STERLING BANCORP, INC.
CODE OF BUSINESS CONDUCT AND ETHICS
Board Approved: October 17, 2017

1. GENERAL PRINCIPLES

STERLING BANCORP, INC., a Michigan corporation and each of its subsidiaries (collectively, the ***"Company"***) is committed to maintaining the highest standards of business conduct and ethics. This Code of Business Conduct and Ethics (the ***"Code"***) reflects the business practices and principles of behavior that support this commitment. We expect every employee, officer and director to read and understand the Code and its application to the performance of his or her business responsibilities. References in the Code to employees are intended to cover officers and, as applicable, directors.

Officers, managers and other supervisors are expected to develop in employees a sense of commitment to the spirit, as well as the letter, of the Code. Supervisors are also expected to use reasonable best efforts to ensure that all agents and contractors conform to Code standards when working for or on behalf of the Company. The compliance environment within each supervisor's assigned area of responsibility will be a factor in evaluating the quality of that individual's performance. In addition, any employee who makes an exemplary effort to implement and uphold our legal and ethical standards may be recognized for that effort in his or her performance review. Nothing in the Code alters the at-will employment policy of the Company.

This Code cannot possibly describe every practice or principle related to honest and ethical conduct. The Code addresses conduct that is particularly important to proper dealings with the people and entities with whom we interact, but reflects only a part of our commitment. From time to time we may adopt additional policies and procedures with which our employees, officers and directors are expected to comply, if applicable to them. However, it is the responsibility of each employee to apply common sense, together with his or her own highest personal ethical standards, in making business decisions where there is no stated guideline in the Code.

Action by members of your family, significant others or other persons who live in your household (referred to in the Code as "family members") also may potentially result in ethical issues to the extent that they involve the Company's business. For example, acceptance of inappropriate gifts by a family member from one of our suppliers could create a conflict of interest and result in a Code violation attributable to you. Consequently, in complying with the Code, you should consider not only your own conduct, but also that of your family members, significant others and other persons who live in your household.

The foundation of our Code consists of basic standards of business as well as personal conduct: (a) honesty and candor in our activities, (b) avoidance of conflicts, or the appearance of conflicts, between personal interests and Company interests, (c) maintenance of our reputation and avoidance of activities that may reflect adversely on the Company, and (d) integrity in dealing with the Company's assets.

You should read this Code carefully. If a provision of the Code is not clear or if there is a question about its applicability, you should consult your supervisor. You should remember that the public sees each of us as a representative of the Company. Accordingly, your understanding and support of this Code means a continued public trust in the Company.

The policies contained in the Code are supplemented, in part, by other policies of the Company, including those set forth in the Company's Employee Handbook. Such other policies, however, are not to be construed in any way to modify the policies contained in the Code. Directors, officers and employees are expected to be aware of all Company policies and to conduct themselves in accordance with all Company policies at all times.

Each employee or officer who violates this Code or permits others to do so will be subject to dismissal or other disciplinary action as deemed appropriate by the Company, in its sole discretion, and, where appropriate, legal action. Each director who violates this Code or permits others to do so will be subject to removal from the Board or such other action as deemed appropriate by the Board of Directors, in its sole discretion, and where appropriate, legal action.

The Board of Directors reserves the right at any time to change, modify or eliminate policies and procedures contained in this Code, or elsewhere.

2. SCOPE

The Code is applicable to all employees (including part-time employees), officers and members of the Company's board of directors. In addition, certain restrictions will apply to certain members of their immediate family, including those involved with any business firm in which they have a substantial financial interest. To avoid confusion, the following terms will be used in this Code with their indicated definitions:

- **Immediate Family** - the child, stepchild, parent, stepparent, spouse, sibling, mother-in-law, father-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law of any employee, officer or director, as well as any other person living in the home of any employee, officer or director or who is getting a majority of his or her support or who is otherwise considered a dependent of the employee, officer or director.

- **Related Business** - any business entity, other than the Company, in which an employee, officer or director, or any member of their immediate family, has a significant financial interest, including ownership of 5% or more of the equity of such business entity.

3. DISCLOSURE OF CONFIDENTIAL INFORMATION

It is essential that you safeguard the confidential nature of information concerning Company transactions, present and prospective customers, suppliers, officers, employees, directors and shareholders. You must use caution in using or sharing such information. Confidentiality applies with equal force to customer and Company affairs. This concern applies to more than customer information which has been explicitly designated confidential. There are other situations in which information is not publicly available, and unauthorized disclosure could have serious effects on a customer or Company.

Confidentiality is important regardless of the form the information takes – oral, in print, or on electronic equipment. You must take care in what you say, to whom and where; about how you treat memos, files and reports; and about seeing that there is no misuse of the information you display either electronically, in paper form, or both, including but not limited to computer screens and handheld devices (whether employee-owned or Company-owned devices), and stored in databases.

Should you remove from the Company's premises any written, printed, or electronically generated material belonging to or generated by the Company or derived from its files, you should do so only for the benefit of the Company and in prior consultation with your supervisor; and you must take every precaution to ensure the security and confidentiality of all information both in electronic and paper form.

A director, officer, or employee may not disclose to unauthorized persons confidential information or records pertaining to or concerning the affairs of the Company or its customers. Within the Company, disclosure of such information must be limited to those persons whose duties require and permit them to have access to it. Confidential customer or Company information, such as information available to one unit of the Company, should be communicated to other units only in cases of legitimate business need as determined by an applicable supervisor.

You should not discuss confidential information relating to customers or the Company with anyone outside the Company, other than the Company's independent auditors, legal counsel, or regulatory examiners, unless authorized by the customer or required by proper legal process as determined by legal counsel.

Confidential information must not be used to further your private interest or for your personal gain. Improper use of this information may make you and the Company liable under federal and state securities and privacy laws, and may also result in civil or criminal penalties, both for you and the Company.

All employees and officers must agree to the confidentiality and post-employment obligations contained in the Confidential Information Usage Agreement.

Additionally, employees, officers, and directors who have access to confidential (or "inside") information are not permitted to use or share that information for stock trading purposes or for any other purpose except to conduct our business. All non-public information about the Company or about companies with which we do business is considered confidential information. To use material non-public information in connection with buying or selling securities, including "tipping" others who might make an investment decision on the basis of this information, is not only unethical, it is illegal. Employees, officers and directors must exercise the utmost care when handling material inside information.

For additional information on insider trading, you can review our Insider Trading Policy which you will be expected to comply with as a condition of your employment with the Company. You should consult our Insider Trading Policy for more specific information on the definition of "inside" information and on buying and selling our securities or securities of companies with which we do business.

4. REQUEST FOR INFORMATION AND MEDIA RELATIONS POLICY

It is Company policy that only designated senior executives are authorized to respond to external information requests. In order to ensure all media inquiries are handled in a consistent and responsive manner, ANY media contacts should be referred to the Chief Operating Officer and General Counsel, who then will determine which senior executive is best prepared to respond to the request.

Unauthorized employees and officers who respond to media inquiries or other requests for confidential information will be subject to disciplinary action up to and including immediate termination.

You also may not provide any information to the media about us off the record, for background, confidentially or secretly, including, without limitation, by way of postings on internet websites, chat rooms or "blogs".

5. COMPUTER, INTERNET AND ELECTRONIC COMMUNICATION ACCEPTABLE USE POLICY

To the extent that you are required or authorized to use or operate computers and/or e-mail and/or to access the Internet or any other database, data storage media or devices (such as disks, hard drives or memory sticks) or information stored in any computer or other electronic data retention source (collectively, "Company Systems"), you are required to comply with the Computer, Internet and Electronic Communication Acceptable Use Policy. Employees, officers and directors who violate this policy will be subject to disciplinary action up to and including immediate termination.

The Company Systems, all electronic communication, e-mail, data communications and information created, accessed or stored on the Company's computer system or using the Company's applications and systems, including but not limited to information transmitted or stored by e-mail, information downloaded from or posted on the Internet or any other data retention source, whether viewed using Company equipment or personally-owned

electronic equipment, (hereinafter, "Personal Equipment") is the sole and exclusive property of the Company. The use of Personal Equipment to access Company Systems is also discussed, below, in Section 6.

Employees have access to the Company Systems consistent with the requirements of their jobs. Different access levels are designated for various job functions and user-IDs and passwords are issued to enable each employee to log onto the Company Systems and use appropriate functions. Employees are expected to develop the necessary skills to use the Company Systems at the appropriate level of proficiency to complete their job-oriented tasks, and are required to use the systems in an employment appropriate manner. If an individual is given access to the Company's computer systems, he or she must not allow any other individual to use his or her assigned access code(s) and must restrict system use to the business purposes for which it was intended. Individuals must logout of the computer system (AS/400, local and wide area network, Internet connections, or Lotus Notes) when their PC or terminal is unattended for any extended period of time (for example, during meetings, lunch breaks and non-business hours). Management will approve Internet access as deemed appropriate and will determine what components of the Internet will be available (such as, email, World Wide Web, newsgroups, chat rooms, etc.). Those individuals that are granted access to the Internet or email should be aware that Internet and email usage will be monitored and distributed to senior management and/or the Information Systems Steering Committee.

Maintaining the integrity and security of the Company and customer information is crucial. Employees must handle all information, whether in paper files or electronic records, and whether accessed on Company equipment or Personal Equipment, in a manner which safeguards its integrity (accurate, timely, and complete) and its security (safety from loss or unauthorized access). No material or information that comes to an individual in the course of his or her work is to be shown to or discussed with anyone else, inside or outside of the Company, except as is necessary to carry out the work or perform the service involved.

All employees shall practice proper network etiquette, which includes being polite and using the computer system, Internet, email, and all other forms of electronic communication in a safe and legal manner. All employees accessing the Internet for Company purposes using Company equipment or Personal Equipment, on a Company Internet access account, or on behalf of the Company by other means, should become proficient in its capabilities, practice proper network etiquette, and must agree to the conditions and requirements of this policy. Employees may be liable for using the Internet, email or any other forms of electronic communication in a way that violates a statute or infringes on the right of others, such as copyright infringement, defamatory materials, sexually explicit materials, harassment, or committing the Company to a business contract or agreement. Employees should write any email messages as if they are business memorandums that are to be kept on file for future reference.

COMPUTER, INTERNET, EMAIL, AND ELECTRONIC COMMUNICATION PRIVILEGES PROVIDED BY THE COMPANY ON BOTH COMPANY EQUIPMENT AND PERSONAL EQUIPMENT ARE COMPANY RESOURCES AND ARE INTENDED TO BE USED FOR PERMISSIBLE COMPANY BUSINESS PURPOSES ONLY. PERSONAL USE OF COMPANY EQUIPMENT IS PROHIBITED. EMPLOYEES DO NOT HAVE A RIGHT TO PRIVACY OR CONFIDENTIALITY IN CONNECTION WITH ANY ACTIVITY CONDUCTED USING THE COMPANY'S COMPUTER SYSTEM, OR E-MAILS, THE INTERNET, OR ELECTRONIC COMMUNICATION UTILIZED IN CONNECTION WITH COMPANY EQUIPMENT **OR** PERSONAL EQUIPMENT, INCLUDING BUT NOT LIMITED TO ANY OTHER ASPECT OF THE COMPANY SYSTEMS. EMPLOYEES THEREFORE SHOULD NOT EXPECT OR TREAT COMPUTER, INTERNET ACCESS, EMAILS OR ELECTRONIC COMMUNICATION AS CONFIDENTIAL OR PRIVATE, WHETHER SUCH COMMUNICATION IS FACILITATED USING COMPANY EQUIPMENT **OR** PERSONAL EQUIPMENT.

The Company reserves the right to access, monitor, inspect, review, disclose, copy, store, or terminate access to, at any time, for any reason and without prior notice, any and all usage of its computer system, the Internet, electronic communication, including email, and all other aspects of the Company Systems, whether such usage was conducted on Company equipment or Personal Equipment. Such usage includes, but is not limited to, the distribution of any information through the Internet or email and messaging systems, any and all emails sent to or received from

supervisors, co-workers and persons outside of the Company, data, communications, information, materials, files, software, and other content transmitted, received, or stored in connection with this usage, Internet access or postings or other information being downloaded, sent through, stored or transmitted to or from the Company's computers, including social media sites (eg. Instagram, SnapChat, Facebook, MySpace, LinkedIn, and Twitter). Usage will be monitored for unusual or unacceptable activity and the Company reserves the right to determine the suitability of this usage. Any accessing, monitoring, inspection, review, copying, and/or storage will be performed by authorized representatives of the Company and/or its auditors.

Use of system security features such as passwords and "delete" buttons do not limit the Company's ability or right to access, monitor, inspect, review, disclose, copy and/or store emails or other information. All electronic communications, including emails transmitted and received are subject to retention by the Company even if the sender and recipient both have deleted the electronic communications from their computers or Personal Equipment.

When sending electronic communications, including emails, employees must use extreme caution to insure that the correct address is used for the intended recipient. Because of the security risks inherent in sending emails to external parties, employees are directed to limit their external email communications to include non-confidential information only. However, in the event that confidential information does need to be sent externally, employees must use the Company's secure email provider or regulatory agency-specific secure email, as appropriate. Use of confidentiality disclosures should be considered for all internal and external electronic communications. Electronic communications should be deleted from the employee's computer as soon as practicable to allow efficient use of the email system and storage space.

<u>As set forth below, the Computer, Internet and Electronic Communication Acceptable Use Policy prohibits certain conduct by employees</u>.

- The solicitation of non-company business for personal gain or profit is prohibited.

- The solicitation of employees or distribution of information via electronic communication, including email or the Internet not related to the Company's business is prohibited.

- Employees are prohibited from using the Company's computer system, the Internet, electronic communication including email, or any other aspect of the Company Systems, for any illegal purpose.

- The defaults on the Company's Internet browsers have been set to provide the most possible protection for the Company against unwanted intrusions and viruses. Employees may not change the default settings without prior written approval. To protect the Company against viruses and unintentional copyright infringement, employees must not download any software or files from the Internet, unless prior written authorization is received.

- Messages or images that are offensive, sexually explicit, obscene or harassing, intimidating, discriminatory, or which are intended to annoy, harass, or intimidate another person, including but not limited to verbal abuse, menacing comments, defamation, disparagement, jokes, statements or innuendos regarding race, color, national origin, sex, gender, sexual orientation, age, religion, height, weight, marital status, or disability, must not be created or stored on, transmitted, posted or received by, or downloaded onto, or accessed by Company computers or equipment. This prohibition includes, but is not limited to the use of the Internet to access any sexually explicit, obscene, harassing or otherwise offensive web site or the use of electronic communication (including email) to transmit or receive any sexually explicit, obscene, harassing or otherwise offensive message or image. The Company reserves the right to monitor all Internet Web sites. Employees are prohibited from knowingly visiting Internet sites that contain or feature

pornography, terrorism, espionage, theft, drugs, or obscene, hateful or other objectionable materials. Employees are also prohibited from making or posting indecent remarks, proposals, or materials.

- Employees are prohibited from using the Company's computer system, the Internet or electronic communication (including email), or any other aspect of the Company Systems, to participate in unauthorized political or religious activities.

- Employees are prohibited from examining, changing or using another person's files, output, or user name for which the employee does not have explicit authorization.

- Employees must not represent personal opinions as those of the Company or purport to represent the Company when not authorized to do so.

- Revealing or publicizing confidential or proprietary information, including, but not limited to, financial information, confidential client information, marketing strategies and plans, databases and any information contained therein, client lists, computer software source codes, computer/network access codes, and business relationships, is prohibited. Trade secrets and confidential business information, including but not limited to product development, financial statements and/or other information, shall not be transmitted by electronic means (including email) outside of the Company or transmitted over or posted on the Internet.

- License agreements vary among suppliers. Loading of all software must therefore be authorized by Information Systems ("I.S.") to ensure compliance with licensing agreements and to ensure the software is virus free. Using any software on the Computer Systems other than that licensed or approved by the Company is prohibited.

- Uploading, downloading or transmitting commercial software or any copyrighted material without permission from the owner of the copyright in those materials, and the prior written approval from the Chief Executive Officer, the President or Chief Information Officer of the Company is prohibited.

- No individual may remove software from the Company's computer system(s) and take it home to use, or bring in software from home to use on the Company's computer system(s). Any duplication of licensed software, except for back-up purposes, may be a violation of the Federal Copyright Act. Individuals must adhere to all software license agreements.

- Intentionally interfering with the normal operation of any aspect of the Company Systems, including the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the Company Systems, is prohibited.

- Due to the increase in detected PC viruses and the potential dangers viruses create, the use of data storage media or devices (such as disks, hard drives or memory sticks) from home, vendor or any other outside source for use at the Company is prohibited. If you currently have such media or devices in your possession for business use, please refrain from using them until they can be checked for viruses. I.S. can be contacted for instructions on this process, if advised by management.

- The use of equipment, which is not owned by the Company, is prohibited. Employees must refrain from bringing equipment into the Company with the purpose of connecting to the Company's

network that has not been purchased and/or registered with the Company. This includes, but is not limited to, desktop PCs, laptop PCs, printers, scanning devices, PC label makers, etc.

- Using Company equipment or other resources for any purpose other than that authorized by management is prohibited.

- When using a laptop, notebook computer, or similar remote device (including Personal Equipment), logging into any Company System from a public internet connection that is not password-protected is strictly prohibited.

- Wasting Company time by using the Internet for non-Company business-related purposes is prohibited.

- Sharing passwords with any other user or unauthorized individual is prohibited.

- Identifying oneself in any way other than honestly, accurately, and completely in instances such as, but not limited to, participating in chats or newsgroups, or when setting up accounts on outside computer systems, is prohibited.

- Performing any other uses or engaging in any other conduct identified by the Company in connection with the Company's computer system, the Internet, electronic communication (including email) or any other aspect of the Company Systems as inappropriate is prohibited.

Any employees who have questions concerning this policy or require assistance understanding its content should consult with their supervisor or manager. Employees must immediately report all violations or suspected violations of this policy to a member of executive management of the Company.

6. USE OF PERSONAL EQUIPMENT

Certain employees with business need for connectivity to Company Systems on Personal Equipment may be approved for such access. Likewise, such access may be revoked at any time in the Company's sole discretion. Such Personal Equipment must be password-protected and exclusively owned and used by the employee granted such connectivity. Employees must keep anti-virus software up-to-date, and agree to notify the Company immediately if the Personal Equipment is lost or stolen. In the event that any Personal Equipment authorized for access to Company Systems is lost or stolen, it will be remotely wiped of data. Employees must understand that personal data, including photos, on Personal Equipment may be lost as a result of remote wiping. The Company may indefinitely retain the Personal Equipment as evidence, if the Personal Equipment is to be used as evidence in a potential or pending legal action. Personal Equipment must be used in accordance with the Computer, Internet and Electronic Communication Acceptable Use Policy, above. Storing of unapproved Company business information on the Personal Equipment or at any unapproved third party site is expressly forbidden. Employees shall not use Personal Equipment to access the internet on a public wireless network that does not require a password. Additionally, any employee approved for connectivity to Company Systems on Personal Equipment agrees to indemnify the Company against any claims of ownership of such Personal Equipment, and shall hold the Company harmless in all matters relating to the use of the Personal Equipment.

7. IDENTITY THEFT OR PRETEXT CALLING

Federal law makes it a crime to knowingly use, without lawful authority, a means of identification (such as an individual's social security number or date of birth) of another person with an intent to commit a crime, such as credit card, check, loan or mortgage fraud.

Federal law also makes it a crime to obtain customer information by means of false or fraudulent statements to an officer, employee, agent or customer of a financial institution, or to request a third party to obtain customer information from a bank or other financial institution, if the third party knows that the information will be obtained through fraudulent methods, such as pretext calling.

An employee or officer who knowingly commits identity theft, engages in pretext calling, or facilitates a third party in doing so IS PERSONALLY LIABLE FOR ANY MONETARY LOSS INCURRED BY THE COMPANY, ITS CUSTOMERS OR SUPPLIERS, AS A RESULT OF THE IDENTITY THEFT OR PRETEXT CALLING.

8. CONFLICT OF INTEREST

It is important for every business to avoid conflicts of interest on the part of its personnel that could impair their independence of judgment. It is the desire of the Company to avoid not only actual and potential conflicts, but also the appearance of conflicts of interest involving any employee, officer or director of the Company. Because it is impossible to list all potential conflicts of interest, you are expected to use common sense and discretion in all transactions and relationships and are required to make a prompt and complete disclosure of any possible or probable conflicts of interest. When there is any question that a conflict of interest may be involved in any existing situation or proposed action, you should not attempt to judge your own case, but you should resolve any doubt in favor of non-involvement or full disclosure of the conflict to the Company.

Examples of conflicts of interest to avoid or for which full disclosure is required include, but are not limited to, the following:

- No employee or officer may engage in any activity (including the ownership of a financial interest in any related business) which is competitive with the business activities and operations conducted from time to time by the Company.

- No employee, director or officer may engage in any part-time business consulting arrangements or other business activities that will affect his or her ability to perform duties properly and efficiently for the Company or adversely affect the good name or reputation of the Company, excluding normal civic or charitable duties.

- No employee, officer or director may take advantage of a business opportunity for his or her own or another person's personal profit or benefit when the opportunity is within the corporate powers of the Company and the opportunity is of present or potential advantage to the Company.

- No employee, officer or director may borrow from customers or suppliers of the Company, except those who engage in the usual course of their business and then only on terms offered to others in similar circumstances, without special treatment on terms, interest rates, security, repayment terms, or similar terms. This prohibition does not include borrowing from persons related to the employee by blood or marriage.

- No employee, officer or director or any member of their immediate family member, may sell or lease to buy or lease from the Company any kind of property, facility, equipment or service directly or indirectly from or to the Company without the approval of the Chief Executive Officer or the President.

- No employee, officer or director or any of their immediate family members, may have any interest, direct or indirect, in any vendor, supplier, contractor or subcontractor doing business with the Company.

- No employee, officer or director may engage in any activity that affects or appears to affect the employee's or officer’s independence of judgment concerning transactions between the Company, its customers or suppliers. In particular, no employee, officer or director should represent the Company in any transaction if the personal interest of the employee or officer, or the personal interest of any of their immediate family members, might affect their ability to represent the Company’s interests fairly and impartially.

- Except in the course of his or her authorized duties as an employee, officer or director of the Company, he or she shall not (i) become obligated for the payment of a customer's debt, (ii) accept any custody or control of a customer's property, (iii) serve as a trustee, agent, attorney, or other fiduciary for a customer, or (iv) engage in any personal financial or business dealings with a customer. Examples of conduct prohibited by this provision include, but are not limited to:

- co-signing a customer's note;

- having signature authority over a customer's deposit account;

- serving as a personal representative of a customer's estate;

- serving as co-trustee of a customer's trust;

- being designated as a customer's agent under a power of attorney;

- having possession of a customer's safe deposit box key; and/or

- having a personal investment in a customer's business.

This provision shall not, however, prohibit any such relationship (a) with a member of the immediate family of the employee, officer or director, (b) involving only investments representing less than 5% of the outstanding shares of a publicly traded company, or (c) which, other than as set forth below, has been approved in advance in writing by the Chief Executive Officer or President of the Company.

Whenever you find that you are inadvertently placed in a potential compromising position due to relationships with business associates, customers, suppliers or competitors, you should report the matter immediately to your supervisor and discontinue any activities associated with the entity until the matter has been resolved.

An employee, officer or director whose immediate family member is employed by a broker who handles transactions for the Company must disclose the existence of the relationship to the Human Resources Department of the Company.

Notwithstanding anything to the contrary in the foregoing, directors and executive officers of the Company must seek determinations and prior authorizations or approvals of potential conflicts of interest exclusively from the Audit Committee.

9. INVESTMENTS

Employees (including officers) must not invest or hold any investment directly or indirectly in any financial, business, commercial, or private transaction that creates a conflict with their official duties. In addition, employees, officers and directors must not allow information that has not been made public to influence their own investments.

You must have the advance approval of the Company's executive management to invest directly or indirectly in the stock or business of a customer, supplier or competitor. However, prior approval of the Company's executive management is not needed to invest in the stock of a publicly-held customer, supplier or competitor if:

- you do not service the corporation's account as a loan officer; and,
- your shares do not exceed one percent (1%) of the corporation's issued and outstanding shares.

Investment analysts and executive personnel must have the advance approval of the Company's executive management to invest directly or indirectly in the stock or business of a customer or supplier.

Inheritance under wills or trusts from customers who are not family members could appear to be the result of a personal dealing by an employee or officer. If you discover that you are about to be named as a beneficiary under a will or trust of a non-family member, you should consult with your supervisor prior to accepting.

10. GIFTS AND FEES FROM CUSTOMERS AND SUPPLIERS

A gift is any type of gratuity, favor, service, discount or price concession, loan, legacy (except from a relative), fee, compensation or anything of monetary value. Federal law prohibits Company employees, officers, directors, and their immediate families from requesting or receiving, directly or indirectly, anything of value requested with or given with the intent of influencing or being rewarded in connection with, any transaction or business affair of the Company, including gifts of value from customers or suppliers.

Federal banking regulators are of the opinion that the federal prohibition is not intended to prevent the receipt of gratuities or favors of nominal value if it is clear that what is accepted is not solicited and is NOT offered or received as an inducement to or as a *quid pro quo* for entering into any transaction or business of the Company, or to influence or affect in any way any decision or action of the Company. Examples of gifts of nominal value are:

- gifts of $50 or less such as those received at holiday time or in connection with other special occasions (e.g., promotions or weddings); or
- unsolicited advertising or promotional materials that are generally or routinely available to others in the ordinary course of business having a fair market value of not more than $50.

You and members of your immediate family may not give gifts to or receive gifts from, as the case may be, a customer or supplier if that gift does not meet the above criteria.

In addition, the acceptance of the following are also generally acceptable if they are not being provided with the intent of influencing or rewarding the recipient in connection with any business or transaction of the Company:

- gifts, gratuities, amenities or favors based on obvious family or personal relationships where the circumstances make it clear that it is those relationships rather than the business of the Company which are the motivating factors;
- meals, refreshments, entertainment or other accommodations of a reasonable value (including business lunches and sporting events) which are made available as part of a meeting or other occasion, the purpose of which is to hold business discussions or to foster better business relations, so long as such expenses would be paid for by the Company as a reasonable business expense if not paid by the customer or supplier; or

- discounts or rebates on merchandise or services that do not exceed those made available to other customers.

Cash, checks, loans (except from established banking or financial institutions), stocks or other marketable securities in any amount must not be accepted or given under any circumstances.

Felony criminal penalties including monetary fines and/or imprisonment can be imposed if a director, officer, employee, or member of their immediate families offers something of value, $100.00 or more, to a customer or supplier, or vice versa, where the intent is to influence a transaction or business matter. Where the value of the offer is considered to be less than $100, the crime is a misdemeanor with monetary penalties of up to $1,000 and/or one (1) year in prison.

All prohibited gifts, gratuities, amenities or favors (those with a retail value of $50 or more or which otherwise do not fall within the exceptions set forth above) offered to any party (employees, directors, members of their immediate families, or customers or suppliers) must be disclosed to the employee's supervisor and the Company's executive management, or the Board of Directors, as the case may be.

Discuss with your supervisor or the General Counsel any proposed entertainment or gifts if you are uncertain about their appropriateness.

11. OUTSIDE COMPENSATION

Employees and officers are also encouraged to support the political party or candidates of their choice. However, employees and officers may not make gifts or contributions in the name of or on behalf of the Company.

- No illegal payments, bribes, or kickbacks in any form whatsoever are to be made under any circumstances to obtain a benefit for the Company or the employee, officer, director, or member of their immediate families;

- All contractual placements of the Company business or acceptance of business by the Company must be awarded purely upon business considerations;

- An employee, officer or director must not accept compensation in any form from any person for directing the Company business to such person or for accepting the Company business on behalf of the Company; and

- An employee or officer must not accept compensation for making an oral presentation, wiring an article for publication, or similar activities prepared or conducted on Company time. If normal honorariums are accepted, an employee must make a written report to his or her supervisor.

12. POLITICAL AND COMMUNITY ACTIVITIES

We encourage you to take an active interest in the political process. But if you participate in politics, you do so as an individual and not as a representative of the Company. The Company's name, logo and address should not be used in any advertisement or literature. Use of the Company's posting or mailing services is also prohibited.

Employees and officers are also encouraged to support the political party or candidates of their choice. However, employees and officers may not make gifts or contributions in the name of or on behalf of the Company.

13. DISHONEST OR FRAUDULENT ACTS

An employee, officer or director who commits a dishonest or fraudulent act IS PERSONALLY LIABLE FOR ANY MONETARY LOSS INCURRED BY THE COMPANY, ITS CUSTOMERS OR SUPPLIERS, AS A RESULT OF THE DISHONEST OR FRAUDULENT ACT. Such actions include but are not limited to:

- misappropriating money (whether belonging to the Company or its customers) or other property;
- deliberately misposting accounts;
- making false entries, records, or reports; or
- deliberately misrouting checks to delay payment.

In addition, an employee, officer or director must not make or cause to be made a materially false or misleading statement about or concerning the affairs of the Company.

Any employee, officer or director who commits a dishonest or fraudulent act will be terminated. Furthermore, the law requires the Company to file suspicious activity reports with the appropriate law enforcement agencies after discovery of known or suspected criminal acts involving the Company or its subsidiaries, whether committed by employees or others, or of crimes or suspected crimes believed to be committed by Company employees or others against another financial institution.

14. FINANCIAL INTEGRITY AND BANK RECORDS

The Company relies on its accounting records to produce reports for management, shareholders, creditors, governmental agencies, and others. The Company is committed to maintaining books and records that accurately and fairly reflect its financial transactions. Each employee, officer or director must maintain accurate and fair records of transactions, time reports, expense accounts and other business records. Each such individual must also comply with any applicable record retention policy of the Company.

In this respect, the following guidelines must be followed:

- No undisclosed or unrecorded funds or assets may be established for any purpose.
- Assets and liabilities of the Company must be recognized and stated in accordance with standard practices and Generally Accepted Accounting Principles.
- No false or artificial entries may be made or misleading reports issued.
- No false or fictitious invoices may be paid or created.
- No information may be concealed from internal auditors or independent auditors.

15. DISCLOSURE

The Company's periodic reports and other documents filed with the Securities and Exchange Commission (the "SEC"), including all financial statements and other financial information, must comply with federal securities laws and SEC rules. Each director, officer and employee who contributes in any way to the preparation or verification of the Company's financial statements or other financial information must ensure that the Company's books, records and accounts are accurately maintained. Each director, officer and employee must cooperate fully with the

Company's accounting and internal audit departments, as well as the Company's independent public accountants and counsel. Each director, officer and employee who is involved in the Company's disclosure process must:

- be familiar with and comply with the Company's disclosure controls and procedures and its internal control over financial reporting; and

- take all necessary steps to ensure that all filings with the SEC and all other public communications about the financial and business condition of the Company provide full, fair, accurate, timely and understandable disclosure.

16. AWARENESS OF ILLEGAL CONDUCT/INTERNAL INVESTIGATIONS

If, in conducting business for the Company, an employee becomes aware of any illegal conduct or suspected illegal conduct (including any dishonest or fraudulent act) on the part of any person, the employee must inform the Internal Audit Department, which will investigate the matter. Such reports will be treated as confidentially as possible.

Furthermore, an employee must not refuse to answer questions of the Company's internal investigative personnel concerning any matter related to the performance of his or her official duties or to any other person dealing with or employed by the Company. The Company does not tolerate acts of retaliation against any director, officer of employee who makes a good faith report of known or suspected acts of misconduct or other violations of this Code.

17. NONDISCRIMINATION

Employees must conduct the affairs of the Company without any discrimination based on age, race, national origin, color, sex, religion or creed, marital status, disability, veteran status or related criteria or other protected classes under applicable federal, state or local law. All business decisions must be considered solely on their own merits.

18. FIDUCIARY RELATIONSHIPS

Employees may not accept appointment as an administrator, trustee, personal representative, conservator, or any similar fiduciary capacity without prior approval of the Company unless the employee acts at the request of the Company or as a fiduciary on a family account.

19. PERSONAL MARKETING AND USE OF SOCIAL MEDIA FOR BUSINESS PURPOSES

Employees are generally prohibited from distributing self-created marketing material or using social media (including but not limited to Instagram, SnapChat Facebook, MySpace, Twitter, and Linked In) to market the Company or the Employee's services on behalf of the Company due to the regulatory compliance and legal risks that arise from so doing. Any request for marketing or advertising must be made pursuant to the Company's Advertising Compliance Policy.

20. REPORTS AND DISCLOSURES

Each year, you will be required to complete and file an annual compliance statement on the interests and activities covered by this Code. In addition to this annual disclosure, you must promptly report any event that might involve or appear to involve any conflict of interest. If you have any doubts, you should disclose the appropriate information.

When disclosure (other than disclosure in the annual compliance statement) or approval is required by this Code, such disclosure and approval must be obtained in writing as follows:

- employees of the Company up to and including an Executive Vice President, must disclose to, and seek approval from, the President of the Bank; and

- the Company's executive officers and directors must disclose to, and seek approval from, the Audit Committee.

All disclosures, including both annual and periodic disclosures, and all requests for approval, will become part of the records of the Board of Directors.

Any waiver of this Code for executive officers (including, where required by applicable laws, our principal executive officer, principal financial officer, principal accounting officer or controller (or persons performing similar functions)) or directors may be authorized only by our Board of Directors or, to the extent permitted by the rules of The NASDAQ Stock Market, a committee of the Board and will be disclosed as required by applicable laws, rules and regulations.

For questions regarding adherence to this Code, you can contact Colleen Kimmel at 248-351-3495.