Bank OZK

Member FDIC

Code of Business

CONDUCT AND ETHICS

Last updated February 24, 2025

TABLE OF CONTENTS

A Message from George Gleason i
The OZK Way i
Introduction 1
General Overview 1
- Who Must Follow the Code 1
- Third Party Code of Conduct 1
- Your Responsibilities 1
- Leading with Integrity – a Message for Supervisors 2
- Violations of the Code 2
- Speak Up! 3
- Amendments and Administration of the Code 3
- Waivers of the Code 3
- Business Unit-Specific Requirements 3
- Access to the Code 3
- Training on Code Content and Certification of Compliance 3
- Seeking Help and Information 3
- Customer Complaints 3

Raising Concerns and Reporting Violations 4
- How to Report Concerns 4
- Our Ethics Helpline and How It Works 4
- If You SEE Something, SAY Something! 5
- Non-Retaliation Policy 5

Code Principles 6
- Avoid Conflicts of Interest 6
- Gifts, Gratuities and Payments 8
- Personal Finances 8
- Political Contributions and Activities 9
- Incentive Policies and Procedures 9
- Fair and Responsible Banking 9
- Anti-Bribery and Anti-Corruption 10
- Interactions and Dealings with Government Employees 10
- Confidentiality and Safeguarding Information 10
- Accurate Records, Filings and Other Regulatory Reporting 13
- Protecting Bank Assets 13
- Trading in Bank Securities 14
- Solicitation or Distribution of Non-Bank Related Materials 14

Our Employees and Work Environment 14
- Workplace Excellence 14
- Harassment and Discrimination 15
- Workplace Violence 15
- Workplace Safety 16

Compliance with Laws and Regulations 16
- Anti-Money Laundering and Financial Crimes 16
- Reporting Unusual Activity 16

Notice to Employees 17

A Message from **George Gleason**

Bank OZK has a reputation for excellence. The Bank expects that you will meet and exceed the excellent standards of work performance and conduct that have allowed the Bank to achieve this respected reputation.

Our Code of Business Conduct and Ethics shows us how to be the most trusted choice for all our stakeholders. It is our shared guide to operating with the highest level of ethics and integrity and a vital part of our risk management strategy. The Code works in conjunction with many of our Bank policies to help you navigate situations and answer questions about what to do in specific circumstances.

Keep in mind that the Code is not intended to be a comprehensive rulebook. Should you find yourself in doubt, it is important for you to ask questions of your supervisor or through one of the resources listed in the Code.

We are all responsible for maintaining the highest possible ethical standards in how we conduct our business and serve customers. After all, our culture is centered on relationships, and those relationships are built on trust.

Thanks for all you do to create and maintain that culture and to serve our clients, communities, and shareholders.

Sincerely,

George Gleason

Chairman and
Chief Executive Officer

THE OZK WAY

The OZK Way reflects the guiding principles that drive our success. These are the standards we expect every Bank OZK team member to strive to achieve:

Better Character

We conduct ourselves and our business with the highest standards of honesty, ethics, integrity and fair dealing.

Better Experiences

We provide exceptional service, develop meaningful products and leverage technology to serve our clients effectively while fostering relationships rooted in trust.

Better^{x}

We relentlessly pursue excellence through continuous innovation and improvement, realizing that many small incremental enhancements can compound mightily over time.

Better Together

We champion teamwork and collaboration, and appreciate that our collective accomplishments lead to exponentially greater results.

Introduction

Bank OZK is committed to the highest standards of ethical and professional conduct. The Code of Business Conduct and Ethics (our "Code" or this "Code") sets forth the guiding principles by which we operate and conduct daily business with shareholders, customers, vendors and all other persons with whom we deal. The Code provides basic guidelines of professional conduct that we expect you to adopt and uphold, and is designed to illustrate the high ethical standards we expect of you. Please read our Code carefully, refer to it when needed, and ask questions when in doubt.

The terms "Bank OZK" and "the Bank" refer to Bank OZK and its affiliates. Unless the context indicates otherwise, the term "employee" or "you" refers to any Bank OZK director, officer or employee.

The use of these terms or issuance of this document does not alter your "at will" employment relationship with the Bank, unless otherwise provided by law or you have a written agreement for continued employment signed by you and an authorized representative of the Bank. We recognize your right to resign at any time for any reason, and we may terminate an employment relationship at any time for any lawful reason. Similarly, the use of these terms or the requirement to read and adhere to this Code does not change the employment status of the employees of the Bank's third parties or contractors.

The Code, as revised from time to time, supersedes and replaces any prior communications, policies, rules, practices, standards, procedures and/or guidelines (whether written or oral) that are less restrictive or to the contrary. If any provision of this Code is less restrictive than your local law, the provisions of your local law apply.

General Overview

Who Must Follow the Code

Our Code applies to anyone who works for or represents the Bank, including our officers, employees and directors.

Our officers, employees and directors are expected to observe the highest standards of ethics, conduct, professionalism, character and personal integrity at all times. You should demonstrate our values daily in each of your interactions. Anyone who violates our Code may face disciplinary action, up to and including termination, and may be subject to other actions available to the Bank pursuant to contracts, laws, regulations or policies.

Our business shall be conducted in compliance with all applicable federal, state and local laws and regulations. This compliance does not comprise our entire ethical responsibility, but instead defines the absolute minimum level of performance.

Third Party Code of Conduct

Certain Bank OZK business relationships, such as those with vendors or suppliers, outside counsel and consultants, serve as extensions of the Bank and, as such, they and their representatives and/or employees are expected to adhere to the spirit of the Code, and to any applicable provisions, when working on behalf of the Bank. The Bank maintains a Third Party Code of Business Conduct and Ethics that reiterates our expectation that our vendors or suppliers, and their employees, adhere to the applicable provisions of our Code and sets forth the ethical business practices we expect them to maintain.

Your Responsibilities

Countless decisions are made every day at our Bank. Each decision we make impacts our customers, employees, shareholders and communities, and our reputation of honesty, integrity, friendliness and excellent customer service has been earned in the eyes of these stakeholders by following the highest standards of ethics and conduct. We expect (and are expected) to deal fairly with all persons at all times. You play an important role in ensuring that we meet those expectations. You are responsible for:

- Following the letter and spirit of all laws and regulations and all Bank policies and procedures, including this Code.
- Dealing fairly with our customers, suppliers, competitors and employees.
- Avoiding actual or perceived conflicts of interest.
- Not taking unfair advantage of any customer, competitor or third party through manipulation, concealment, misuse or abuse of proprietary or confidential information, knowingly false misrepresentation of material facts or any other unfair business practice.
- Protecting our reputation as a trusted and respected financial institution.
- Not giving or accepting bribes, kickbacks, promises or preferential extensions of credit.

- Protecting our customers from unauthorized or inappropriate disclosure of their information and privacy, unlawful discrimination and unfair, deceptive or abusive acts or practices.
- Speaking up promptly to report violations.
- Avoiding favoritism or perceived favoritism by approving or awarding orders, contracts and commitments based on objective business standards.
- Being clear, truthful, fair and transparent in all of your dealings.
- Not conspiring or colluding in any way with our competitors.
- Always conducting our business in a manner that you are willing in good conscience to explain and defend.

You must fully and truthfully cooperate with any investigation or audit, or any regulatory examination or request for information. You should be aware of and comply with applicable practices and procedures regarding contact with regulators, including requirements to report such contact to your supervisor or other personnel. If you are the subject of an external investigation, you must immediately inform your supervisor unless laws, regulations or the investigating authority prohibit you from doing so.

While compliance with this Code is critical, it is not all inclusive and does not attempt to address all potential issues that you may face. Employees in specialized departments like lending, mortgage and trust and wealth, for example, must comply with additional licensing requirements and rules that may be more restrictive than other departments. You are expected to be aware of the particular policy requirements of your position.

While some decisions will have an obvious right result, in many cases the correct outcome is not clear. In all situations, you should:

- Carefully review the relevant facts.
- Identify and analyze applicable laws, rules, regulations and Bank policies.
- Review potential options and their consequences.
- Consider competing interests.
- Uphold our values.

Leading with Integrity - a Message for Supervisors

We hold supervisors to a higher level of accountability for ethical behavior. As a supervisor, you're expected to uphold the spirit and intent of our Code, demonstrate our core values in everything you do and lead with integrity. This means:

- setting an example of ethical behavior;
- emphasizing ethical awareness within your team;
- creating an environment of open communication;
- inviting questions/concerns from your employees without fear of reprisal;
- holding others accountable for acting appropriately;
- avoiding actions that could be seen as an abuse of your position;
- handling all ethics complaints confidentially and in accordance with this Code and other Bank policies and procedures; and
- publicly celebrating examples of ethical behavior.

As a supervisor, you are responsible for taking reasonable steps to ensure that employees under your supervision comply fully with both the letter and the spirit of this Code. Supervisors who fail to take action or who retaliate against employees who report misconduct may be held responsible for their failure to report or take steps to remediate the issue.

Violations of the Code

We are all responsible for living up to the high standards of ethical behavior set out in our Code, and for being accountable in all we do. When one person fails to adhere to our Code, it has the potential to reflect negatively on the entire Bank, and that is why ethical behavior and personal integrity are the core of our culture.

We investigate all alleged violations of our Code. Following the investigation, if necessary, the Bank will take appropriate action to address its findings. Employees who are found to have violated the Code or

any other Bank policy, or fail to cooperate fully with any inquiries or investigations, are subject to discipline, up to and including termination of employment, and may be subject to other actions available to the Bank pursuant to contracts, laws, regulations or policies. Furthermore, any illegal or improper acts committed by employees during their relationship with the Bank may be reported to regulators, which could result in civil or criminal penalties, disqualification from serving in certain capacities, or other consequences.

Speak Up!

Subject to applicable laws and the *Notice to Employees* included in this Code, you must report unethical or illegal conduct promptly including any violation or potential violation of our Code, our policies or applicable laws, rules or regulations — whether the conduct relates to you, other employees of our Bank or one of our third parties. During investigations, we keep the identities of employees who report concerns confidential to the fullest extent possible. We ensure that questions and concerns are handled promptly, discreetly and thoroughly.

Amendments and Administration of the Code

Substantive revisions to the Code are approved by the Board of Directors. Periodic reports regarding violations of the Code will be made to the Audit Committee.

Waivers of the Code

The Board of Directors must approve any waiver of the Code for any executive officer or director. The Bank will promptly disclose any such waiver on our Investor Relations page at ir.ozk.com or through a press release or other public filing as required by applicable law, rule or regulation.

Business Unit - Specific Requirements

Some business units have additional or supplemental guidelines, procedures or other requirements in addition to those specifically discussed in the Code. You are responsible for knowing and abiding by any additional requirements of your business unit.

Access to the Code

Our Code is maintained electronically and is posted on the Bank's internal website, OZK Inside, and the Bank's external investor relations website at ir.ozk.com under "Governance Documents."

Training on Code Content and Certification of Compliance

Everyone employed by the Bank, including officers, is required to complete annual training on the Code through the Bank's online training platform. All employees, officers and directors are required to certify that they have read and understand the Code.

Seeking Help and Information

This Code is not intended to be a comprehensive rulebook and cannot address every situation that you may face. If you need advice or advice would be helpful, you should ask for it. If questions or concerns arise about how this Code or our policies apply, you should discuss them with your supervisor (or higher levels of management) or one of the Bank's Human Resources Business Partners.

The Bank has also established a Confidential Ethics Helpline and web reporting tool that is available 24 hours a day, 7 days a week at 1-844-406-2411 or via the website at ozk.ethicspoint.com ("Ethics Helpline"). You may remain anonymous and will not be required to reveal your identity in calls to the Ethics Helpline or if submitted online, although providing your identity may assist the Bank in addressing your questions or concerns.

If you need clarification about anything in this Code or guidance about a situation you're experiencing, or if you need to report a concern, you may start with your supervisor, but you don't have to if you're not comfortable doing so. Feel free to contact your Human Resources Business Partner, higher levels of management, the Ethics Helpline or any of the resources listed in this Code. You also may raise your concerns in writing to the chair of the Audit Committee of the Board of Directors.

If there appears to be a conflict between this Code, other Bank policies, and/ or any agreements, laws or regulations, you should contact the Office of General Counsel; however, as a general matter the more restrictive requirement will prevail.

Customer Complaints

Remember that customer complaints must be entered in the Bank's Customer Complaint System ("CCS") located on the OZK Inside homepage. ALL employees have access to and a responsibility to enter customer complaints into the Bank's CCS. If you receive a customer complaint, it should be entered into the CCS immediately. The *Complaint Management Policy* and *Complaint Management Program* provide additional information and guidance around reporting customer complaints, including examples of complaints.

RAISING CONCERNS AND REPORTING VIOLATIONS

We have a responsibility to protect the reputation and integrity of our employees, stakeholders and shareholders. We take all reports of misconduct seriously.

How to Report Concerns

Employees have a responsibility to promptly report knowledge of or information regarding any violation or suspected violation of the law, any provision of the Code or other Bank policies or procedures. If you see or suspect illegal or unethical behavior involving the Bank, including possible violations of this Code, or violations of laws, rules or regulations—whether it relates to you, your supervisor, a coworker, a customer or a third-party service provider—you have several ways you can report:

- Bank OZK's Ethics Helpline (1-844-406-2411) or via the EthicsPoint Website at ozk.ethicspoint.com.
- Contact your Human Resources Business Partner or report complaints by mail (anonymously or otherwise) by sending the notice to: Bank OZK Human Resources Department, Attention: Chief Human Resources Officer, P.O. Box 8811, Little Rock, Arkansas 72231-8811.
- To report a concern regarding accounting, internal accounting controls, or auditing matters, you can use the Ethics Helpline or report a concern directly to the Audit Committee of the Board of Directors. To report such matters directly to the Audit Committee, send the notice to Bank OZK Audit Committee Chair, c/o General Counsel and Corporate Secretary, P.O. Box 8811, Little Rock AR 72231.

We are committed to investigating potential violations and dealing with each report fairly and reasonably.

Our Ethics Helpline and How It Works

You may contact the Ethics Helpline 24 hours a day, 7 days a week, either:

- By telephone at 1-844-406-2411; or
- Through the EthicsPoint Website, ozk.ethicspoint.com, which is our Web Reporting tool.

The Ethics Helpline call center is staffed by third-party interview specialists. You may choose to remain anonymous.

When you contact the Ethics Helpline, the interview specialist will listen, ask clarifying questions if necessary, and then write a summary report of the call. The summary will then be provided to the Bank for assessment and appropriate action.

When you contact the Ethics Helpline, it is important to provide as many details as possible (e.g., who, what, when, where). Because the Bank may need some additional information, you will be assigned a report number and asked to call back at a later date to answer any follow-up questions.

ETHICS HELPLINE

24 hours a day / 7 days a week

EthicsPoint
A Confidential Reporting Resource

CALL
1-844-406-2411

WEB
ozk.ethicspoint.com

The Ethics Helpline call center is staffed by third-party interview specialists. You may choose to remain anonymous.

Any information provided to the Ethics Helpline will be treated as confidential to the fullest extent possible. In some instances, during the course of investigations, information may be shared on a need to know basis. Under some circumstances, the Bank may be required to report certain types of suspicious activity and other activities that may potentially violate criminal laws.

If You SEE Something, SAY Something!

Your most important responsibility as a Bank OZK employee is to make sure that you, and that we as a Bank, adhere to the highest standards of character, ethics, integrity and fair dealing.

Spot something that looks fishy or seems "off"? Bank OZK has multiple channels for you to report unusual activity, including confidential reporting. Every team member has a responsibility to report unusual customer activity and employee activity that appears to be unethical or suspicious. Don't assume someone has already reported it. **If YOU see something, YOU should report it.**

Non-Retaliation Policy

Bank OZK prohibits retaliation of any kind for good faith reports of alleged ethical violations or misconduct of others. Retaliatory conduct includes termination, demotion, suspension, threats, harassment, and any other manner of discrimination in the terms and conditions of employment as a result of any lawful act you may have performed in connection with such reporting.

Supervisors are held accountable for the retaliatory behavior of employees under their supervision. Employees who engage in retaliation against a colleague who has raised a concern in good faith and in accordance with this Code are subject to disciplinary action, up to and including termination of employment or other relationship with the Bank. You should report any incident of retaliation using one of the methods described above. All reports of retaliation shall be investigated and, if appropriate, prompt, effective remedial action shall be taken. For more information, refer to the Bank's *Whistleblower Policy* available on PolicyTech.

CODE PRINCIPLES

Avoid Conflicts of Interest

We face actual, potential and perceived conflicts of interest on a regular basis during the normal course of business. The Code provides basic guidelines of ethical business practices, management of conflicts of interest, and conduct that we are expected to adopt and uphold as Bank employees or as individuals performing duties and assignments on behalf of the Bank through third party relationships.

For purposes of this Code, "family member" includes a spouse or domestic partner, child (including by adoption), parent, grandparent, grandchild, sibling, parent-in-law, brother-in-law or sister-in-law of you or your spouse or domestic partner, and step relationships of the foregoing.

You are expected to be conscientious in avoiding any action or interest that conflicts, or gives the appearance of conflicting, with our interests or which could make it difficult to objectively and effectively perform your work. Conflicts of interest are prohibited as a matter of Bank policy.

A conflict of interest exists when you (or one of your family members) have a personal or professional interest that is (or appears to be) at odds with the best interests of the Bank. Conflicts of interest may occur when:

- personal business or financial interests or activities compete or interfere (or appear to compete or interfere) with your obligations to the Bank or our shareholders or customers;
- the interests of two or more of our customers conflict, which could potentially damage the interest of one or both of the customers;
- the Bank's interests conflict with those of our customers; or
- you or your family members receive improper personal benefits, products, services or preferential treatment as a result of your position with the Bank.

You are responsible for identifying and managing actual, potential or perceived conflicts in accordance with applicable laws and regulations and our policies, including this Code. It is impossible to define every action that could reasonably be interpreted as a conflict of interest. This section of our Code identifies guidelines with respect to certain specific potential conflicts of which you should be aware.

Relationships with Customers

If you or one of your family members has any financial interest in any transaction with the Bank, you must immediately fully disclose the nature of such interest to the Bank employees involved with the transaction. This requirement does not apply to: (i) routine deposit account relationships on terms equivalent to those offered generally; (ii) lending relationships which shall be handled by an unrelated lending officer not subordinate to you; (iii) trust relationships which shall be disclosed to the Trust Committee; (iv) ownership of minority interests solely as an investor in publicly held companies; and (v) interests in a governmental entity solely through ownership of government or municipal bonds.

Involvement in Transactions

You must refrain from personally handling any Bank transactions for yourself, family members, affiliates or related business associates, including any accounts of the foregoing or any other accounts in which you have a personal interest or on which you are an authorized signer, without the prior approval of the Chief Executive Officer, President or Chief Operating Officer. Such transactions include, without limitation, opening accounts of any type, cashing checks, accepting deposits, making or approving loans, accepting loan payments, approving overdrafts, accepting checks on uncollected funds, waiving insufficient, overdraft or late charges, waiving the requirement for financial statements, collateral documents or other supporting documents or approving or processing any other type of transaction.

Loans

You may not personally borrow money from or lend money to any party with whom the Bank deals, except a loan to you from another financial institution on customary terms and where there is no conflict of interest. An occasional loan of nominal value (such as for lunch) to another employee or acquaintance is acceptable, as long as no interest is charged.

Fiduciaries

You may not serve personally as executor, trustee or guardian of a customer's estate or trust, or accept any legacy or bequest therefrom, without the prior written approval of the Chief Executive Officer, President or

Chief Operating Officer, unless the customer and you are related. In any appointment, the family relationship (and not your position with the Bank) must be the foundation for the appointment, the relationship must not arise from or have its basis in the business activities of the Bank, and any such appointment shall be of you in your personal capacity, and not the Bank. In the event that any exception to this policy is approved, such approval shall not imply, and you shall not represent, that you are serving at the direction or request of the Bank.

Investment Officers

If you serve as an investment officer, you must exercise extreme caution when trading securities for your own or related accounts through dealers from which you trade securities for the Bank's account. In every transaction, it should be clearly understood by all parties, including the dealer, from the inception of such transaction whether the transaction is for the Bank's account or your personal or related account. You shall never utilize your position with the Bank to carry out a transaction on terms more favorable than those which you could have obtained apart from your position with the Bank.

Directorships

You must obtain the approval of the Chief Executive Officer before accepting any appointment or election to a board of directors or officer position of any privately-held or publicly-traded company or financial institution (other than governmental, charitable, educational, religious or other non-profit organizations). The Chief Executive Officer will evaluate whether such position might interfere with your loyalty to, or performance of your duties with, the Bank.

Outside Employment

Outside activities by you should not compromise the interests of the Bank. Outside employment must be approved by your supervisor and the head of your business unit. Keep in mind that we engage in a broad variety of business activities, so other businesses or organizations may be either a customer or considered to be competing with the Bank even if they do not directly compete with your particular business activities.

Gambling

You shall not gamble on or with Bank property.

Corporate Opportunities

You may not (i) personally take for yourself opportunities that properly belong to the Bank or are discovered through the use of Bank property, information or position or through access to Bank facilities, (ii) use Bank property, information or position for your personal gain, (iii) directly or indirectly compete with the Bank or (iv) take for yourself an opportunity that belongs to the Bank, or help others do so, if they are in a position to divert a corporate opportunity for their own benefit.

You owe a duty to the Bank to advance the Bank's legitimate interests when the opportunity to do so arises. You shall exclusively promote the purchase and sale of products or services offered by the Bank.

When an apparent or possible conflict of interest arises, you should promptly report the matter to any Human Resources Business Partner (or, if you are a director, to the Chairman and/or the Chair of the Governance and Compensation Committee) for a determination on how to proceed.

Gifts, Gratuities and Payments

Internal Gifts

A conflict of interest may also arise when you provide or receive gifts to or from other employees, especially if such gifts are exchanged among employees in the same business unit or in positions of influence. You may not give or receive gifts to or from another employee that may create a real or perceived conflict of interest. Gifts may also not be used as a form of compensation or reward for job performance, other than awards given as part of approved Bank-sponsored recognition programs or other internal incentive initiatives provided by the Bank. (Note that you may provide gifts in connection with life events (e.g., weddings, birthdays, births, etc.) where the circumstances make it clear that it is the life event, rather than an employment relationship, that is the motivating factor for the gift.) Under all circumstances, you must exercise good judgment to ensure that any gift is reasonable for the occasion, is not lavish or frequent, does not create any appearance of impropriety, and could not be perceived to be compensation.

External Gifts

You are legally prohibited from (1) soliciting or offering anything of value in return for any business, service or confidential information of the Bank and (2) accepting or offering anything of value (other than bona fide compensation from the Bank) from or to anyone in connection with business of the Bank, either before or after a transaction is discussed or consummated. The policy of the Bank is to comply strictly with laws and regulations governing these types of gifts.

Notwithstanding the above, you may accept or give something of nominal value to or from someone doing or seeking to do business with the Bank as long as it does not impair your ability to make an objective decision or compromise your undivided loyalty to the Bank.[1] Examples include:

- acceptance of meals, tickets and accommodations in the course of a business meeting or other occasion;
- special occasion gifts from customers;
- acceptance of advertising or promotional material; and
- awards from charitable organizations.

[1] "Nominal" value means "within your ability to reciprocate on a personal basis" and would usually include any gift, meal or award which has a fair market value of not more than $250.

Specifically, such gifts may not be solicited, must be given on an occasion when gifts are customary, may not be in cash or cash equivalents, must not be frequently offered to or given by the same source, and must not involve any government officials or labor unions.

You may accept meals, tickets and accommodations in the course of and incidental to a business meeting or other occasion for a business purpose, provided the expense would be paid or reimbursed by the Bank consistent with our own expense reimbursement policy, if not paid by the other party.

If, after reviewing this section, you are uncertain whether a potential gift is in compliance with the Code, you should seek guidance from the Chief Executive Officer, President or Chief Operating Officer, who will evaluate whether such gift would impair your ability to make an objective decision or compromise your undivided loyalty to the Bank.

Personal Finances

Because of the nature of our business, you should manage your personal financial matters prudently. Not doing so could undermine your professional credibility and jeopardize your employment.

- Misuse of Bank accounts and products is prohibited. The following are examples of misuse (and in many cases are illegal): fraud, dishonesty, kiting, making false ATM deposits, and viewing employee account information for non-business reasons. We reserve the right to monitor all account activity, subject to applicable law.
- You must follow guidelines for incurring business-related expenses and comply with expense reimbursement procedures. Bank credit cards may be used for business-related expenses only. These

expenses must be submitted to Accounts Payable in full when due. Expense reports must be submitted in a timely manner. If your employment ends, any outstanding expenses on Bank credit cards must be resolved immediately.

- You may not mishandle account transactions in violation of Bank policies, procedures and guidelines. Examples include: misappropriating funds; opening, closing or altering accounts without proper authorization; transferring funds without proper authorization; or performing any transaction that does not comply with our policies and procedures.

Political Contributions and Activities

We encourage you to participate in political activities on your own time, at your own expense, and in accordance with your individual desires and political preferences. In general, you may make personal political contributions, within applicable legal limits, to candidates, parties, committees, and other entities that make political expenditures. Due to industry regulations and applicable laws, employees of particular businesses or having certain responsibilities may be restricted from making some political contributions or engaging in certain political activities. No political contributions will be made at any time with Bank funds, directly or indirectly, except as permitted by law and with the prior written consent of the Chief Executive Officer. No individual contributions will be reimbursed by salary, bonus, expense account or in any other manner. As an employee, it must be clear at all times that any political contribution or participation by you is done as an individual and not as a representative of the Bank.

Under no circumstances may you coerce or pressure other employees, customers, or vendors to make political contributions. You may not engage in political fundraising or solicitation activities for your own political interests (i) on Bank premises, (ii) from customers or vendors of the Bank, or (iii) from other employees during work hours.

The Bank supports the desire of any employee to serve the public in elected or appointed office. Because the election process is time consuming, if you plan to seek public office, you must first obtain the permission of your supervisor and the written consent of the Chief Executive Officer, after discussing with those persons the performance of your duties as a Bank employee and appropriate steps to avoid conflicts or perceptions of conflicts of interest.

Bank resources are not to be used in any way in connection with an employee's campaign for or service as a public official. Employees who seek or hold elected or appointed office must comply with state and federal election laws and, if the performance of official duties or running for public office conflicts with the performance of normal Bank duties during regular business hours, employees must comply with all time off and leave policies of the Bank.

Incentive Policies and Procedures

The intent of our incentive programs is to justly reward high-performing sales, service and support team members. You may not directly or indirectly manipulate records, open bogus accounts, create sham products, falsify applications or skew results in any way for the benefit of yourself or other employees. Vendors and third parties are also prohibited from doing this in support of the Bank, our customers or potential customers. All incentive programs and related activities shall be conducted in accordance with our policies and procedures. Anyone who manipulates or attempts to manipulate incentive results or circumvents or attempts to circumvent our policies and procedures related to incentive programs will be subject to appropriate disciplinary action, up to and including termination of employment.

Fair and Responsible Banking

Unfair, Deceptive and Abusive Acts or Practices

We are committed to treating prospective and existing customers in a manner that is equitable, transparent and consistent with laws and regulations, including consumer protection laws and regulations that prohibit unfair, deceptive or abusive acts or practices.

Discrimination in Banking

We prohibit discrimination in banking on the basis of race, color, religion, sex, marital status, familial status (including pregnancy and parental leave), national origin, sexual orientation, gender identity, age, disability or handicap, military and veteran status or any other protected status under federal, state or local law, the fact that all or part of a customer's income is derived from any public assistance program, the fact that a customer has in good faith exercised any of his or her rights under the Consumer Credit Protection Act and on any other basis prohibited by law. Our commitment to fair and responsible banking is a basic responsibility of all employees.

Anti-Bribery and Anti-Corruption

You are expected to comply with the U.S. Foreign Corrupt Practices Act and all other applicable anti-bribery and anti-corruption laws whenever and wherever you conduct business on behalf of the Bank. You may not give, promise or offer money or anything of value, or authorize any third party working on behalf of the Bank to give, promise or offer anything of value, including but not limited to currency, offers of employment, and lavish gifts and entertainment to any customer, government employee or any other person for the purpose of improperly influencing a decision, securing an advantage, avoiding a disadvantage or obtaining or retaining business; provided, that gifts may be given or received in strict compliance with the *"Gifts, Gratuities and Payments"* and *"Interactions and Dealings with Government Employees"* sections of this Code. If you engage in such prohibited behavior, you expose yourself and the Bank to potential civil and/or criminal liability and significant reputational harm, and undermine the trust of our customers, shareholders and communities.

Interactions and Dealings with Government Employees

Our interactions with government entities and their employees may expose us and our employees to a wide range of policy, legal and compliance concerns. Prior to communicating with a governmental entity, you must comply with any limitations or requirements that apply to your contact (e.g., limits on gifts and entertainment, requirement to register as a lobbyist). If you are not sure whether any such limitations or requirements apply, you should contact your supervisor or a member of management.

You are expected to be particularly conscious when interacting with government employees and must not engage in behavior that could be viewed as an attempt to improperly influence a business relationship. You must be sensitive to situations or circumstances that could create an appearance of impropriety or potential conflict of interest, or raise bribery or corruption concerns.

You must not offer, give or promise to give money or anything of value to any executive, official or employee of any government, agency, state-owned or controlled enterprise, political party or candidate for political office if it could be seen as being intended to influence a business relationship of the Bank.

Nothing in this section, or any other section of our Code or policies, is intended to prohibit you from filing a complaint with governmental agencies such as the Securities and Exchange Commission, the Financial Industry Regulatory Authority, Inc., the National Labor Relations Board, the Occupational Safety and Health Administration, or similar regulatory entities. Refer to the *Notice to Employees* on the last page of this Code for further guidance.

Confidentiality and Safeguarding Information

In order to remain competitive, the Bank must protect the confidentiality of its proprietary information. Therefore, dissemination or disclosure of the Bank's sales reports, business plans, costs for goods, marketing strategies, profits, internal databases containing information regarding customers, computer software and programming, and/or pricing information is strictly prohibited.

The term "confidential information" means, without limitation, trade secrets, proprietary and legally protected information regarding the Bank, its customers, and third parties, including: financial performance (if not yet publicly announced); vendor pricing and contracts; Bank products, services, and pricing and research and development projects; patents and other intellectual property, including inventions related to any of the Bank's business units; information regarding security and security system protocols; technology systems platforms, plans and information; secure data centers or other property information; individual system ID's, passwords, computer programs and platforms for which you may have access; strategic business plans that have not been made known to the public; strategic marketing plans, strategies, and costs; and knowledge of the Bank's potential merger and acquisition activities and considered divestitures.

We expect you to comply with the following confidentiality requirements and to otherwise protect confidential information at least as securely as you would your own personal information; your role in privacy protection is critical.

We are proud of our good reputation. Any unauthorized disclosure of confidential information or unauthorized access to confidential information may damage our customers' trust in the Bank and could be detrimental to the Bank,

potentially resulting in loss of business or new business opportunities and (in some circumstances) legal action against the Bank.

Except as permitted by applicable Bank policies, and subject to the *Notice to Employees* in this Code, you must keep the following information confidential and secure:

Customer Information

You must not access customer information or use customer information except for appropriate business purposes and must protect the confidentiality and security of customer information. You should be familiar with, and handle customer information in accordance with, the Bank's privacy notices, which detail our commitment to privacy and information protection, and internal privacy and information security policies and standards. For more information, please visit PolicyTech (accessible via OZK Inside) and review the *Acceptable Use Standard* and the *Corporate Information Security Policy.*

Supervisory Information Received from Regulatory Authorities

Supervisory information received from our regulatory authorities must be treated as confidential. Depending on the agency, such material may be deemed government property that the Bank is not authorized to share or disseminate without express written consent. Information received from regulatory authorities should be kept secure and not disseminated outside of the Bank without proper authorization. Such information should only be shared within the Bank with other employees who "need to know" the information. Consult with the General Counsel if you have questions about these restrictions.

Bank OZK Information

Subject to the *Notice to Employees* in this Code, you must keep secure and not disclose confidential information about the Bank such as business plans, market conditions and third party information. Such confidential information used in the course of your job duties is intended solely for use within the Bank and is limited to persons with a business need to have access to and know such information, to the extent commensurate with their respective positions. Consult your supervisor if you have questions about sharing information about the Bank on a "need to know" basis. Employee records are considered confidential information and should be disclosed only to authorized persons or in accordance with legal process.

All information used, collected, created or generated by you in your capacity as an employee of the Bank, including all digital records originating from the use of email, the Internet, and Bank computers or technology by you while at work or originated by you in the course of your duties, are considered Bank records and may be transmitted only to individuals who have a business need to receive them. Such information is to be used solely for the Bank's purposes and never for personal gain and may not be used to compete with the Bank.

These duties of confidentiality continue even after your employment with the Bank has ceased. If you leave the Bank for any reason, you may not disclose or use any confidential information in a manner that is harmful to the Bank or useful to competitors, or for your own or another's gain, or keep any originals or copies (in electronic or any other form) of journals, lists, manuals, notebooks, drawings, notes, reports, proposals, other documents, technology, credentials, tokens, materials,

tools, or equipment or property belonging to the Bank. Bank records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other legal process and shall only be disclosed at the direction of the General Counsel. Requests for the production of information through subpoena or other legal means shall not be disclosed either to the customer or other party about whom confidential information is sought or to any other person, except as allowed by written policy of the Bank or required by law.

Mergers and Acquisitions and Other Confidential Transactions

Some employees and directors ("Transaction Employees") may from time to time have access to certain nonpublic information ("Transaction Information") regarding potential confidential transactions that we are considering, evaluating or pursuing ("Potential Transactions"). Potential Transactions might include, for example, the acquisition of a bank or other financial services company, the sale or purchase of branch facilities, the sale or purchase of financial assets or liabilities, the issuance or repurchase of stock, or the issuance or retirement of debt. Transaction Information includes any and all nonpublic information and materials pertaining to a Potential Transaction, all analyses, compilations, forecasts, studies or other documents prepared by us or our representatives in connection with the Potential Transaction, the identities of any parties to the Potential Transaction, and the fact that we are considering or are engaged in discussions with any other party regarding the Potential Transaction.

In addition to the general obligations of all employees to protect confidential information, each Transaction Employee has a special duty to hold in confidence, protect and safeguard Transaction Information in accordance with our policies and procedures and not to use or disclose Transaction Information except as required to perform his or her responsibilities in connection with the Potential Transaction, to comply with applicable law or regulation, or as otherwise directed or permitted by his or her supervisor. Each Transaction Employee also should be aware that any Potential Transaction is likely subject to a confidentiality or nondisclosure agreement between us and the other party(ies) to the Potential Transaction ("Potential Transaction NDA"). Supervisors of Transaction Employees who receive Transaction Information that may be subject to a Potential Transaction NDA are responsible for apprising such Transaction Employees of the terms of the Potential Transaction NDA.

Business Communications

Email messages you send outside the Bank via public networks may be intercepted or misdirected. You must take great care not to include information that may be egregiously offensive, constitute unlawful discrimination or harassment, or knowingly false. Be mindful and follow our *Social Media Policy and Guidelines.*

Use our SecureMail Encryption product when you must send confidential or customer information to external parties via email. For more information on how to access and use the SecureMail Encryption product, please refer to the *Secure Email Guideline* on PolicyTech.

If a customer emails a service request that contains personal information or account numbers, remove this information from your email reply. This will reduce the risk of exposing this information.

Third Party Information

You must keep confidential and secure any information about the Bank's purchase of products or services, including the existence and nature of any of our third party relationships. Sharing this information with the wrong source could provide an improper advantage to the third party or its competitors and may violate our agreements with third parties.

Information regarding our third party relationships may only be used by you in good faith support of your assigned duties and responsibilities on behalf of the Bank, and may not be used in violation of any provision of this Code, legal or regulatory requirements, or our policies and procedures.

Intellectual Property of Others

We respect the intellectual property rights of others. Employees must not obtain or use the intellectual property of others in violation of confidentiality obligations or law. The use, sale or other distribution of intellectual property in violation of license agreements or intellectual property laws is prohibited.

Accurate Records, Filings and Other Regulatory Reporting

Records and Filings

As a publicly traded company and state bank, we make filings with the FDIC, the Arkansas State Bank Department and other regulators of the Bank. Our disclosures must be full, fair, accurate, timely and understandable. We have strict disclosure controls and procedures and stringent internal controls over financial reporting. You may be called upon to provide necessary information to assure that the Bank's filings and reports are complete, accurate and understandable. If you are involved in preparing our public disclosures, you have a special responsibility to help us meet these standards. The Bank expects you to take this responsibility seriously and to provide complete and accurate answers to inquiries related to the Bank's regulatory reporting requirements.

Each one of us is responsible for ensuring the information we record, process, analyze and disclose is:

- Complete, accurate and recorded in a timely manner.
- Handled according to applicable accounting standards, legal requirements and internal controls.
- Corrected immediately if errors occur.

This information includes accounting and audit records, loan documents, phone records, transaction records, ATM and teller balancing, expense reports, and all other records that are part of our day-to-day business. You also must follow notary requirements.

All employees must maintain and adhere to these controls so that all underlying transactions, both within the Bank and with third parties, are properly documented, recorded and reported.

Reporting Accounting Concerns

In addition, we all have the responsibility to promote full, fair, accurate, timely and understandable disclosure in reports and documents that the Bank files with or submits to regulators. The Audit Committee has established procedures for the receipt, retention and treatment of complaints regarding accounting, internal accounting controls or auditing matters. If you have unresolved concerns or complaints regarding questionable accounting or auditing, you may report such concerns or complaints anonymously through the Ethics Helpline or any of the other available procedures described in the *"How to Report Concerns"* section of this Code. You will not be retaliated against for reporting information in good faith in accordance with this requirement.

Accurate Records and Retention

Accurate record keeping and reporting reflects on our reputation, our integrity and our credibility, each of which promotes the interests of the Bank and our shareholders. You must maintain accurate books and records consistent with business needs and legal requirements. Misrepresenting facts or falsifying records shall not be tolerated. All records, including email and Internet records, shall be retained or destroyed according to the Bank's record retention policies. See the *Record Retention Schedule* on PolicyTech for more information.

Protecting Bank Assets

You must properly care for and protect, and ensure the efficient use of, Bank property and assets, which should be used for legitimate business purposes only. Examples of Bank assets include (but are not limited to) computer software, databases, files, intellectual property, technology and innovations, data processing systems, the Bank's computer systems (including your email and Internet access and usage), records, supplies, customer lists or information, information about corporate or customer transactions, money and funds, equipment, furnishings, reports, and ideas.

You may not:

- Steal, embezzle or misappropriate money, funds or anything else of value from the Bank.
- Use Bank assets for personal gain or advantage.
- Remove Bank assets from Bank facilities unless you first receive your supervisor's approval.
- Use official Bank stationary, the corporate brand, documents or the Bank name for commercial gain.
- Misuse your Internet, phone or email privileges.

The Bank may monitor and inspect your use of these resources to protect productivity, maintain the integrity of information systems, and prevent activities that may create exposure for the Bank. As a result, you should have no expectation of privacy when using these privileges.

Proper use of Bank property, electronic communication systems, information resources, materials, facilities and equipment is your responsibility. Occasional personal use, if any, shall be strictly in accordance with Bank policy, including, without limitation, the *Corporate Information Security Policy* and related procedures and standards on PolicyTech.

Trading in Bank Securities

You may not buy, sell, recommend or trade in Bank securities – either personally or on someone else's behalf – while in possession of material nonpublic information relating to the Bank, except through personal trading programs pre-approved by our legal staff. You also may not communicate or disclose any material nonpublic information to others who may trade in Bank securities (including family members); doing so may not only be a violation of your duty to keep such information confidential, but may also violate federal and state laws.

You are subject to additional restrictions on trading in Bank securities that can be found in the *Insider Trading Policy* located on PolicyTech.

Solicitation or Distribution of Non-Bank Related Materials

It is the policy of the Bank to prohibit solicitation and/or distribution of non-Bank commercial marketing material on its premises or through corporate email or internal mail. The Bank prohibits solicitation and distribution of non-Bank commercial marketing material on its premises because, when left unrestricted, such activities can interfere with the normal operations of the Bank, can be detrimental to efficiency, can be annoying, and can pose a threat to security.

Persons who are not employed by the Bank are prohibited from offering specials, "deals or discounts", soliciting signatures, conducting membership drives, posting or distributing literature or gifts, offering to sell merchandise or services (except by representative of suppliers properly identified), or engaging in any other solicitation, distribution, or similar activity on Bank premises.

Additionally, the Bank maintains OZK Inside as an internal intranet to communicate Bank information to employees and bulletin boards in each banking office to post notices required by law. Any unauthorized posting of notices, photographs, or other printed or written materials in violation of this policy on bulletin boards or any other Bank property is prohibited.

OUR EMPLOYEES AND WORK ENVIRONMENT

We strive to provide a safe and healthy work environment for all employees. We expect you to follow all Bank policies and practices designed to maintain a safe and productive work environment. It is your responsibility to know and adhere to these policies, including the following:

Workplace Excellence

We are committed to creating and maintaining a productive and team-oriented work environment where individual contributions are recognized, welcomed, and valued. We strive to create a culture that promotes dignity, courtesy, and respect for all. These commitments, reinforced by our shared values, are embedded in the day-to-day working practices with employees, customers and business partners. For more information, see our Workplace Excellence Policy available on PolicyTech.

Harassment and Discrimination

Our *Freedom from Harassment and Discrimination Policy* prohibits unlawful discrimination and harassment of any type and affirms the Bank's commitment to afford equal employment opportunity to employees and applicants without regard to race, color, national origin, religion, sex (including gender, pregnancy, sexual orientation or gender identity), age, disability, genetic information, veteran status or any other protected status under federal, state or local law. Violations of this policy will not be tolerated. The Bank will promptly and thoroughly investigate every issue brought to its attention and will take appropriate disciplinary action, up to and including termination of employment. Furthermore, the Bank prohibits retaliation against any individual who in good faith files a charge of discrimination or reports harassment internally or externally, or who assists, testifies in an investigation of harassment or discrimination, or opposes a discriminatory or harassing practice or conduct in the workplace.

We do not tolerate harassment or discrimination by anyone in the workplace or at any work-related activity or event, including other employees, independent contractors, temporary workers, applicants, visitors, vendors, suppliers, and customers. We consider such behavior unacceptable and contrary to the Bank's core values.

Discrimination generally means treating differently or denying or granting a benefit to an individual because of the individual's actual or perceived protected characteristic. Harassment generally means unwelcome verbal, visual or physical conduct that denigrates or shows hostility or aversion towards an individual based on or because of any actual or perceived protected characteristic or has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment. For more information, review the *Freedom from Harassment and Discrimination Policy* available on PolicyTech.

Every supervisor has a responsibility to keep the workplace free of any form of unlawful harassment (including sexual harassment), discrimination, and retaliation. Supervisors are required to report any complaints of violations of our *Freedom from Harassment and Discrimination Policy* no later than the next business day so that a prompt internal investigation may occur. Disciplinary action will be taken against supervisors who knowingly allow such behavior to continue.

It is every employee's responsibility to ensure their conduct does not include or imply harassment, discrimination and/or retaliation in any form. Any individuals who feel they have become aware of, observe, or who have been subjected to any form of harassment, discrimination and/or retaliation by a supervisor, employee, intern, or non-employee through their actions or words has a responsibility to report or make a complaint about the situation immediately or as soon as practicable by using any of the options provided in this Code or in the *Freedom from Harassment and Discrimination Policy*.

Reported incidents of this type of behavior and/or retaliation will be investigated. Investigations are conducted in as discreet a manner as is compatible with a thorough investigation of the complaint. If the Bank finds that a violation of the *Freedom from Harassment and Discrimination Policy* or other inappropriate conduct of a harassing, discriminatory or retaliatory nature has occurred, disciplinary action up to and including immediate termination of employment may result.

Workplace Violence

We do not tolerate violence in the workplace and seek to prevent violent incidents from occurring. Examples of violence include, but are not limited to, physically harming another, verbally assaulting, shoving, pushing, harassment, intimidation, coercion, brandishing a weapon and threats or talk of violence. You must immediately report any incident that may involve a violation of this policy to the Corporate Security Department, Branch or Facilities Management. For more information, see the *Workplace Violence Policy* available on PolicyTech.

Workplace Safety

We are committed to the safety and security of our employees. You are expected to follow all applicable laws and regulations and safety and security procedures and to practice good safety habits. You should report violations of our safety and security procedures or unsafe working conditions to your supervisor, Corporate Security or one of our Human Resources Business Partners.

COMPLIANCE WITH LAWS AND REGULATIONS

The banking industry is highly regulated and the Bank is subject to numerous laws, rules and regulations in a variety of state and federal jurisdictions. We are regulated by the Arkansas State Bank Department, the FDIC, and the Consumer Financial Protection Bureau. The Securities and Exchange Commission, Nasdaq, and other regulators also supervise us.

You must abide by the laws and regulations and policies impacting the banking industry, as well as other federal and state laws and regulations such as employment laws, antitrust laws, insider trading laws and criminal laws governing fraud, anti-corruption, bribery, embezzlement, and conflicts of interest.

While the Bank does not expect all employees to understand every detail of these technical and complex banking regulations, laws and rules, you are expected to be knowledgeable about and comply with the letter and spirit of the laws, regulations and rules that affect and apply to your specific job and should seek guidance when issues or questions arise. This requires that you avoid not only actual misconduct but also the appearance of impropriety.

Bank policies and procedures involving laws, rules and regulations and additional information are posted on PolicyTech. However, these policies and procedures do not constitute a complete listing of the laws, rules and regulations that must be adhered to by every individual subject to this Code in the conduct of his or her duties at the Bank.

Anti-Money Laundering and Financial Crimes

Money laundering is the process of converting the proceeds of criminal activity into what appears to be legitimate funds. Money laundering generally involves 3 steps - placement of cash or other assets into the banking systems; moving this cash or the assets around multiple accounts or financial institutions (often referred to as "layering"); and the blending of the assets back into the mainstream economy. To protect the Bank and combat money laundering, terrorist financing or other criminal activity, it is important that we comply with the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) laws, regulations and guidance. To do this, you must be able to identify and escalate potentially unusual or suspicious transactions or situations.

Reporting Unusual Activity

If you see something, say something. All employees have obligations to monitor and timely report potentially unusual activity by completing and submitting an Unusual Incident Report ("UIR") through OZK Inside.

If an employee receives or becomes aware of a customer complaint which suggests fraud may have taken place, or has reason to believe that fraud may have taken place, the employee should complete and submit a UIR through OZK Inside.

Examples of situations in which a UIR should be immediately submitted include, but are not limited to:

- Customer behavior that is out of the norm, suspected money laundering, loan fraud, check fraud, or elder financial exploitation;
- Potentially unusual and/or suspicious activity after the employee becomes aware of the activity;
- Alleged fraud or theft on a customer's account;
- Unusual activity by a coworker which may suggest they are involved in a fraudulent transaction or cooperating with a customer to commit fraud;
- Potentially suspicious criminal activity that may be detected through direct dealing with a customer; and
- Potentially suspicious criminal or fraudulent activity by another employee.

When you file a UIR, our systems prefill your contact information. If you prefer to remain anonymous, you may report the activity through the Ethics Helpline.

Each employee is responsible for compliance with the *Bank Secrecy Act Policy*, the *BSA-AML Compliance Program*, and other applicable BSA/AML procedures for their business.

Employees should never disclose to a customer or other party that the Bank has filed or is contemplating filing a Suspicious Activity Report.

Notice to Employees

Nothing in this Code prohibits or limits any employee or their counsel from initiating communications directly with, responding to any inquiry from, volunteering information to, or providing testimony before, the Securities and Exchange Commission, the Department of Justice, Financial Industry Regulatory Authority, Inc., the National Labor Relations Board, the Equal Employment Opportunity Commission, any other self-regulatory organization or any other governmental, law enforcement, or regulatory authority, in connection with any reporting of, investigation into, or proceeding regarding suspected violations of law, and no employee is required to advise or seek permission from the Bank before engaging in any such activity. In connection with any such activity permitted above, employees should identify any information that is confidential and ask the government agency for confidential treatment of such information. Additionally, nothing in this Code prohibits or restricts any employee from exercising any employee rights under the National Labor Relations Act (NLRA), including rights under Section 7 of the NLRA, such as the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, or any other activities protected by the NLRA. Despite the foregoing, employees are not permitted to reveal to any third party, including any governmental, law enforcement, or regulatory authority, information employee came to learn during the course of employee's employment with the Bank that is protected from disclosure by any applicable privilege, including but not limited to the attorney-client privilege, attorney work product doctrine and/or other applicable legal privileges. The Bank does not waive any applicable privileges or the right to continue to protect its privileged attorney-client information, attorney work product, and other privileged information. Additionally, employees recognize that employee's ability to disclose information may be limited or prohibited by applicable law and the Bank does not consent to disclosures that would violate applicable law. Such applicable laws include, without limitation, laws and regulations restricting disclosure of confidential supervisory information or disclosures subject to the Bank Secrecy Act (31 U.S.C. §§ 5311-5330), including information that would reveal the existence or contemplated filing of a suspicious activity report. Confidential supervisory information includes any information or materials relating to the examination and supervision of the Bank by applicable bank regulatory agencies, Bank materials responding to or referencing nonpublic information relating to examinations or supervision by bank regulatory agencies, and correspondence to or from applicable banking regulators.