;
- Not collecting on the loan or selling it to a debt collector; and
- Instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

CLEARING FIRM AND OTHER SERVICE PROVIDERS

Company may use various service providers in connection with our customer loans. Each service provider that performs activities in connection with our customer loans are required to comply with reasonable policies and procedures designed to detect, prevent, and mitigate identity theft. Company will verify that the service providers have such policies and procedures in place. While not required, this can be done by requesting appreciate certifications or audits such as SSAE 16 SOC 1, 2, or 3 Compliance.

REPORTING

Compliance is responsible for developing, implementing, and administering this Policy will report at least annually to the Management on compliance with the Red Flags Rule. The report will address the effectiveness of this Policy in addressing the risk of identity theft in connection with new loans, existing loans, service provider arrangements, and incidents involving identity theft and management's response. Compliance will provide recommendations for changes needed to this Policy.

RED FLAG AREAS OF CONCERN

1. **Red Flags in Connection with an Account Application or an Existing Account Information From a Consumer Reporting Agency**

   a. A fraud or active duty alert, or a notice of credit freeze is included with a consumer report or in response to a request for one.

   b. A notice of address discrepancy is provided by a consumer reporting agency.

   c. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
      - A recent and significant increase in the volume of inquiries.
      - An unusual number of recently established credit relationships.
      - An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. **Documentary Identification**

   a. Documents provided for identification or the application appears to have been altered or forged.

   b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

   c. Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.

   d. Other information on the identification is not consistent with information that is on file.

3. **Personal Information**

   a. Personal information provided is inconsistent when compared against external information sources. For example:
      - The address does not match any address in the consumer report; or
      - The Social Security Number ("SSN") has not been issued, or is listed on the Social Security Administration's Death Master File.

   b. Personal information provided is internally inconsistent. For example, there is a lack of correlation between the SSN range and date of birth.

c. Personal information provided is associated with known fraudulent activity. For example:
- The address on an application is the same as the address provided on a fraudulent application; or
- The phone number on an application is the same as the number provided on a fraudulent application.
- The address on an application is fictitious, a mail drop, or prison.
- The phone number is invalid, or is associated with a pager or answering service.

d. The address, SSN, or home or cell phone number provided is the same as that submitted by other persons opening an account or other customer's application.

e. Personal information provided is not consistent with information that is on file.

f. The person opening the account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. **Address Changes**

a. A request for address or other account information change is requested during or shortly after loan funding.

b. Mail sent to the customer is returned as undeliverable.

5. **Anomalous Use of the Account**

a. A new loan is used in a manner commonly associated with fraud. (Company typically does not verify and is not made aware of the customer's use of loan proceeds after loan funding).

b. An account is used in a manner that is not consistent with established patterns of activity on the account. For example, nonpayment when there is no history of late or missed payments, especially if the nonpayment is the first payment due on a new loan.

6. **Notice from Customers or Others Regarding Customer Accounts**

a. Company is notified of unauthorized charges in connection with a customer's account.

b. Company is notified that it has opened a fraudulent account for a person engaged in identity theft.

c. Company is notified that the customer is not receiving account-related communications.

d. Company is notified that a customer has provided information to someone fraudulently claiming to represent Company. In this scenario, the customers may have been asked to provide information to a fraudulent website that looks very similar, if not identical, to Company's website.

7. **Other Red Flags**

a. A Company employee has accessed or downloaded an unusually large number of customer account records.

b. Company detects attempts to access a customer's account by unauthorized persons.

c. Company detects or is informed of unauthorized access to a customer's personal information.

d. The person opening an account or customer is unable to lift a credit freeze placed on his or her consumer report.

COMPLAINTS AND INQUIRIES POLICY

PURPOSE

Company provides financial services to consumers, and therefore relies on the goodwill of its customers to remain in business. Company earns that goodwill by ensuring that it provides the quality of service that its customers demand. Therefore, Company strives to be a market leader in its industry with regard to customer service. To be a leader, Company will address and resolve all Complaints and Inquiries in a responsive and timely manner.

SCOPE

Company's Compliance Management System will ensure the accurate and responsive handling of consumer and customer Complaints and Inquiries. Intelligence gathered from Complaints and Inquiries will be organized, evaluated, and retained as part of the Complaints Management System.

POLICY

It is the policy of Company to address and resolve all Complaints and Inquiries in a responsive and timely manner. The Chief Legal and Compliance Officer is responsible for the Complaints Management System. The Compliance Department will work with the Office of the President ("Presidential") to effectively manage the Complaints and Inquiries process.

COMPLAINTS AND INQUIRIES

Complaints

A **Complaint** is a consumer or customer oral or written communication that expresses dissatisfaction with a person, process, policy, product or service provided by Company. Examples of a Complaint includes, but is not limited to, the following:

- Threat of or escalation to a Federal regulatory agency such as the Consumer Financial Protection Bureau ("CFPB"), Federal Deposit Insurance Corporation ("FDIC"), Federal Trade Commission ("FTC"), Federal Communications Commission ("FCC"), Department of Justice ("DOJ"), Department of Defense ("DOD"), etc.
- Threat of or escalation to a state regulatory agency such as the State Attorney General, Department of Financial Services, Department of Consumer Protection, etc.
- Threat of or escalation to the Better Business Bureau ("BBB").
- Threat of or escalation to an attorney.
- Threat to write negative comments or reviews on Social Media.
- A consumer or customer states they have been unfairly treated, deceived, misled, or abused.
- A consumer or customer states they have been discriminated against.

Inquiries

An **Inquiry** is not a Complaint as defined above. It is a consumer or customer oral or written

communication that requests information or action regarding a person, process, product or service provided by Company.

OFFICE OF THE PRESIDENT

It shall be the responsibility of all Company employees to ensure that all Complaints and Inquiries received are immediately sent to Presidential for review and response. Presidential will research the allegations of all Complaints and Inquiries and respond in a timely manner.

COMPLIANCE REVIEW

The Compliance Department will review all Complaint responses before they are sent to ensure accuracy and timeliness of the response. Compliance is responsible for tracking and reporting all Complaint and Inquiry trends and potential compliance issues.

TRACKING SYSTEM

Company will implement a Complaint and Inquiry Tracking System. The Tracking System will be utilized to store all Complaints and Inquiries, trends, the channels in which they are received, and areas that may need improvement for training purposes.

COMPLAINT AND INQUIRY CODES

Complaint and Inquiry Codes will be created to track and report different metrics. Every Complaint or Inquiry will have a Code or Codes assigned. The Code(s) will be assigned once a review of the Complaint or Inquiry is completed by Presidential.

REPORTING

Compliance will generate various reports regarding Complaints and Inquiries. The reports will be provided to the Complaints Review Committee for review and analysis on a quarterly basis. There will also be daily Complaints and Inquiries reports generated as delineated below:

- **Complaints and Inquiries Filed – Leads Report**
  Daily, a Complaints and Inquiries Report regarding Leads will automatically be generated and sent to Presidential for review. The Report will show any new Complaints and Inquiries from Leads that were received and entered into the Complaints and Inquiries tracking system.

- **Complaints and Inquiries Filed – Accounts Report**
  Daily, a Complaints and Inquiries Report regarding loan Accounts will automatically be generated and sent to Presidential for review. The Report will show any new Complaints and Inquiries from loan Accounts that were received and entered into the Complaints and Inquiries tracking system.

COMPLAINTS REVIEW COMMITTEE

A Complaints Review Committee, chaired by the Chief Legal and Compliance Officer, will be established and meet on a quarterly basis. At the quarterly Complaint Review meeting, members of the Committee will review Complaint or Inquiry reports for issues or trends of concern. The Committee will determine if any corrective action needs to be implemented.

COMPLAINTS REPORT TO THE BOARD AUDIT COMMITTEE

The Compliance Department will provide the Audit Committee for the Board of Directors with a Complaints and Inquiries Management Report on a quarterly basis.

TRAINING

The Compliance Department will provide ongoing training to Presidential regarding reviewing and responding to Complaints and Inquiries. The Compliance Department will also provide training to other applicable Departments as needed, but no less than annually.

COMMUNITY REINVESTMENT ACT POLICY

PURPOSE

The Community Reinvestment Act Program ("CRA Program") of Company is designed to identify and implement where available, the necessary funding or services aimed at meeting the needs of the low to moderate-income sector of the community.

POLICY

Although not required, Company's policy shall be to comply with all applicable requirements of the *Community Reinvestment Act* ("CRA") and *Regulation BB*, which implements the CRA (hereinafter, collectively referred to as the "Law" through the remainder of this Policy) in the implementation of the CRA Program. The following items outline the way Company intends to implement the CRA Program:

- Establish a CRA Committee comprised of no less than one member of executive management and one member of the Board of Directors. The Board of Directors will approve the CRA Program. Once the Program is implemented, the CRA Committee will meet at least semi-annually to receive CRA Program updates as well as future initiative recommendations from the CRA Officer.

- The CRA Committee will appoint a CRA Officer to devise, implement, and maintain the approved CRA Program.

- The CRA Program will ensure:

    - Company addresses Community Development (CD) needs by providing a high level of innovative CD services.

    - CD includes the following: (1) Affordable housing for low or moderate income individuals; (2) Community services targeted to low or moderate income individuals; (3) Activities that promote economic development by financing Small Business Programs; and (4) Activities that revitalize or stabilize low or moderate income geographies, designated disaster areas, or distressed or underserved nonmetropolitan middle income geographies.

    - Grant Funding disbursements to non-profit agencies will be issued as applicable.

    - Company representatives that participate on the Boards of Directors of nonprofit agencies will track and report their community service activities to the CRA Officer as requested.

- The CRA Officer will maintain all appropriate records about the CRA Program, including but not limited to: funding disbursements, service test activities, non-profit

correspondence and all requisite financial information as it pertains to both non-profits and affiliated activities within the CRA Program.

- The CRA Program will be periodically audited internally to assess the overall effectiveness and performance within the CRA Program.