Code of Ethics and Business Conduct

Integrity | Respect | Responsibility | Good Citizenship

All of us serving you®

usbank.com

HR1109I (09/11)

usbank®

Dear fellow employees:

At U.S. Bank, strong ethics are the cornerstone of our business and our culture. While teamwork and innovation play an important role in our company's growth and future, preserving an ethical workplace is critical to our long term success and will continue to differentiate us from our peers.

All of us share a personal responsibility to exemplify our principles of uncompromising integrity, respect, responsibility, and good citizenship. Ethics are so important at U.S. Bank that every employee, starting with me and including each member of the Managing Committee, is expected to certify their compliance with these standards annually.

The dates for the annual certification this year are October 28, 2011 through November 18, 2011. During this period, you will be prompted to certify online when you access Employee Self Service beginning on October 28, 2011.

Read the U.S. Bank Code of Ethics and Business Conduct carefully. Discuss it with your manager and peers, ask questions, and accept nothing short of remarkable ethical conduct from yourself and others at U.S. Bank. If you suspect our Code of Ethics is being violated or are unsure what to do in a particular situation, you have an obligation to promptly report it. Reach out to your manager, your Human Resources representative, or our Ethics Line.

I ask each of you to join me in reflecting a standard of conduct that preserves the strong tradition of integrity and trust that we have worked so hard to earn and is critical to our future.

Sincerely,

Richard K. Davis
Chairman, President and Chief Executive Officer

The Code of Ethics and Business Conduct applies to all employees and directors of U.S. Bank and its affiliates. These policies and standards do not alter your "at will" employment relationship. We recognize your right to resign at any time for any reason; similarly, U.S. Bank, or its affiliates, may terminate any employee, at any time, for any reason. Company directors are expected to comply with all applicable provisions of the Code of Ethics and Business Conduct, even where the terms used may refer only to employees.

Waivers to the Code
Do not expect a waiver of the U.S. Bank Code of Ethics and Business Conduct; whether implicit or explicit, waivers are generally prohibited. Any waiver for executive officers or directors must be approved by the U.S. Bancorp Board of Directors, and will be publicly disclosed. Waivers of the code for employees must be approved by the CEO.

Introduction

U.S. Bank's Code of Ethics and Business Conduct

The ethical principles contained in the U.S. Bank Code of Ethics and Business Conduct (also referred to as "the Code" or "the Code of Ethics") are intended to be a guide and provide a framework for ethical behavior. These principles cannot, however, anticipate every circumstance in which you may be required to act. You must exercise good judgment and conduct yourself in a manner that preserves and enhances the reputation of U.S. Bank.

U.S. Bank Ethical Principles

Uncompromising Integrity: doing the "right thing" without compromise for our customers, suppliers and shareholders – even when circumstances make it difficult. We are clear, truthful and accurate in what we say and do.

Respect: treating one another with respect and dignity; appreciating the diversity of our workforce, our customers and our communities.

Responsibility: taking accountability for ethical decisions and actions; asking for clarification when necessary and reporting concerns or violations in the workplace.

Good Citizenship: complying with the spirit and intent of the laws that govern our business; contributing to the strength and well-being of our communities and shareholders.

You are expected to act lawfully, ethically and professionally in the performance of your duties at all times. While we may compete aggressively, we will not compromise ethical standards and will not violate governing laws. You may not justify illegal or unethical acts by saying it benefited U.S. Bank, nor that someone else in the organization, even a higher authority, directed you to do so. You are never authorized by U.S. Bank to commit, or direct another employee to commit such an act. Also, disparaging remarks or comments to or about fellow employees, U.S. Bank customers, or suppliers that compromise or jeopardize the Company's reputation are not acceptable. However, nothing in the preceding statement is intended to improperly limit or interfere with non-managerial employees discussing the terms and condition of their employment.

In addition to complying with these standards, you are expected to report violations or suspicious activity as outlined in Section 2 of this handbook, Seek Clarification and Report Problems. U.S. Bank provides confidential reporting vehicles and prohibits retaliation against employees who report issues in good faith.

We support our high ethical standards with enforcement. Any action or behavior that, in the opinion of U.S. Bank, violates or jeopardizes our ethical standards as described throughout this Code may result in immediate disciplinary action up to and including termination. To underscore the commitment to ethics at U.S. Bank, Jennie Carlson, Executive Vice President of Human Resources, has been appointed as the Chief Ethics Officer with responsibility for the oversight of all aspects of the Code of Ethics and Business Conduct.

1. Take Responsibility

It is up to you to protect the reputation of U.S. Bank and the privacy of our customers. You are expected to be familiar with Company policies and the laws that govern our business in order to maintain our high ethical standards. In addition to other obligations described below and throughout this handbook, you are responsible for:

- reading, understanding and complying with all of the provisions of this Code;
- complying with the laws and regulations that apply to U.S. Bank's business;
- reporting violations and suspicious activity that may jeopardize the Company's reputation or business; and
- being clear, truthful and accurate with customers, regulators, suppliers, shareholders and other U.S. Bank employees.

There are many resources available to you if you have questions about the Company's ethical standards or need to report problems, violations or suspicious activities. Please familiarize yourself with those resources as well as our non-retaliation policy in Section 2 of this handbook, Seek Clarification and Report Problems.

Your Action is Required

- **When in Doubt, Seek Clarification.** When the right course of action is unclear, ask for help or examine your options with the Ethics Quick Test below:

Ethics Quick Test

- Could it harm the reputation of U.S. Bank?
- Could it be illegal, or is it the wrong thing to do?
- Would it look unfavorable in the newspaper or on the news?
- Would friends, family, the community or shareholders view it negatively?
- Is it inconsistent with U.S. Bank's values, policies and guidelines?
- Would additional advice be helpful?

If you answer "yes" to any of the above questions, contact the appropriate resource to discuss or report concerns. (See Section 2 of this handbook, Seek Clarification and Report Problems, for further guidance.) U.S. Bank's reputation, and your conscience and good name, are far too valuable for you to do anything that may raise an issue under our ethical standards.

- **Complete Ethics Training and Certify your Compliance.** Within 30 days of becoming a U.S. Bank employee, you must successfully complete ethics training and certify your compliance with the Code of Ethics and Business Conduct. Thereafter, you must remain familiar with the Code, complete ethics training on a regular basis, and certify your compliance with the Code annually in conjunction with benefits open enrollment (regardless of your benefit eligibility).
- **Cooperate with Investigations.** Suspected acts of dishonesty, misconduct, or conduct that is inconsistent with these important ethical standards will be investigated in a fair and thorough manner. You are expected to cooperate fully with all inquiries and investigations and maintain confidentiality regarding the investigation.

Q. I can only control my own behavior. Why am I required to report what others are doing?

A. Our success and reputation are dependent upon all of us doing the right thing. One person, one violation, or one indiscretion can significantly compromise the trust of our stakeholders. You cannot ignore or allow others to abandon or disregard our values and expect to succeed yourself. It is up to each of us to protect our reputation by reporting ethical issues immediately.

A Critical Message to Managers

Managers should exemplify the highest standards of conduct and ethical behavior. As a manager, in addition to the responsibilities you have as an employee, you are expected to:

- Lead according to U.S. Bank standards of ethical conduct, in both words and actions.
- Communicate Company ethical standards and procedures on the job, and help employees translate how these standards of conduct and ethics apply to their positions and everyday behavior.
- Promote job effectiveness and compliance by completing all required training in a timely manner and ensuring your employees do the same.
- Create and maintain an environment where employees feel comfortable asking questions or reporting concerns.
- Be diligent in enforcing the Company's ethical standards and taking appropriate action if violations occur.
- Preserve the spirit and intent of these important policies and guidelines through your uncompromising support.
- Contact Human Resources when you have questions or need assistance.

2. Seek Clarification and Report Problems

If you do not understand the meaning of any part of U.S. Bank's Code of Ethics and Business Conduct or how it applies to a particular situation, or if you have concerns about possible unethical conduct, contact your manager or supervisor. If you do not receive a clear explanation or believe you may not receive an adequate review of the issue by your manager or supervisor, or you are uncomfortable asking your manager, contact Human Resources directly or call the confidential Ethics Line (see below) for assistance. If your concerns remain unresolved, you should pursue reporting through other available channels, such as higher levels of management or Human Resources, or contact the Ethics Line.

Assuring The Integrity of Our Financial Reporting/Escalating Complaints or Concerns

At U.S. Bank, the integrity of all of our actions, including our financial reporting, is vital. All business transactions must be properly and accurately recorded in a timely manner on U.S. Bank's books and records and in accordance with applicable accounting standards, legal requirements, and our system of internal controls. U.S. Bank is committed to providing a work environment in which its employees can raise concerns over accounting, audit or internal control matters, or potential violations of laws or Company policies, without fear of discrimination, retaliation, threats, or harassment. U.S. Bank's Employees are strongly encouraged to raise any such concerns to their managers, to Human Resources or anonymously to our Ethics Line. U.S. Bank employees may also raise such concerns directly to the Chair of the Audit Committee of the

Board of Directors. U.S. Bank will treat all such complaints or concerns received as confidential and privileged to the fullest extent permitted by law, and will exercise particular care to keep confidential the identity of any individual making a complaint. All such complaints or concerns will be thoroughly reviewed and appropriately investigated, and reported to the Audit Committee of the Board of Directors of the Company.

Integrity in the Reporting Process

Making false allegations due to improper motives is a serious issue and may result in disciplinary action. Such allegations undermine the effectiveness of the reporting process, compromise the reputation of others, and will not be tolerated.

Non-Retaliation Policy

U.S. Bank does not tolerate any retaliatory action against any individual related to good-faith reporting of ethics violations, illegal conduct, sexual or other forms of harassment, discrimination, inappropriate workplace behavior, or other serious issues. Allegations of retaliation will be appropriately investigated and, if substantiated, appropriate disciplinary action will be taken, up to and including termination. Diligent enforcement of non-retaliation measures are vital to the success of the reporting process because employees must feel they can report problems without fear of reprisals. You may report suspected retaliation to a supervisor, a manager, Human Resources, the Legal Department, or the Ethics Line.

Q. I made a complaint about my manager through the Ethics Line. I am worried that my manager will be upset and start treating me differently because of my complaint. How can I be sure my complaint will not negatively affect my job?

A. U.S. Bank reviews the non-retaliation policy and consequences of retaliation with managers when situations are reported. Managers are forbidden from taking retaliatory actions, expected to guard against retaliatory conduct, and required to proactively watch for signs that retaliation may be occurring. Managers may be subject to discipline and/or termination if they violate this important policy. If you suspect retaliation by your manager, report it.

3. Protect the Privacy of Customers and Confidential Company Information

The Bank's continued success depends on its ability to keep "information assets" (e.g., customer account numbers, social security numbers, and other private data) safe from fraud, theft, identity theft and accidental disclosure. All Bank employees must comply with information security requirements that teach us how to keep valuable confidential information safe. These requirements are set forth in U.S. Bank Information Security documents available from USBnet. In addition, please refer to guidance under Section 12 of this handbook, Public Statements on Behalf of U.S. Bank and Online Social Media and Other External Communications.

Information Classifications

All information about U.S. Bank customers, employees, business partners, and others about whom information is collected, processed, stored, or transmitted, is the property of U.S. Bank. This information is classified as U.S. Bank Public, Internal, Confidential, or Customer Confidential. You must become familiar with these information classifications and their associated handling requirements, described as follows:

U.S. Bank Public	Information controlled by the corporation that has been made available to the public through authorized Company channels or has been placed in the public domain by the information owner.
U.S. Bank Internal	Information controlled by the corporation that may be made available to all U.S. Bank employees and authorized contractors, consultants or other third parties, but not to the general public because unauthorized external disclosure could cause some damage to the corporation or any of its stakeholders (employees, customers, etc.).
U.S. Bank Confidential	Information that provides the corporation with a competitive advantage or that is otherwise sensitive because disclosure could cause significant damage to the corporation or any of its stakeholders (employees, customers, etc.). The level of protection required is generally determined by the degree of damage that could result from its disclosure. Access to the information must be restricted based on the need-to-know principle. Data owned by third parties and obtained under contract, such as non-disclosure agreements, is considered U.S. Bank Confidential, at minimum.
U.S. Bank Customer Confidential	Information about any individuals, including business customers and personnel, that is subject to protection under laws, regulations, contractual agreements, and/or Company policy. This includes personal data that could be used to identify an individual or family and information about individuals that is owned by third parties.

See the U.S. Bank Classification and Handling Standards for more detailed information regarding these information classifications. This policy is not intended to improperly limit or interfere with non-managerial employees discussing the terms and conditions of their employment.

Confidentiality of Bank Information

The use of any banking information to which you have access as an employee or director shall be restricted to that which is absolutely necessary for the legitimate and proper business purposes of U.S. Bank. Sharing information about our customers with anyone inside or outside the Company

who does not have a business need for the information is prohibited, unless required by law. A casual remark to family, friends, or acquaintances can form the basis for misinterpretation or otherwise violate the integrity of Company relationships. Inappropriate discussions or the improper release of information may result in disciplinary action up to and including termination.

In addition, business information such as strategic plans, products, other nonpublic information, and confidential employee information (such as Social Security numbers or health information), must be treated with utmost discretion. When your employment or your service as a director ends, your obligation to maintain the confidentiality of information continues to apply.

Information is Bank Property

While at U.S. Bank, you may produce, develop and have access to information, ideas, inventions, techniques, processes, computer software, "know-how," materials, programs, reports, studies, records, data, customer lists, customer information, trade secrets, confidential employee information, and other information not generally available to the public regarding U.S. Bank and all related entities, their employees, customers, prospective customers, and other third parties. The above listed items are examples of U.S. Bank Internal, Confidential, or Customer Confidential information. This information may be in original, duplicated, electronic, memorized, handwritten, or in another form. Employees and directors may not use such information outside of U.S. Bank business. As a condition of employment, employees are required to acknowledge and agree that U.S. Bank Internal, Confidential and Customer Confidential information is U.S. Bank's sole property and disclaim any rights and interests in any U.S. Bank Internal, Confidential, or Customer Confidential information and assign these rights to U.S. Bank. Employees may access and use U.S. Bank Internal, Confidential, and Customer Confidential information available on or through work computers or through the Bank’s network only for legitimate and authorized business purposes. Employee access and use rights to such information will be considered revoked where unauthorized access and/or use occurs.

All records, files, documents and other U.S. Bank Internal, Confidential, or Customer Confidential information that you prepare, use or come into contact with shall remain U.S. Bank's property and may not be used for any unauthorized purpose, or divulged, or disclosed to any unauthorized third party. Under no circumstances should you reveal or permit this information to become known by any competitor of U.S. Bank, or any other unauthorized third party, either during or after your employment or service as a director. You are expected to use reasonable care to prevent the disclosure or destruction of U.S. Bank Internal, Confidential, and Customer Confidential information. If you become aware of the loss, theft, or other unauthorized acquisition of such information, you must follow the procedures described in “Reporting Information Security Problems,” below. If your employment with U.S. Bank ends, you must return all U.S. Bank Internal, Confidential, or Customer Confidential information (and any copies of this information), including information you may have retained in personal items (e.g., electronic devices or home computers). Also, be sure to delete any Company-related and customer phone numbers and messages you may have on your personal cell phone or other personal devices.

U.S. Bank expressly forbids the unauthorized use or duplication of U.S. Bank Internal, Confidential, or Customer Confidential information, such as customer lists. You may not make unauthorized copies in electronic form or use personal recording devices, including camera phones, to record communications containing proprietary information. Any authorized recordings of Company communications may be used and reviewed only in a manner consistent with this policy. See also Section 9 of this handbook, Prohibited Recordings and Photography.

Q. A former employee called and requested that I send her a copy of a proposal she worked on before she left the Company. May I send it to her?

A. No. This proposal is either U.S. Bank Confidential information or U.S. Bank Internal information and may not be released outside of the Company – not even to the individual who created the material.

Information Security Policies and Training

You are responsible for reviewing and adhering to the U.S. Bank Information Security Policies and all other Information Security Requirements applicable to your job function and responsibilities. You are also expected to complete all information security awareness training courses on a regularly scheduled basis, and as assigned. While this document provides an overview of some of the more common information security requirements with which you must become familiar, it is by no means comprehensive. The Information Security Policies and other information security requirements you will learn about in mandatory training contain many provisions in addition to those specifically discussed here.

Safeguarding U.S. Bank Information

Every employee is responsible for safeguarding information. Below are some of the basic guidelines employees should follow at all times to safeguard U.S. Bank Internal, Confidential and Customer Confidential information:

- **Know what information you handle and follow the proper safeguarding policies.**
  - Recognize the classification categories noted above and handle information accordingly.
  - Customer Confidential Information, which includes information about people, such as social security numbers (SSN), credit card or transactional account numbers often in combination with a name, address or phone number, require special safeguards.
  - The identities of customers, their banking activities, or account relationships is considered confidential information. Sharing or discussing such information for non-business purposes is prohibited.
- **Handle information securely.**
  - Make sure U.S. Bank Confidential or Customer Confidential information is not left in plain view on your desk, in your cubicle or office space, or in a shared area.
  - Store U.S. Bank Confidential or Customer Confidential information where only authorized individuals can view or access it.
  - Use secure disposal containers to discard confidential information.
  - Limit and protect U.S. Bank Internal, Confidential or Customer Confidential information taken off bank premises, whether in physical or electronic format. See Section 10 of the U.S. Bank Classification and Handling Standards for more information.
  - Laptops, PDAs and other electronic devices are valuable bank assets. Extra care is required to safeguard these items from theft regardless of whether they contain confidential information.
- **Use secure email (key123) when required.**
- **Keep passwords secure.**
  - Never share your passwords with others.
  - Never leave passwords where they might be found by someone else.
  - Create passwords at least seven characters long that are difficult to guess.
- **Minimize sharing of information with others.**
  - Do not provide access to U.S. Bank Confidential or Customer Confidential information to anyone, inside or outside the Company, who is not authorized to receive it.

  - Eliminate confidential information not needed. Provide only the requested information.
  - Be alert to pretext calling and email phishing scams. When in doubt, verify.
  - Do not attempt to gain access to information you do not need to perform your job.
- **Use caution when required to transfer confidential information.**
  - Question the need for any confidential or customer information that is being shipped or received.
  - All tapes and portable electronic media (PEM) (i.e., CD's/DVD's, USB drives, etc.) must be encrypted according to Bank standards.
  - Physical documents must be transported securely.
- **Be alert to new business changes that could impact safeguarding practices.**
  - Use of vendors must be tightly monitored following bank policy.
  - Make sure newly acquired businesses or newly developed products follow our safeguarding policies.
  - Promote the importance of information security training.

Please review the U.S. Bank Information Security Policies at USBnet for additional information.

Additional Information Security Obligations

In addition to safeguarding Bank information as described above, employees have additional security obligations. The following requirements, which are fully detailed in the U.S. Bank Information Security Policies, apply to all employees and other users of U.S. Bank systems and information:

- U.S. Bank is subject to legal and regulatory requirements for handling customer information and for maintaining accurate and complete financial records. As a credit/debit card issuer and processor, the Bank is also subject to the Payment Card Industry Data Security Standards (PCI). You must comply with legal, regulatory, and PCI standards, as well as other contractual requirements that apply to the work you do. Your manager can tell you what is required of you if you are ever in doubt.
- Everyone who uses a U.S. Bank system is assigned a personal user ID and associated password that is intended for use by the assigned individual only. The person assigned a personal user ID is responsible for all actions executed under that ID and must adhere to applicable information security requirements to prevent user ID misuse. In certain limited circumstances, for purposes of managing some systems, user names and passwords may need to be shared to facilitate maintenance or other system-required accessibility. In such cases, Information Security Services must approve the use of a shared user name and password.
- Employees must use, and may not alter, required security controls on Bank systems.
- Employees are responsible for taking steps to protect information on U.S. Bank computer systems. It is possible for unauthorized individuals to steal information or otherwise tamper with computer systems left unprotected.
- Employees who have been issued a laptop computer, who have remote access to Bank systems, or who have been authorized to use other Portable Electronic Media (PEM) devices in the conduct of U.S. Bank business must comply with additional security measures designed to prevent the inadvertent disclosure of U.S. Bank information.

Getting More Information

For more information regarding the above-described obligations, or any other questions about information security policies, please refer to the U.S. Bank Information Security Policies on USBnet, or contact the Information Security Policies Shared Mailbox at iss.policy@usbank.com.

Reporting Information Security Problems

As a user of U.S. Bank information systems, you have an affirmative obligation to report security problems. If you know of or suspect a security weakness or a violation of any information security requirement, you must report it to your manager and to Information Security Services using the following resources:

- Report violations or potential violations of U.S. Bank Information Security Policies to the Information Security Policies Shared Mailbox at iss.policy@usbank.com.
- Report unauthorized disclosure of U.S. Bank Customer Confidential Information to Dan Burks or Rick Rushing in the Privacy Office.
- Report unsafe handling of U.S. Bank Customer Confidential information you observe to Dan Burks or Rick Rushing in the Privacy Office.
- You may also report any violations or potential violations to the Ethics Line.

4. Prevent Money Laundering and/or Fraud

Money laundering (converting illegal proceeds to make the funds appear legitimate) is a global problem with far-reaching and serious consequences. As a financial services provider, we take our obligation to help close the channels used by money launderers seriously. Compliance with the Bank Secrecy Act (BSA) and related Anti-Money Laundering (AML) laws and regulations is also critical to preventing our organization from being used as a conduit for money laundering or for funding terrorist or other criminal activity.

The penalties for failure to comply with these laws can be severe. In the United States, an individual convicted of money laundering and can face up to 20 years in prison, and a company can face significant monetary fines, not to mention significant reputation damage.

As an employee, you are expected to identify and report suspicious activity in a timely manner; and follow established Customer Identification Procedures.

Anti-Money Laundering laws are just a few of the many laws and regulations with which the Company must comply. Therefore, it is important that you understand and follow the policies and procedures established to meet the Company's legal and regulatory obligations. You should also complete regular training regarding BSA/ AML and other applicable laws and regulations. Contact your manager or Human Resources generalist for further information regarding required training.

Reporting Procedures

If you encounter a customer or transaction that appears suspicious, report it as follows:

Suspected Issue	Reporting Procedure
Money laundering, Bank	Access the Suspicious Activity and Fraud Referral Center,

Secrecy Act violations, or terrorist financing activities	select the type of activity to be reported and complete an Investigative Referral Form (IRF) on USBnet, within five days of detection. Once submitted, the IRF will be automatically filed with the AML ID Department.
Actual or suspected criminal activity, unusual or suspicious activity, or an unexplained loss not related to money laundering, the Bank Secrecy Act, or terrorist financing	Access the Suspicious Activity and Fraud Referral Center, select the type of activity to be reported and complete an Investigative Referral Form (IRF) on USBnet.

For additional examples of reportable suspicious activity, please refer to the *U.S. Bancorp Guidelines for Suspicious Activity Reporting* on USBnet.

U.S. Bank prohibits the internal or external disclosure that suspicious activity is or was reported. Employees may not disclose to any parties other than appropriate law enforcement or regulatory agencies that an Investigative Referral Form (IRF) or a Suspicious Activity Report was filed, or provide any information that would divulge that a Suspicious Activity Report has been prepared or filed,

If you have questions about applicable laws or regulations, consult with your immediate manager or supervisor, or the Corporate Compliance Department (Compliance Hotline 612-303-3810).

Q. When is an Investigative Referral Form (IRF) required and who prepares it?

A. Whenever a customer or transaction appears suspicious, in regards to money laundering, Bank Secrecy Act violations, or terrorist financing, the employee with the suspicion must complete and submit an IRF within five days of noticing the suspicious activity.

5. Demonstrate Workplace Respect

Respect and Consideration in All Interactions

You are expected to treat fellow employees with professionalism, respect, consideration, and understanding, which fosters a climate conducive to a high level of performance and open communication at all levels. You are expected to conduct your day-to-day business with the highest standards of integrity and to devote your efforts to successful performance of your job. Open discussion of job-related problems and prompt resolution of those problems is encouraged.

Treat customers, potential customers, vendors and the communities U.S. Bank serves with equal respect and professionalism. Provide courteous service and conduct business ethically and in compliance with all laws and regulations. Always act in ways that reflect favorably on U.S. Bank.

Commitment to Workplace Diversity

U.S. Bank is committed to a work environment that values each individual's unique talents and background, respects differences, and recognizes the opinions and ideas of every employee. It is important for you to develop, encourage, and maintain a positive attitude towards diversity and to value and respect differences among the people with whom you interact. Valuing and

respecting such differences helps you to be more successful in identifying and meeting customer needs and developing effective work relationships.

We are committed to Equal Employment Opportunity (EEO) and Affirmative Action. Embracing diversity is not only the right way to do business, it is essential to the success of the Company. Employees, the labor market, and existing and prospective customers comprise a widely diverse population. U.S. Bank is better able to effectively serve a diverse marketplace by having a diverse workforce. As an employee, you are expected to promote Affirmative Action and EEO and help ensure that the work environment is free from unlawful discrimination.

U.S. Bank prohibits both discrimination against and harassment of any employee or applicant, and ensures that all personnel practices are administered on individual merit and capability without regard to race, religion, color, age, sex, national origin or ancestry, sexual orientation including gender expression or identity, genetic information, disability, veteran status, or other factors identified and protected by law. These practices include, but are not limited to, recruitment, advertising, selection, performance management, compensation, training, placement, transfer, demotion, promotion, disciplinary action and termination.

If you have a concern about EEO or Affirmative Action issues, contact your supervisor, manager, Human Resources or the Ethics Line. Allegations of behavior inconsistent with U.S. Bank's workplace diversity commitment, including suspected discrimination, will be investigated. Appropriate corrective action will be taken where a violation of U.S. Bank policy has occurred.

If you are a veteran, disabled veteran, or an individual with a disability and wish to be considered under the U.S. Bank Affirmative Action Program, or if you would like more information about the EEO or Affirmative Action Program, please contact Human Resources.

Employees and Customers with Disabilities

Individuals with disabilities are entitled to access to goods, services, products, accommodations, and employment. We are committed to providing reasonable accommodations for employees and customers with qualified disabilities.

Reasonable accommodations will be made so that an employee with a disability may have the opportunity to perform the essential functions of a particular position and otherwise participate fully in employment. This may involve special equipment or simple physical adjustments to the work site. If you have a disability that requires accommodation within your current job or in a position for which you wish to apply, please discuss your situation with your manager or Human Resources. They will work with you to try to evaluate accommodation options.

Customers may also have disabilities that need to be accommodated. Whether you work with customers in person or over the phone, pay attention to any physical or communication barriers and offer assistance when needed. In some situations, you may need to consult with your manager to assess appropriate assistance measures, especially where a customer requests a specific type of accommodation. We will remedy architectural and communication barriers in accordance with applicable law so that all customers have access to U.S. Bank products and services.

Offensive Behavior and Harassment

It is U.S. Bank's policy and the responsibility of all employees to maintain a working atmosphere free of discrimination, harassment, intimidation and unwelcome, offensive, or inappropriate conduct, including sexual overtures, offensive jokes, graphic material, etc. We will not tolerate

verbal or physical conduct of a demeaning or sexual nature that creates an intimidating, hostile or offensive working environment that in any way affects the employment relationship or is otherwise deemed by U.S. Bank to be offensive and/or inappropriate. Conduct may be deemed offensive behavior prohibited by this policy even if it does not meet the legal definition of harassment under state and/or federal law.

Conduct prohibited by this policy may include, but is not limited to, verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of the individual's race, religion, age, color, sex, national origin or ancestry, sexual orientation including gender expression or identity, genetic information, disability, veteran status or other factors protected by law. Specific examples of conduct prohibited by this policy may include, but are not limited to: disparaging remarks, slurs, negative stereotyping, threats, intimidation, hostile acts, and denigrating or hostile written or graphic material posted or circulated in the workplace.

Sexual harassment is specifically prohibited by this policy. Sexual harassment includes any unwelcome sexual advance, request for sexual favor, and other verbal or physical conduct of a sexual nature where:

- submission to the conduct is, or is threatened to be, a condition of employment;
- submission to or rejection of such conduct is used, or is threatened to be used, as the basis for employment decisions;
- the conduct has the purpose or effect of unreasonably interfering with an individual's work performance; or
- the conduct has the purpose or effect of creating an intimidating, hostile or offensive work environment.

Also see the Sexual Harassment: Keeping it out of the workplace policy for further information.

To help keep our workplace free of offensive behavior and harassment, you must complete Workplace Harassment Awareness training. If you are a manager, you may be expected to complete more specific Harassment Awareness training.

Employees who violate this policy are subject to disciplinary action up to and including termination. If you believe you have been discriminated against or harassed by a co-worker, manager, vendor or customer, or you have knowledge about harassing behavior involving others, promptly report this to a supervisor, manager, your Human Resources generalist, or the Ethics Line. An appropriate investigation will be conducted and appropriate action will be taken if a violation of U.S. Bank policy has occurred.

Q. A co-worker keeps telling jokes and making comments that I find offensive. Most people just laugh, but I know others are uncomfortable with it, too. My supervisor knows about it, but nothing has changed. What should I do?

A. Report the problem to the next-level manager, your Human Resources generalist, or to the Ethics Line for investigation. If you are comfortable doing so, it is also appropriate to tell co-workers when you are offended by their comments and ask them to stop.

Non-Retaliation Policy

U.S. Bank does not tolerate any retaliatory action against any individual related to good-faith reporting of ethics violations, illegal conduct, sexual or other forms of harassment, discrimination,

inappropriate workplace behavior, or other serious issues. See the complete Non-Retaliation Policy in Section 2 of this handbook, Seek Clarification and Report Problems.

Substance Abuse and Drug and Alcohol Workplace Rules

Alcohol and drug abuse adversely affects job performance and safety in the workplace. A productive and safe work environment is in the best interests of all employees, customers and shareholders. Therefore, being under the influence of and/or the use of alcohol, narcotics, depressants, stimulants, hallucinogens, marijuana, intoxicants (any substance whether legal or illegal that produces a condition of diminished mental or physical capabilities, including medical marijuana) or any other controlled substances during working hours as well as during other work-related events is prohibited. In addition, if the use of prescription medication adversely affects your work performance, you should contact your Human Resources generalist to discuss the situation.

This policy applies to all applicants for employment and to all employees, including independent contractors or employees of temporary staffing agencies. The policy is applicable at U.S. Bank facilities or wherever U.S. Bank employees are performing Company business. The only exception to this policy is the moderate use of alcoholic beverages at Company-sponsored or sanctioned events where authorized by senior management and Human Resources, for example, company-wide or business group holiday parties.

Drug and alcohol abuse are serious problems that may be successfully treated. If substance abuse is a problem for you or a family member, obtain confidential help through LifeWorks, our employee assistance program.

If you are unable to work due to alcohol or drug use, you come to work under the influence of alcohol, illegal drugs, or other intoxicants, or you use illegal drugs at or outside of work, or you otherwise violate this policy, you may be sent home and may be subject to disciplinary action. You may also be referred to the employee assistance program for an evaluation. A referral of this nature does not preclude disciplinary action, nor does it imply or constitute disciplinary action.

Q. Sometimes my friends invite me to lunch where they have a beer or two before returning to their jobs at a different employer. Is it ok for me to have an alcoholic drink over my lunch hour?

A. No. You may not consume alcohol during your working hours, which includes lunchtime. We are responsible for ensuring a workplace not adversely affected by the influence of alcohol or prescription or illegal drugs, and even if consumed in small amounts, alcohol can impair your ability to perform your job.

Drug and Alcohol Testing

Drug and alcohol testing may be conducted:

- for external job applicants who are offered a position;
- for employees where required by law or contract;
- when the employee has caused or is involved in a work-related accident resulting in injury or property damage;
- when there is a reasonable suspicion, as determined by U.S. Bank, that the employee has violated this policy or any other applicable U.S. Bank policy;
- when the employee has been referred by U.S. Bank for chemical dependency treatment or evaluation; or

- randomly in positions that have been designated as "safety sensitive" or "high risk."

We will abide by all applicable laws governing testing, use only certified laboratories to conduct tests, keep test results confidential, and use results only for business purposes.

You may refuse to submit to a drug or alcohol test; however, to the extent permitted by law, refusal may result in disciplinary action up to and including termination.

Individuals tested may explain a positive test result on a confirmatory test or request and pay for an additional confirmatory test using the same specimen. Positive test results may result in one of the following:

- referral to a rehabilitation program; and/or
- disciplinary action, up to and including termination.

Individuals tested may receive copies of their test results upon request.

Review the Drug and Alcohol Workplace Rules and Testing Policy and Procedures on USBnet for the full text of the policy and more information regarding drug testing procedures.

Use of Company Vehicle or Personal Vehicle for Company Purposes

- **Drug and Alcohol Use While Driving Prohibited.** You are prohibited from operating a Company-owned, personal, rental, or other vehicle while performing Company business after consuming alcohol, narcotics, depressants, stimulants, hallucinogens, marijuana, or any other controlled substances. Refrain from driving if the use of prescription medication adversely affects your ability to safely operate the vehicle. See the Policy Regarding Use of Company Vehicles on USBnet, at for additional policies that apply to the use and operation of Company-owned vehicles.
- **Proof of Insurance and/or Driving Record Requirements.** If you use a Company-owned car or your personal vehicle to perform Company business, you may be required to provide (or consent to the release of) proof of insurance and/or driving record prior to commencing work, and periodically thereafter.
- **Cell Phone Use and Text-Messaging While Driving.** If you drive a vehicle while on Company business, during normal working hours or for business use while driving outside of normal business hours, whether the vehicle is personally-owned, Company-owned, rental or otherwise, you are responsible for the safe operation of the vehicle. Accordingly, you must comply with all federal, state and local laws while driving, including but not limited to laws regarding the use of cellular phones, personal digital assistants (PDAs) or other handheld devices while driving. You are strongly encouraged to avoid making or receiving telephone calls while driving. To the extent allowed by law and when necessary to make or receive calls when driving, cellular phones must be used only when the vehicle is safely parked, or with approved hands-free devices, such as a headset. Operating PDAs, text messaging or engaging in other similar conduct while operating a company vehicle, or while on Company business is prohibited.

Violation of this policy may result in disciplinary action up to and including termination.

6. Be Honest and Above Reproach

The nature of U.S. Bank's business demands integrity in all personal and professional business practices. As an employee, you are accountable to a number of constituencies – shareholders, customers, government agencies, the communities we serve, the general public, and other employees.

You are expected to treat all Company resources, including its name, with the respect befitting a valuable asset. Never use these resources in ways that could be interpreted as imprudent, improper, or for personal gain.

U.S. Bank's business is based on mutual trust and absolute honesty in all of its affairs, both internally and externally and these standards are diligently enforced. Respect this philosophy at all times, in both your personal and corporate behavior. Exercise complete candor with the Company's legal counsel, auditors, loan review and compliance staff, Controller, regulators Human Resources, and Corporate Security. Be frank and objective, which allows for the early identification of problems – real or potential, small or large. Be clear, truthful, and accurate in your interactions with customers and other employees. Deal fairly with customers, suppliers, competitors, and other employees. These standards are diligently enforced.

This philosophy calls not only for proactive behavior, but also prohibits inaction intended to conceal relevant information. Intentional concealment or alteration of accurate and/or truthful information, for whatever reason, will be considered a violation of this Code. Violations of laws involving dishonesty, breach of trust, or which may affect the reputation of U.S. Bank, must be disclosed and reported to U.S. Bank even if they are outside the scope of employment.

Q. I think a co-worker recently exaggerated the financial position of a customer in order to get the loan through. I know this has happened before, but I am reluctant to come forward with the information. What should I do?

A. Falsifying records and misrepresenting a customer's financial position are serious violations of our ethics policies. They also create a business risk and must be reported immediately. Talk with your manager or report the problem to Human Resources. If you are uncomfortable reporting the problem through those channels, report it confidentially through the Ethics Line or the U.S. Bank Ethics Line Web Form.

7. Handling Gifts, Entertainment, and Other Benefits

Prohibition on Giving and Receiving Gifts or Anything of Value

U.S. Bank policy and certain laws and regulations prohibit employees, officers, directors, agents, and attorneys of financial institutions from seeking or accepting anything of value in connection with any transaction or business of their financial institutions. These prohibitions can apply even if the individual does not benefit directly from the item of value. Accepting or soliciting benefits or items of value for the benefit of a third person or party (other than U.S. Bank) is also prohibited. Directors, officers, employees, and members of their families may not solicit or allow themselves to be solicited or accept gifts, entertainment, or other gratuities intended to or appearing to influence decisions or favors toward the U.S. Bank's business. Certain restrictions also apply to giving gifts to U.S. Bank customers, vendors, or officials.

Guidelines on Giving Gifts

If you wish to give reasonable gifts (including entertainment) to customers or potential customers, or any other third party with whom your business line has a business relationship, you must consult with your manager about any specific gift-giving rules or guidelines that apply to your business line or work group and follow standard expense authorization procedures. Gifts of cash are strictly prohibited. (Gifts to vendors is covered under "Other Payments and Uses of Vendor Resources," below.) These restrictions generally are not intended to apply to gifts or entertainment based on family relationships where it is clear that the relationship is the motivating factor for giving the gift. Additional laws apply to the provision of gifts, meals, entertainment or anything else of value to certain recipients.

You must obtain pre-clearance from the Legal Department before providing any gift, meal, entertainment or anything else of value to federal, state, local, or foreign public officials. See Section 12 of this Code of Ethics Handbook under "Gifts and Entertainment of Public Officials" for further details. There may be restrictions on giving gifts to federal, state, or local public officials who are also family members, so please consult with the Legal Department for additional information.

Guidelines on Receiving Gifts

There are certain circumstances under which acceptance of gifts or other items of value do not violate the general policy prohibition of gifts. The below guidelines are intended to address situations that are the most likely to raise questions. However, certain U.S. Bank business units have more restrictive policies with respect to gifts. *You are required to be aware of and comply with any additional policies and procedures applicable to your work group*.

Generally, accepting an item or benefit will not violate the policy against giving/receiving gifts, entertainment, or other benefits if:

- the acceptance is based on an obvious family or personal relationship existing independent of any business of U.S. Bank (such as those between the parents, children or spouse of a representative of U.S. Bank) where the circumstances make it clear that it is that relationship, rather than the business of U.S. Bank, that is the motivating factor;
- the benefit is available to the general public on the same conditions on which it is given to the representative of U.S. Bank; or
- the benefit would be paid for by U.S. Bank as a reasonable business expense if not paid for by another party.

In addition, provided there is no intent to influence by either the giver or the receiver of the benefit, the following may be accepted under the circumstances described:

- advertising or promotional material of reasonable value, such as pens, pencils, note pads, key chains, calendars and similar items;
- discounts or rebates on merchandise or services that are available to other customers under similar circumstances;
- awards of a reasonable value from civic, charitable, educational, or religious organizations for recognition of service and accomplishment;
- gifts awarded as part of a random drawing where it is clear that no possible inference can be drawn that acceptance of the gift could influence you in the performance of your duties for U.S. Bank.

Generally, the below listed gifts or benefits may be acceptable under the circumstances described. However, please consult with your manager *before* accepting any of the following to

ensure your actions are in line with this policy, regulatory guidance, and your business line's expectations:

- meals, refreshments, entertainment, accommodations or travel arrangements of reasonable value in the course of a meeting or other occasion where the purpose is to hold bona fide business discussions or to foster better business relations, provided your host is present, your attendance is related to your job duties, the level of expense is reasonable and customary in the context of your business and the relationship with the host, and the frequency of such invitations from one host, is not excessive;

- gifts not to exceed $100, or $25 in the case of gift cards or gift certificates for use at specific establishments, that are related to commonly recognized events or occasions, such as a promotion, new job, wedding, retirement, holiday or birthday. However, gifts in cash or in check form in any amount are strictly prohibited (stored value cards that are not tied to a specific retailer are prohibited - a Visa gift card, for example).

Exceptions occasionally are made allowing or encouraging employees or directors to attend events that exceed this policy if a significant customer or vendor sponsors an event, or attendance at an event is important to maintaining U.S. Bank's relationship with that customer or vendor. However, consult with your manager and Human Resources to determine if such an exception is appropriate before attending any such event.

If you encounter a situation in which you are not sure how to proceed, or if the application of these guidelines appear to be unduly restrictive, consult your manager or Human Resources generalist for guidance.

Under no circumstances should you accept any personal gift or favor if it appears that by giving it the donor hopes to influence any business of U.S. Bank or to reward them for actions taken on behalf of U.S. Bank.

This policy is not intended to apply to nominal gifts between co-workers. However, other business line restrictions may apply, so please consult with your manager or Human Resources generalist for further clarification if needed.

Q. I was invited to attend a local sporting event with a customer. May I attend?

A. You may attend the event if the purpose is to hold bona fide business discussions or further the customer relationship, unless your business line has a more restrictive policy. If the customer is offering the tickets for your personal use and will not be attending the event with you, the gift rules apply, and the gift must not be accepted unless it is related to commonly recognized events or occasions, and the value of the tickets does not exceed $100. Consult with your manager before accepting the invitation in either case to ensure your actions are in line with this policy, regulatory guidance, and your business line's expectations.

Q. I am a Teller, and a regular customer gave me a $5 gift card to a local coffee shop as a token of appreciation on my birthday. Can I keep it?

A. First, consult your manager about your business unit's policies regarding gifts. In general, however, accepting a gift card in the amount of $5 to a specific establishment would be acceptable under this policy.

Other Payments and Uses of Vendor Resources

Payments that include fees and commissions are an integral part of business activity. U.S. Bank regularly engages the service of vendors as well as lawyers, consultants and other professionals. While selection for performance of a specific service may involve a degree of subjectivity, the choice should always be predicated on quality, competence, competitive price and service, business relationship, and evidence of the same ethical standards of integrity demanded by this Code.

Q. One of my colleagues has a brother-in-law who is a freelance computer programmer. Whenever we need some code written, the brother-in-law gets a call from my colleague and gets the job. The brother-in-law does a good job, but somehow, this does not seem right.

A. Clearly your colleague's approach is, at a minimum, creating an appearance of impropriety. However, you may not have all the facts. It could be that your colleague's manager has been fully informed and the manager approves because the appropriate processes have been followed. You should discuss this matter with your manager.

In all cases, U.S. Bank will compete for business only on the basis of the quality and price of its services and to meet its customers' needs today and over time. At no time will U.S. Bank enter into any payment or other arrangement that violates this statement, lowers its ethical standards or could conceivably bring disrepute to the Company. Gifts, monetary payments, loans, lavish entertainment, or other items of value or favors made to or received from vendors or other outside parties in exchange for business or influence of any kind are strictly prohibited.

Q. I have been invited by a client, along with several co-workers, to attend a non-business related special event. The cost of the event tickets is difficult to calculate. May I attend this function with the client?

A. Generally, no. Contact your manager or Human Resources to fully explore the ethics issues involved.

Personal Benefit

You may not take advantage of your position at U.S. Bank to profit personally from information, corporate property, services, or other business opportunities, unless the situation is deemed incidental or authorized by the Company.

Commitments

You may not make commitments, formally or informally, on behalf of the Company without appropriate authorization in accordance with approved procedures. Approved commitments within the scope of your authority should be properly documented and retained.

8. Avoid Conflicts of Interest

What is a Conflict of Interest?

A conflict of interest exists when you have an outside interest that interferes with your responsibilities to U.S. Bank or affects your ability to act in the best interest of U.S. Bank and its customers. Avoid conflicts of interest, and potential conflicts of interest and situations where there may be an appearance of a conflict of interest.

You may not engage in any employment or activity which competes with any business of the Company, conflicts with the fiduciary obligations of any other department, or creates a conflict of interest with your position or department. In all cases, additional employment outside of U.S. Bank must be approved in advance by your manager.

Q. I recently started working for U.S. Bank as a Personal Banker. I also have my real estate license and was planning to work as a residential real estate agent on the side. Is this a conflict of interest?

A. Yes, as a Personal Banker, this outside activity will always be considered a conflict of interest. As a real estate agent, you are in a position to recommend banking services to your clients that may include referrals to non-U.S. Bank financial institutions. This prohibition is applicable to many positions throughout the Bank. In addition, there may be very limited exceptions to this policy depending on your position and the specific business line. Consult with management and Human Resources for further guidance before you perform any real estate agent work on the side.

Consistent with U.S. Bank's commitment to community involvement, you are encouraged to participate in civic affairs, including service with constructive and legitimate for-profit and non-profit organizations. There are cases, however, in which organizations have business relationships with U.S. Bank or in which the handling of confidential information might result in a conflict of interest.

All actual, perceived, and potential conflicts of interest must be reported immediately to your manager. In the case of an actual, perceived, or potential conflict involving a senior officer, report the matter to your Human Resources generalist and the Legal Department.

Q. I work full time in the Retail Bank group, and I have a part-time position with another financial services company doing telemarketing on the weekends. Is this a problem?

A. Yes. While every situation is evaluated on a case-by-case basis, telemarketing for a competitor organization presents a conflict of interest. Ideally, additional outside employment opportunities should be disclosed prior to starting such employment, or prior to starting work with U.S. Bank.

Directorships and Outside Business Activities

You may accept election or appointment to public or civic commissions and to boards of non-profit corporations if you give reasonable notice to your manager before you are elected or appointed.

Q. May I sit on the Board of Directors for a non-profit organization?

A. You may serve as a board member for a non-profit organization. However, you must notify your manager first to ensure that these activities do not create a conflict of interest with your job and that you would not be participating in decisions regarding U.S. Bank and its services.

Outside "For-Profit" Enterprises

There are a number of laws that prohibit certain interlocking corporate directorships and management positions or have other restrictions regarding corporate directorships while being employed by U.S. Bank or an affiliate.

In addition, all candidacies or appointments to for-profit business corporation boards must be reviewed for any possible conflicts of interest and approved in advance by the vice chair of the business line and must also be approved by U.S. Bank's President and Chief Executive Officer. Please work with your Human Resources generalist to obtain the necessary approvals.

Each year during the annual ethics certification period, senior managers are required to report if they serve on any outside for-profit corporate boards of directors.

Restrictions on Public, Non-Profit, and For-Profit Service; No Endorsement of Activities

To avoid a potential conflict of interest you may not, without the approval of the head of the business line, serve on the board or commission of an entity whether public, non-profit, or for-profit, that:

- competes with U.S. Bank;
- is in substantial default to U.S. Bank on a loan, contract or other obligation; or
- is involved in a substantial controversy or litigation with U.S. Bank.

In all cases, management's knowledge and approval of the appointment or candidacy does not imply that you are serving at the direction or desire of U.S. Bank, nor does it imply U.S. Bank's endorsement of the organization or its purposes.

Fiduciary Appointment

You may not accept an appointment or continue to act as a fiduciary or co-fiduciary of any estate, trust, agency, guardianship or custodianship account of a U.S. Bank customer (other than a family member or where a personal relationship exists independent of any business of U.S. Bank such as those between the parents, children, or spouse of a representative of U.S. Bank) unless authorized by Human Resources and the head of the business line or except as appropriate in the regular and proper discharge of your job responsibilities.

Inheritance Under Wills or Trusts

You and your immediate family members may not accept an inheritance from a customer, unless the customer is a family member, or where a personal relationship exists independently of any

business of U.S. Bank, or you have never dealt with the customer as a representative of U.S. Bank. If you have been named as a beneficiary in a prohibited situation, immediately notify your Human Resources generalist and the head of the business line.

Q. A valued customer of U.S. Bank, whose accounts I have handled for many years, wants to leave something in her will for my children. I know I cannot accept these types of gifts, but since they are intended for my children, is that OK?

A. No. You should thank the customer for the offer and inform her that the Code of Ethics prohibits you and your family members from inheriting gifts from customers with whom you have worked as a representative of U.S. Bank, or who are not your family members.

9. Comply with Laws, Regulations and Company Policies

Banking is a highly regulated industry and there are a variety of laws with which U.S. Bank is required to comply. Laws regulating U.S. Bank business include areas such as the Bank Secrecy Act, Anti-Money Laundering, Fair Lending, Foreign Corrupt Practices Act, the U.K Bribery Act of 2010, municipal securities rules including “pay to play” provisions, mutual fund securities, corporate opportunities, inside information and trading in securities, and more. In many cases, U.S. Bank may establish Company policies that exceed the standards required by law.

You are expected to comply with all of the laws, regulations, and Company policies that apply to its business and must ensure you are aware of your individual legal and regulatory responsibilities.

Public Reporting Requirements

Senior officers and directors are responsible for full, fair, accurate, timely, and understandable disclosure in periodic reports required to be filed by the Company with the SEC, the Federal Reserve, and other primary regulators of the Company and its affiliates. In this regard, you must never violate or fail to comply with the Company's established disclosure controls and procedures or accounting rules and controls.

All records, including accounting records, should accurately reflect transactions in a timely manner, and errors must be corrected immediately. Suspected violations of the Company's accounting rules and controls or disclosure obligations should be reported to your manager, Human Resources, the Legal Department, or the Ethics Line. If the instance involves a senior officer or director, report the suspected violation to the Chief Ethics Officer, Chief Risk Officer, Chief Executive Officer, or the Chairman of the Audit Committee of the Board of Directors.

Accuracy of Records

In addition to ensuring that all records are accurate for the purpose of public reporting requirements, you are responsible for ensuring that all documents you complete are accurate. This includes accounting and audit records, loan documents, phone records, transaction records, ATM and Teller balancing, and all other records that are a part of the Company's day-to-day business. The notarization of documents must be in full compliance with notary requirements.

In addition, U.S. Bank complies with all state and federal wages and hours laws. If you are a non-exempt employee, your time records should accurately reflect the times you start and end each work shift, including the meal period and time worked after being called in/paged from off-duty. You may not work hours without recording them, even if you are instructed or feel obligated to do so. Managers must not instruct employees to over- or under-report time worked. It is a violation of Company policy and federal and state wage and hour laws to over- or under-report your time worked, or to report time in a week other than the week in which it was worked. Falsifying documents or failure to maintain accurate records in accordance with U.S. Bank policies and procedures is grounds for disciplinary action, which may include termination.

Q. I worked overtime for several days by working through my lunch. Now my manager has told me to record my regular hours on my time sheet and he will give me some extra time off next week to make up for the lunch hours. What should I do?

A. Even though your manager may mean well, inaccurately recording hours worked is a policy and legal violation. We are each responsible for ensuring that all documents we handle are complete and accurate, including time records. Record your time accurately and report the issue to the Ethics Line or the U.S. Bank Ethics Line Web Form, or to Human Resources.

Notary Public Obligations

If performing duties as a notary public is part of your job duties, you must comply with your business line's requirements as well as state notary requirements, as notary commissions or licenses are issued by the state in which they will be used. Check with your manager or Human Resources generalist if you if have questions, or see the Notary Public page of USBnet for additional information.

Q. A customer recently dropped off some loan documents but he forgot to have them notarized. My co-worker told me I should go ahead and notarize them since we know the customer. Is that acceptable?

A. No. The notary process requires the notarization to occur in person with you, as the Notary, physically present to verify the signing process and the identification of the signer, and to ensure the signer is signing the document voluntarily. Following the specific procedures of your state notary license is absolutely essential even if someone else, including a manager, tells you to ignore them.

Unauthorized "Advice"

Employees are occasionally asked by customers to offer opinions on legal or tax matters. U.S. Bank is legally prohibited from doing anything that can be construed as the unauthorized practice of law.

Compliance with Legal Records Hold Policy

From time to time, you may need to preserve documents due to legal or regulatory obligations or proceedings. It is imperative that you understand and comply with such document retention obligations, which include completing any required training. If you have any questions, review the Legal Records Hold Policy on USBnet, or contact the Legal Department directly with your questions.

Compliance with Anti-Bribery Laws

U.S. Bank strictly complies with all anti-bribery laws, including the Foreign Corrupt Practices Act and the U.K. Bribery Act of 2010. It is essential to our way of doing business to act with the utmost integrity, honesty and transparency. We also require that our business partners adhere to these same principles. Accordingly, all of our employees and business partners are expected to comply with the Foreign Corrupt Practices Act, as well as all other anti-bribery and anti-corruption laws. Employees may not give, promise or offer anything of value 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.

Compliance with Immigration Laws

U.S. Bank strictly complies with all immigration laws and employs only those who are lawfully authorized to work.

Use of Former Employer Information

In connection with your duties as a U.S. Bank employee, do not use or disclose, confidential information, copyrighted information or documents, or trade secrets belonging to a former employer. If you are in possession of documents or electronic media containing such information, you must return it to the former employer.

Prohibited Recordings and Photography

In order to preserve the safety, security, and privacy of our employees and customers, unauthorized recordings of conversations, meetings, etc. and unauthorized photography on U.S. Bank premises are prohibited. Likewise, you may not use camera phones or any other kind of personal recording devices to record workplace communications, including those containing confidential information. For further information regarding appropriate authorized photography, please see the U.S. Bank Policies and Programs Employee Handbook, Photographic Equipment policy. See also Section 3 of this handbook, Information is Bank Property, as well as the U.S. Bank Information Security Policies on this topic for additional information.

Q. My manager holds quarterly meetings that I attend via teleconference. Is it okay for me to record the meeting on my handheld tape recorder so I can create meeting notes for my coworkers?

A. No, unauthorized recording conversations or meetings is prohibited. You may, however, take written notes of the meeting.

10. Exercise Prudent Judgment in Financial Transactions

Financial Responsibility

Your personal financial matters should be handled with prudence at all times. Employee privileges carry the responsibility of prudent use of U.S. Bank products and services, which includes prompt payment for such services, where applicable. In addition, you and your family are prohibited from borrowing money from (or lending money to) customers (other than financial institutions), suppliers, other employees, or independent contractors. This policy is not intended to

keep you from borrowing or lending money to a family member or other individual where a personal relationship exists independently of any business of U.S. Bank. Occasional loans of minimal value (such as for lunch, coffee, or other minor expenditures) between employees will not violate this policy, so long as the interaction is voluntary and no interest is charged.

Q. My co-worker has asked me if she can borrow $75 to pay her utility bill this month. I would consider this a voluntary loan of minimal value, and would not charge interest. Is this OK for me to lend her the money?

A. Unfortunately, no. $75 is not a loan of minimal value as contemplated by the policy. The policy seeks to avoid employee involvement in co-workers' personal financial situations, which can become disruptive to work relationships and create unnecessary distractions in the workplace.

Q. A customer offered to lend me money to buy a boat. I did not ask the customer for a loan. We have discussed and agreed on the terms of the repayment. Is this a problem?

A. Yes. You may not ask for or accept a loan of money from a customer or vendor. A loan is considered to be akin to a gift and may appear to be intended to influence you in the performance of your job. Also, the loan may create the potential for a conflict among your interests, the customer's interests and those of U.S. Bank. Employees in the securities industry are legally prohibited from borrowing from or lending to clients.

Loan and Investment Decisions

Your loan and investment decisions should be made in the most responsible and constructive manner possible, as well as with strict attention to legal and financial implications and in strict accordance with U.S. Bank's credit quality standards.

It is important for you to carefully evaluate the long-term implications of decisions. You must not act on behalf of U.S. Bank in transactions involving people or organizations with which you (or your family) have a financial commitment, interest, or decision-making influence.

Use of inside or confidential information in any personal investment decision is prohibited. It is also a violation of United States securities laws to buy or sell securities on the basis of material inside information that has not been made public, or to provide material inside information to others for their use. Refer to additional U.S. Bank policies in this handbook, including this section, Insider Trading, and Section 3, Protect the Privacy of Customers and Confidential Company Information, for more information. When required by regulation or your business line's policies, you may be required to disclose your personal security holdings and transactions, and/or seek approval prior to engaging in securities transactions. Refer to your business line policies and procedures for further guidance.

U.S. Bank Corporate Credit Card Policy

If you travel or have a business need to incur reimbursable business expenses, you may obtain a U.S. Bank corporate credit card. The corporate credit card should be used for business-related expenses only and may not be used to secure personal cash advances or for personal purchases, except in the case of non-reimbursable personal expenses incurred in the course of business activities that are incidental in nature and where it is not otherwise practical for you to pay for those expenses separately. You must separately itemize such incidental personal expenses on your travel and expense reimbursement form and pay for the personal expense in

full when due. Follow U.S. Bank's guidelines regarding business-related expenses and expense reimbursement procedures.

Submit your expenses in a timely manner and ensure payment on your corporate card account is up to date. Misuse of the corporate credit card, falsification of business expenses, repeated late payments or excessive personal use of the corporate credit card may result in termination of card privileges and/or disciplinary action up to and including termination. If you are terminated, you must pay any outstanding corporate card balance immediately. Where possible, an expense reimbursement may be applied to your outstanding corporate credit card balance.

Q. As long as I pay my corporate VISA off each month, is it all right if I occasionally use the card for personal purchases?

A. No. Your corporate VISA card is strictly for the purpose of charging business-related expenses, except in the case of incidental expenses incurred in the course of business travel (such charges must be paid promptly). Personal expenses should be charged to a personal credit card.

Business-Related Expenses

Falsifying business-related expenses violates this Code. You must follow all guidelines for business-related expenses and expense reimbursement procedures.

Misuse of Accounts and Products

If you misuse an employee checking or other financial account or any other Company product or service, you may lose your account privileges and face consequences of an ethics violation. Examples of misuse of an employee account that may also constitute a violation of U.S. Bank's ethical standards and warrant immediate termination of employment include kiting (the practice of floating funds between two or more different accounts to cover withdrawals) and making false ATM deposits (intentionally depositing empty envelopes) or inflated ATM deposits, to receive immediate cash. U.S. Bank reserves the right to monitor all account activity, including but not limited to accounts held by employees, subject to applicable law, for any reason, including when it appears that use of the account may violate criminal or civil law, violate U.S. Bank policy, or have an adverse effect on U.S. Bank or its employees.

Prohibited Account Transactions

All account transactions must be handled in strict compliance with U.S. Bank policies and procedures. Examples of inappropriate transactions include, but are not limited to, misappropriation of funds; opening, closing or altering accounts without proper authorization; unauthorized transfer of funds; Branch To Branch Cash Transfers without Corporate Security's approval whether the employees uses their personal accounts or branch funds, and transactions that are inconsistent with policies, procedures or practices.

If your job duties include processing customer account transactions such as cashing checks, waiving service fees, approving credit, etc., you may not process or approve any transactions (including paperless or on-line transactions) relating to your own personal accounts, the accounts of immediate family members, or to accounts on which you may have a personal financial interest or on which you are an authorized signer.

“Immediate family members” are defined for purposes of this policy as parent, spouse, common law spouse, domestic partner, child, or sibling, and any such in-laws. This definition includes

biological, step, and foster care relationships, as well as relationships created by adoption.

A "personal financial interest" means an economic interest, including an interest as an owner, partner (active or silent), officer, director, shareholder/stockholder, beneficiary, or holder of debt, a roommate with whom you share housing expenses, or other persons with whom one shares a financial account or interest.

“Transactions” encompass any action taken on an account, including, but not limited to, refunding, reversing or waiving fees; approving or increasing credit lines; cashing checks; opening accounts; transferring, depositing or withdrawing funds; cash advances, performing maintenance on an account, ordering checks, etc., even where you or the family member do not benefit from the transaction.

In addition, you are not eligible for any form of pay that may be available to other customers who experience service problems.

You may be required to comply with other business-line specific restrictions pertaining to any transactions, or any other activity, on personal accounts or the accounts of family members or co-workers, including but not limited to account inquiries or other non-monetary changes to account information. Talk with your manager about specific restrictions and appropriate procedures that apply to your business line and your job.

Q. I am a Banker authorized to waive service fees for customers. If a U.S. Bank employee asks me to waive a service fee on her account, is this acceptable as long as it is consistent with customer procedures?

A. Generally, no. You should talk with your manager or another member of retail management who will process such refunds as appropriate.

Incentive Plans

U.S. Bank's incentive plans provide employees an opportunity to earn financial rewards for performing at their highest level while executing their jobs in the best interests of the shareholders and customers. You may not at any time attempt to circumvent the incentive programs by manipulating records, opening bogus accounts, falsifying applications or otherwise inappropriately reporting or booking business or skewing results to gain incentives or production points.

Furthermore, customer sales must be based on the requests or needs of the customers at all times, as opposed to those that will meet incentive program goals. Behavior intended to circumvent the incentive systems, or to create false results, may be considered an ethical violation.

For more detailed information on incentive plans, refer to your individual incentive plan and/or consult with your manager with any questions.

Q. A co-worker is opening numerous checking accounts with $5 in them for family and co-workers in order to earn the incentives. Is this acceptable? What should I do?

A. No, this is not acceptable and is a serious violation of our ethical standards. Report the violation to either your manager or confidentially to the Ethics Line or U.S. Bank Ethics Line Web Form. Provide as much information as possible, including customer names or other account information, so that a thorough investigation can be conducted.

Insider Trading

U.S. Bank activities frequently result in obtaining material and non-public information – also known as "inside" information – about other companies or about U.S. Bancorp.

Anyone who possesses material non-public information concerning a company or specific securities is prohibited by law from effecting any transactions in that company's securities. This applies to U.S. Bancorp securities as well as the securities of other companies.

Employees, directors, and others may not buy or sell securities of companies with which they have significant dealings on behalf of U.S. Bank or for which they have responsibility on behalf of U.S. Bank. If you believe you may have come into possession of material inside information about U.S. Bancorp, you are strongly encouraged to consult with the Legal Department, who will help you to determine whether a trade would violate U.S. Bank's policy or applicable laws. The definition of "material, non-public" information is broad, and generally means information that a reasonable investor would consider important in making a decision to trade in the securities. It is also illegal to "tip" or pass on inside information to any other person whom you know (or reasonably suspect) might use the information to trade in securities or pass the information on further to someone who may do so.

Q. While at work, I learned that U.S. Bank is about to announce material information that could affect our stock price. I had already been planning to buy some of our stock, since the current price is attractive. Can I go ahead even if the sensitive information has not been publicly disclosed yet?

A. No. Even if you had been planning to buy or sell some stock before you learned of the information, you must now refrain until the information is publicly disclosed. Also, you cannot pass the information to anyone else, or recommend the purchase or sale of our stock to anyone, during this time period.

Q. As part of my job, I work with a large vendor and have learned that the vendor is having serious financial difficulties that have not yet been announced to the public. My sister happens to own some stock in the vendor, which is a publicly traded company, and I want to warn her so she can sell her stock before the bad news comes out. May I tell her?

A. No. If you are in possession of material inside information about any company, you may not pass the information along to anyone else, or buy, sell or recommend the purchase of that company’s securities until the information is publicly disclosed.

Transactions with Affiliated Investment Companies

U.S. Bank complies with all affiliate transaction requirements and self-dealing prohibitions found under Section 17 of the Investment Company Act of 1940 (the Investment Company Act) relating to investment funds advised, underwritten or otherwise affiliated with U.S. Bancorp. All business lines, and particularly business lines that advise, underwrite, administer, act as custodian for, or provide other services to registered investment companies must ensure that transactions involving such companies and any affiliate of U.S. Bancorp are allowable under that section and other laws and regulations. To ensure compliance with Section 17 of the Investment Company Act, U.S. Bancorp has established the 1940 Act Affiliated Transactions Compliance Program and related procedures that apply to all U.S. Bancorp subsidiaries and affiliates, as well as their

employees. You are encouraged to contact Corporate Compliance, the Legal Department, or, if applicable, your own business line's compliance department with any questions or concerns involving affiliate transaction requirements.

Market Timing Trading in the U.S. Bank 401(k) Savings Plan

You may not use U.S. Bank's 401(k) plan as a vehicle for excessive short-term trading of funds, which includes taking advantage of either stale pricing or pricing anomalies in the net asset value of the mutual funds available in the plan. This type of activity is often referred to as market timing trading and causes harm to plan participants as long-term shareholders of mutual funds.

U.S. Bank requires each of the mutual funds available to its 401(k) plan participants to confirm on a regular basis that it remains in compliance with this stated policy on market timing and that it has made no special exceptions to the stated policy except as expressly disclosed to all fund shareholders.

U.S. Bank will cooperate with the mutual funds in which plan participants are permitted to invest by imposing, strictly enforcing and monitoring compliance with the market timing policies that the mutual funds have established to prevent excessive market timing trades. Please review the funds' prospectuses for additional information.

If a participant in U.S. Bank's 401(k) plan is found to be engaged in impermissible market timing activity in one or more of the funds in the plan, prompt action will be taken to curtail such trading, which may involve limiting or canceling the participant's fund exchange privileges.

Antitrust Laws

Antitrust law, known in some countries as "competition law," is an extremely complex area of the law that is intended to protect and promote competition and protect consumers from unfair business arrangements and practices. You may not enter into arrangements with competitors to set or control prices, rates, trade practices or marketing policies, or to allocate markets or customers, and avoid any situation that could give the appearance of doing so. Avoid conversations with competitors regarding pricing, trade practices, marketing policies, or similar unpublished information.

It also is an antitrust violation in many countries and a violation of U.S. Bank policy to require customers to engage in certain "tied" or reciprocal transactions. This is any transaction where a customer is required to purchase or provide one product or service in exchange for another being made available.

You are encouraged to contact Corporate Compliance or the Legal Department when contemplating transactions involving multiple products and services. You may also review the Company's Anti-Tying policy, available from the Corporate Risk Management page of USBnet.

11. Use Company Resources as Intended

Company Resources

In order to perform your job duties, you may be assigned workspace, equipment or other company resources or property. For purposes of this policy "Company resources" includes but is not limited to: U.S. Bank-owned email systems, text messaging and instant message devices, telephones and cell phones, personal digital assistants (PDAs) such as a Blackberry or IPhone®, and tablet devices such as an iPad®, as well as portable electronic media (PEM), pagers,

voicemail systems, computers, copy and fax machines, supplies, mail service, email, Sharepoint, team rooms, Quickr or other internal collaborative Intranet-hosted sites such as US Place, Company supported external social networking sites, Internet access, bulletin boards, and conference rooms. In addition, if you are authorized to use any personal devices to conduct Company business, your business use of such devices must comply with the policies contained in this Code.

Company resources are intended primarily for Company business. Personal use of these or other company resources can disrupt the vital flow of information or tie up resources on which the Company and its customers depend. You may, however, make occasional, inconsequential personal use of Bank systems, provided that it is not unreasonable and does not interfere with business use, consume system resources, or violate any U.S. Bank policy. Personal telephone calls should be limited, and Company addresses, mail, or email should not be regularly used for personal correspondence. See also Section 3 of this handbook, Protect the Privacy of Customers and Confidential Company Information.

You may not use Company resources to conduct outside business activities, to engage in unethical or illegal activities such as gambling, or to gain access to, transmit, or store material that is offensive or that in any way violates Bank policies for maintaining a respectful, harassment-free work environment. Even where access to a particular Internet site is not blocked by the Bank's Web-filtering tools, you may not visit sites that otherwise violate Company policies.

Excessive use of personal cell phones and text messaging devices for personal reasons during work time can reduce employee productivity and be distracting to others. You are expected to refrain from excessive use of personal devices during work time. You also are responsible for knowing and complying with any business line policies or guidance relating to use and/or possession of personal cell phones and text messaging devices in the workplace, which may include additional restrictions or controls on such activity.

Misuse or abuse of Company resources, including inappropriate or excessive access to and use of the Internet, is a violation of Company policies. Company resources assigned to you during the course of your employment must be returned at the request of U.S. Bank or when your employment ends.

Q. Sometimes I need to fax information to my child's school. Is it okay to use a Company fax machine?

A. Occasional personal use of a Company fax machine is okay, as long as the number of pages is not excessive and the time to transmit the fax does not unduly interfere with business. If you are unsure, check with your manager.

U.S. Bank Technology

Technology, including computer hardware and software, is an important asset for U.S. Bank and its customers. Leading-edge technology is a significant component of the services U.S. Bank provides to its customers. The U.S. Bank Information Security Policies on USBnet, provide direction for using technology and identify precautions that should be taken to secure data from unauthorized access. If you use U.S. Bank's technology resources, you are expected to be familiar with and understand these documents and ethical standards and comply with their provisions. Also, refer to Section 3 of this handbook, Protect the Privacy of Customers and Confidential Company Information.

Q. I purchased some software for personal use that would be helpful to me at work. May I load it on my PC at work?

A. No. This is a violation of U.S. Bank Information Security policies. If you need to add software to your computer, submit a Production Service Request (PSR) at http://psr.us.bank-dns.com/.

You may not use Company trademarks or logos for any purpose, including registering a domain name for business purposes, without written authorization from Corporate Marketing or the Internet Channel group and the Legal Department (see also guidance under Section 12 of this handbook, Public Statements on Behalf of U.S. Bank and Online Social Media and Other External Communications. Please contact the Portfolio Management Services in the Quality Assurance Group of Technology Services for information on registering new domain names.

Business Communications and Records

Conduct all verbal and written business communications professionally and in compliance with U.S. Bank's ethical standards. What you say, write, and do should reflect a clear understanding of U.S. Bank's ethical values and expectations and should demonstrate sound personal judgment. Be clear, truthful, accurate, and respectful. Always avoid exaggeration, colorful language, guesswork, legal speculation, and derogatory remarks or characterizations of people, companies or their products and services. What you say, write, or do should preserve or enhance U.S. Bank's integrity and reputation – it should never jeopardize it.

This policy applies to communications of all kinds, including informal notes and memos, telephone conversations, as well as communications using company resources as described earlier in this section. See also the Communications Guidelines on USBnet.

Your communications may also be subject to the U.S. Bank Information Security Policies, guidelines contained in Section 12 of this handbook - Public Statements on Behalf of U.S. Bank and Online Social Media and Other External Communications, the USBnet Terms and Conditions, and any applicable Intranet-hosted site Collaboration Policy guidelines.

Email Use

Email is an important form of internal and external communication. Emails are written records that may be required to be disclosed in legal proceedings or otherwise made public. U.S. Bank's ethical standards apply to every email you create – no matter how informal its intent. Never create or send an email using Company resources or personal devices used for business purposes if it does not first pass the scrutiny of U.S. Bank's ethical standards. These standards apply to all other forms of communication as well, including voicemail and memos.

All emails should be created with the understanding that they may be formal records and should be written in a professional tone. The transmission of all messages must comply with all policies and be protected from unauthorized disclosure or access. For specific information on communication tips and guidelines, see Communication Guidelines on USBnet.

The standards for safeguarding information and information security also apply to email communications. Because email messages sent outside the Company via public networks, such as the Internet, may be intercepted or misdirected, take great care not to include information that may be used to harm U.S. Bank, its customers, its employees, or any of its other stakeholders. When business needs require that you communicate with external parties using email containing U.S. Bank Confidential or Customer Confidential information, use U.S. Bank's secure (encrypted) email facility using the "Key123" function.

If a customer emails a service request containing personal information or account numbers, remove this information from your email reply. This will reduce the risk of exposure of U.S. Bank Customer Confidential information. For further information on email security requirements, see the Information Security Standard on Email on USBnet.

Q. Can I send an email that contains U.S. Bank Confidential or Customer Confidential Information outside of the Company to one of my vendors?

A. Once you have confirmed who the recipient is, that he/she is authorized to receive the information, and that there is a business need to share the information, you may email U.S. Bank Confidential or Customer Confidential Information outside the Company. Be sure to select the "Send Secure (Key123)" button or enter "key123" into the subject line of the email, ensure you have the correct email address, and limit the information you send to only what the authorized recipient needs. Don't send information the recipient should already have such as an account number or a social security number.

Soliciting During Work

Solicitation during working time for products, services, charities or interests not related to Company business can have a negative impact on U.S. Bank's ability to serve its customers and can be disruptive to internal workflow. For this reason, U.S. Bank prohibits any solicitation of employees by other employees and non-employees during work time, regardless of the reason or cause, i.e., whether it is for participation in volunteer agencies, the sale of goods or services, requests from customers, or contributions to a charitable organization unless it is for a Company-sponsored charitable fundraising or business-related event. In addition, business customers or other third parties are not allowed to post, advertise, or otherwise solicit for business or other activities at any U.S. Bank sites.

Q. A coworker came to my desk to ask me for a donation to disaster relief sponsored by an outside organization. Is that okay?

A. No. Employees may not solicit other employees for contributions to charitable organizations or any other fundraising efforts, such as charitable walk-a-thons, during work time as it can disrupt workflow and reduce our ability to serve our customers. The only exception is for Company-sponsored charitable fundraising or business-related events.

"Work time" is defined as time spent in the performance of job duties. Even if you are not on work time, you may not solicit employees who are on work time. Additionally, you may not use Company resources such as email or voicemail for unauthorized solicitation, or post or distribute pamphlets, leaflets, emails, or other literature in work areas or on Company bulletin boards. The only exceptions to this policy are Company-sponsored, charitable fundraising or business-related events (i.e. United Way or Development Network) which require Senior Management and Human Resources approval.

Q. A local business owner approached one of our branches with flyers advertising his used car business and asked if it was okay to leave them in the branch lobby for our customers. Is this permissible?

A. No. U.S. Bank prohibits business customers or other third parties from advertising or otherwise soliciting U.S. Bank employees and customers at U.S. Bank sites.

Monitoring Use of Company Resources

As discussed earlier in this section, U.S. Bank may assign Company resources to you for use in performing your job. You should be aware that there is no expectation of privacy in your use of Company Resources and systems, whether the use is for business or personal reasons, and U.S. Bank reserves the right to access and search workspace and equipment that has been assigned to you and to conduct reasonable surveillance of activities on Company premises based on business needs, subject to applicable law. In addition, equipment owned by employees but used for U.S. Bank business purposes, such as cell phones, text messaging devices, personal digital assistants (PDAs), or personal computers, is not considered private and may be accessed and -searched for any business-related purpose, subject to applicable law. Communications transmitted to and/or stored by a third-party vendor are also subject to monitoring and access by the Company and may be disclosed to the Company by the third-party vendor, subject to applicable law.

U.S. Bank also reserves the right, subject to applicable law, to monitor electronic records and activities associated with usage of employees' systems accounts (user IDs); such usage includes electronic forms of communication (such as email, text messaging, instant messaging (IM), telephones and cell phones, personal digital assistants (PDAs) such as Blackberries, pagers, voicemail, and other communications systems), other computer systems, and any other electronic records and activity for any reason. U.S. Bank may ask employees to consent to the disclosure of electronic communications stored at a third-party service provider or on a personal electronic device used to conduct U.S. Bank business, and their failure to do so could result in discipline for failure to cooperate in a Company investigation.

U.S. Bank may monitor your email for any reason, including when it appears that use of a system violates criminal or civil law, violates U.S. Bank policy, or may have an adverse effect on U.S. Bank or its employees. Examples include, but are not limited to, emails containing sexual innuendo or other inappropriate or offensive jokes; chain letters; downloading, copying or sending confidential information to an unauthorized party; excessive or unauthorized personal use that violates Company policy; or other use that may be harmful to U.S. Bank or its stakeholders.

All information sent, received or viewed on the Internet, including non-business emails, emails transmitted through a personal e-mail, Web-based communications, instant messages, text messages or other forms of communication, can be stored on a computer’s hard drive, the Company’s servers, or any component of the network, etc. and can be reviewed and retrieved by the Company at any time. In addition, back-up copies of electronic communications may exist, even if they have been deleted from the computer.

Additional Information

See "Logging and Monitoring of Personnel Use of Information Systems" and "Representation on the Internet and Other External Networks" in the U.S. Bank Information Security Policies on USBnet for more information.

Employee Consent and Agreement

By certifying your compliance with the U.S. Bank Code of Ethics and Business Conduct as a new employee and annually thereafter, you consent to the monitoring of activities as described in this section, and consent and agree to the disclosure of communications transmitted or stored by a third-party vendor on behalf of the Company. If you use employee-owned equipment for business purposes, you agree to the disclosure of such communications stored by a third-party vendor on your behalf where a business purposes exists as determined by the Company.

Q. I heard that my email and Internet access are being monitored. Is that true?

A. Yes. Email and Internet access are property of U.S. Bank and may be monitored, even if you conduct personal activity via password protected personal Internet sites using U.S. Bank equipment or systems. We are able to mitigate organizational risk caused by misuse of technology through monitoring of these resources.

12. Exercise Discretion in Public and Political Activities

Media Relations

We are committed to building and maintaining effective and ongoing communications with our key stakeholders through the media. Effective media relations also ensure that U.S. Bank's public statements express a clear and factual representation of the Company. To this end, all media inquiries should be forwarded to Media Relations and only Media Relations is authorized to initiate contact with the media. Certain exceptions to this policy may be granted in writing by the CFO.

Public Statements on Behalf of U.S. Bank

All public statements on behalf of U.S. Bank must be accurate and consistent. Only authorized spokespersons may communicate on behalf of the Company and its policies, practices and procedures in any media including online forums, bulletin or message boards, chat rooms, blogs or other Internet facilities. Exceptions to this policy, such as for systems staff participation in technology forums, require management authorization and are subject to policies governing sharing of U.S. Bank Confidential information. In addition, comments by employees about U.S. Bank made in a personal capacity must adhere to all applicable Company policies and Social Media Guidelines, as discussed below.

Online Social Media and Other External Communications

Online social media is a growing method of communicating and doing business. You may have questions about how participating in social media relates to your work environment or job — or what's appropriate. For purposes of this policy, "online social media" includes but is not limited to online forums, bulletin or message boards, chat rooms, blogs, social networking, wikis, Facebook®, MySpace®, LinkedIn®, Twitter®, Company–sponsored sites, etc. Since online social media tools are rapidly evolving, we want you to be aware of how your use of social media may impact your work, our Company's reputation, and may even violate the law.

Personal Social Media Activities

U.S. Bank believes that, used responsibly, online social media activity can be a vehicle that drives organizational and individual development through information sharing and collaboration. U.S. Bank respects the legal rights of its employees, and understands that employees' time outside of work is their own. However, online social media activity, whether done in or outside of work, may affect your job performance, the performance of other U.S. Bank employees, and the business interests of U.S. Bank as a whole. As such, online social media activity is a legitimate focus or Company policy. If you communicate about U.S. Bank externally using online social media, you must comply with the guidelines described below, the U.S. Bank Information Security Policies and applicable policies contained in the U.S. Bank Policies and Programs Employee Handbook on USBnet.

Authorized Business Activities Using Online Social Media

You must be explicitly authorized by appropriate management to conduct business for U.S. Bank using online social media, such as Facebook®, MySpace®, Twitter®, YouTube®, and LinkedIn®.

Prior to engaging in any business activities using online social media, all new initiatives related to social media and emerging communications must be assessed by the Collaboration & Social Media Policy Group (CSMPG)and approved as follows:

- Authorization requires approval by business line management, senior business line risk management, Enterprise Revenue Office (ERO), Corporate Marketing, and may also include approval by U.S. Bancorp Media Relations, or other risk or management groups. Consistent with existing corporate policies and processes, management authorization may include prior review and approval through the Business Change Assessment (BCRA) process. See USBnet for the BCRA policy, process, and submission forms.
- Content that is posted on social media sites about U.S. Bank's products and services may be viewed as marketing or advertising. In addition to the approvals referenced above, content must be reviewed and approved by business line management, business line risk management, Corporate Marketing, and must be submitted through the Marketing Material and Web site Review (MMWR) process. Business lines must also have established processes to review and approve content and is responsible for the legal, compliance and reputation risk associated with such materials. See USBnet for information about the MMWR process, including the MMWR policy, MMWR procedure and MMWR submission form.
- You are expected to comply with the U.S. Bank Code of Ethics and Business Conduct, the U.S. Bank Information Security Policies, and any other applicable business line, risk management, legal, or compliance policies related to your business activities and online social media use.

Social Media Guidelines for Bank Business and Personal Use

The following principles apply to all of your external communications using online social media and in other external communications, whether personal or business-related, including activities on behalf of the U.S. Bank and on Bank-sponsored sites. Nothing in this section of the Code is intended to improperly limit or interfere with non-management employees discussing the terms and conditions of their employment.

- **Personal responsibility.** You are personally responsible for the content you publish or communicate externally and in all online activities. Online social media is generally considered public and once posted, information may exist indefinitely on the Internet. Use good judgment and post at your own risk.
- **Respect.** Respect your audience and avoid offensive language, ethnic slurs, personal insults, obscenity, or any conduct that would not be acceptable in U.S. Bank's workplace.

- **Monitoring.** In circumstances deemed appropriate, U.S. Bank monitors online social media postings to the fullest extent permitted by applicable law, Internet usage, email use, and other forms of online social media, and may take disciplinary action where violations of policy occur.
- **Confidential information.** You may not disclose U.S. Bank Internal, Confidential or Customer information. See U.S. Bank Classification and Handling Standards on USBnet.
- **Comply with all other Company polices.** When using online social media, you are expected to comply with the guidelines in this Code, the U.S. Bank Information Security Policies, and policies contained in the U.S. Bank Policies and Programs Employee Handbook on USBnet.
- **Follow business line-specific rules.** Your business line or work group may have additional policies or rules regarding use of online social media and you are responsible for knowing and complying with all such policies.
- **Use of personal online social media tools for U.S. Bank business.** Similar to television, print, and radio advertising, social media is subject to a number of regulatory and business-related restrictions. Therefore, unless specifically authorized by Corporate Marketing and appropriate management, you may not use any personal online social media accounts or platforms (such as Facebook®, Twitter®, LinkedIn®, YouTube®, etc.) to conduct U.S. Bank business, including advertising, soliciting, and communicating in a business capacity. Examples of inappropriate activities include:
    - Twitter® post – “Great rates on Home Equity Loans and Lines, see me at 123 Main Street Office!”
    - Facebook® post – “First 100 customers to open a U.S. Bank checking or savings account with me at the Elm Street Branch will receive a $10 gift card…”
    - YouTube® personal video advertisement about your branch or your sales opportunities; video shot on U.S. Bank premises; spoof video about U.S. Bank on U.S. Bank non-public premises that shares non-public confidential information
    - LinkedIn® post advertising products, rates, campaigns or U.S. Bank; commenting on U.S. Bank business strategies or policies
    - “Friending” U.S. Bank customers on personal Facebook® sites for the purpose of conducting U.S. Bank business.

  Check with your manager first if you are not sure whether your use of personal online social media would be considered prohibited business conduct or otherwise inappropriate under the Code of Ethics.

- **Disclosure requirements for endorsements of U.S. Bank or U.S. Bank products and services; third party partners.** Federal regulations require you to disclose that you are a U.S. Bank employee if you make a recommendation or endorse U.S. Bank or its products or services. Similarly, if you make a recommendation or endorse a third-party partner of U.S. Bank, you must disclose that you are a U.S. Bank employee and that U.S. Bank has a marketing partner relationship/joint venture relationship with that Company. This requirement applies in any form of media, including public online forums and social media and applies to employees’ posts on any official U.S. Bank online sites. It is not sufficient disclosure to simply list your employer on your website, blog site, or personal social media platform (such as Facebook®). Examples of appropriate disclosures include:
    - "Hey everybody, I work at U.S. Bank, and I’m just sharing this link to a story in Kiplinger’s Magazine, rating the FlexPerks credit card No. 1 for travel perks, click here."
    - “I love working and banking at U.S. Bank! My Main Street Branch rocks!”
    - “I work at U.S. Bank at 123 Birch Street Branch has the best customer service.”

- "I give Syncada my highest recommendation. They have state of the art technology and world class service that can support all your fleet transportation needs. I am a U.S. Bank employee and Syncada is a joint venture between VISA and U.S. Bank to offer global supply chain management services."

This disclosure requirement does not apply to anonymous "Like" or 'Approve" buttons in online social media platforms.

- **Stating an opinion on topics related to U.S. Bank or the financial services industry.** If you identify yourself in any social media platform as an employee of U.S. Bank and comment in your personal capacity on topics relating to U.S. Bank or the financial services industry, you must make clear that your views and positions are not those of the Company (unless you are specifically authorized to speak on behalf of the Company). An example of an appropriate disclaimer is:
  - You post the following comment on a discussion forum for homebuyers: "I'm a broker at U.S. Bank, and I'm optimistic the government is going to increase the tax credit for first-time buyers next year." In parentheses after the comment, your disclaimer could say: "I'm speaking for myself only, not for my employer."

  Some topics, even if appropriately disclaimed, would be inappropriate for commenting in a public forum, for example:
  - You post a comment on your personal blog saying "There was a fire at our branch office. All our documents are destroyed. Looks like we will be shut down for weeks. I am speaking for myself and not for U.S. Bank." This would be inappropriate because information about a branch closing should be handled by Media Relations. Comments like these may cause customer anxiety and confusion, and it may appear that you are an authorized spokesperson for the Bank. In addition, the comments inappropriately disclose non-public confidential information about the condition of Bank documents.
- **Honesty.** Statements regarding the Company and its products or services must be honest and reflect the writer's experience or opinions.
- **FINRA-governed employees are prohibited from making covered communications on social media.** FINRA has made clear that social media communications are considered the same as in-person or written communications, and as a result, must adhere to FINRA regulations, and content must be monitored, disclosed, archived and discoverable. If you are employed in a FINRA-governed department, you are responsible for complying with all applicable business line policies and regulations relating to use of online social media.
- **Non-public photographs or images of bank premises, processes, employees, or customers may not be posted on online social media sites, platforms or image/file sharing sites.** For purposes of the security of our employees and customers, you may not post any photographs or images, including video, of non-public U.S. Bank premises, processes, employees or customers without their consent and the consent of the Company, on any of your personal online social media accounts or platforms in any circumstance. This includes photo sharing sites such as Flickr, See also Section 9 of this handbook, Prohibited Recordings and Photography.
- **U.S. Bank logos and trademarks.** Unless otherwise authorized, you may not use U.S. Bank logos or trademarks, or proprietary graphics and must respect copyright, privacy, fair use, financial disclosure, and other applicable laws.
- **Media Relations.** If a member of the news media or blogger contacts you about an Internet posting that concerns the business of U.S. Bank, please refer that person to U.S. Bank's Media Relations department.

- **Comply with laws.** Be mindful not to engage in any unlawful conduct, such as invasion of privacy, violations of security laws, defamation, etc.
- **Comments about company performance.** Because you are a bank employee, people may think you know more about the Company's performance or than you actually do, and buy or sell shares of Company stock or create rumors in the market based on your opinions about the Company. To be safe, avoid all statements, including personal opinions, about the Company's future performance, worth, or share price (unless you are specifically authorized by the Company to make such statements).

If you are uncertain about whether your use of online social media and other external communications comply with this policy, consult with Human Resources or your manager. Failure to follow all applicable policies may result in disciplinary action up to and including termination. Please review the U.S. Bank Information Security Policies, available on USBnet.

Acting as an Expert

The expertise you develop in the course of your employment may provide opportunities to participate in outside activities as a paid or unpaid speaker or consultant. Discuss these opportunities with your manager or supervisor to ensure there is no conflict between organizational and personal interests. Use or distribution of materials or products developed as part of your responsibilities with U.S. Bank should occur only with the authorization of your manager or supervisor.

Political Activities

U.S. Bank is an active participant in the public policy arena. Whether legislative activity occurs in Washington, D.C., or in one of the states in U.S. Bank's United States footprint, it may affect the way the Company does business or serves its customers. As an employee, you are encouraged to be knowledgeable and active regarding state and federal legislative issues affecting the financial industry.

In any jurisdiction, if you interact with any government official or employee on behalf of the Company, you must ensure the contact complies with all legal requirements. Federal, state, and local laws govern all aspects of working with public officials. For example, the federal government requires lobbyist registrations and reports. Also, if you are involved in business relationships with government entities, you may be subject to lobbying laws in some jurisdictions. Lobbying activity generally includes attempts to influence the passage or defeat of legislation. The U.S. Government and many states, however, have extended the definition of lobbying activity to cover efforts to influence formal rulemaking by executive branch agencies or other official actions of agencies, including the decision to enter into a contract or other financial arrangement. In addition, even if you do not have direct contact with the government official, in certain circumstances the assistance you provide an employee who does lobby a government official can also count as lobbying activity. Moreover, "grassroots" activity (where one communicates with the public or segment of the public, such as U.S. Bank employees, encouraging them to call their representative or another public official for the purpose of influencing the passage of legislation or a rulemaking) is in many cases also considered lobbying activity.

To ensure that U.S. Bank and its employees are in compliance with these laws, you may not engage in any of the lobbying activities, as described above, on behalf of U.S. Bank without prior approval from Government Relations and must be in full compliance with applicable federal, state, and local laws. To ensure compliance with applicable laws and regulations, contact Government Relations concerning any activities that might be considered lobbying.

Activity with the U.S. Bancorp Political Participation Program

U.S. Bancorp's employee federal political action committee (PAC), the U.S. Bancorp Political Participation Program, was created to encourage employee involvement in political activities and contributions in the United States. Employees who are eligible to participate in the PAC are invited to join. Using the program's evaluation criteria, the PAC Board determines whether the PAC will make a political contribution to a candidate. Participation is completely voluntary. Employees have the right to refuse to contribute without reprisal. For more information, please contact Government Relations.

Political Contributions

Federal and state laws, and the laws of many countries, govern political contributions, including monetary contributions (e.g., in the form of a corporate check or a purchase of tickets to a political fundraiser) as well as "in-kind" contributions (e.g., the use of corporate personnel or facilities, or payment for services). In the United States, federal law prohibits a national bank from making a contribution or expenditure in connection with any election to any political office, including local, state, or federal offices. The Federal Election Commission enforces federal law and regulations governing federal political contributions. Other federal regulations, such as Municipal Securities Rulemaking Board Rule G-37, also apply to political contributions within the financial services industry, including personal contributions made by certain employees. Each state also has its own laws and regulations governing political giving to state and local candidates and issues.

U.S. Bank or the U.S. Bancorp Political Participation Program or the U.S. Bancorp Federal PAC, submits compliance reports to several jurisdictions regarding these requirements. To ensure compliance with applicable laws and regulations, you must comply with the following requirements:

- Any proposed political contribution or expense incurred by U.S. Bank on behalf of any candidate, campaign, political party, political committee (e.g., a PAC or ballot measure committee), or any entity exempt from federal income taxes under Section 527 of the Internal Revenue Code must be approved in advance by Government Relations.
- No corporate assets, funds, facilities, or personnel may be used to benefit any candidate, campaign, political party, or political committee (e.g., a PAC or ballot measure committee), or any entity exempt from federal income taxes under Section 527 of the Internal Revenue Code without advance approval by Government Relations.
- No one at U.S. Bank may make a political contribution to obtain or retain business or to obtain any other improper advantage.
- No one at U.S. Bank may use or threaten force or reprisal against an employee to contribute to, support, or oppose any political group or candidate.
- Some federal, state and local laws contain prohibitions on certain employees from making political contributions if their employer (i.e., U.S. Bank) is seeking to be, or has been, selected to provide services or enter into a contract with a governmental entity. To ensure compliance with these laws, contributions must be approved in advance by the Legal Department.

U.S. Bank maintains two federal PACs, the U.S. Bancorp Political Participation Program and the U.S. Bancorp Federal PAC, which make contributions at the federal and state level where allowed. Nothing in this policy is intended to prohibit the activities of that PAC or the ability of eligible employees to participate in the PAC.

Gifts and Entertainment of Public Officials

If you are involved in business relationships with government entities, you may be subject to gift laws. Any type of gift to a public official is subject to legal restrictions or prohibitions in some

jurisdictions. Moreover, certain gifts to public officials may have to be reported by the Company. The Executive Branch of the Federal Government, the U.S. Senate and House of Representatives, the various states, and certain local jurisdictions each have separate gift laws restricting gifts (e.g., meals, entertainment, transportation, lodging, and gift items) that may be provided to their officials and employees. Additionally, offering or giving anything of value to any foreign government official is severely restricted under anti-bribery laws including the Foreign Corrupt Practices Act. To comply with these laws, you must obtain pre-clearance from the Legal Department before providing any gift, meal, entertainment, or anything else of value to a government official or employee.

In addition, you must comply with the Foreign Corrupt Practices act as well as all other anti-bribery and anti-corruption laws. Please see Section 9 of this Code under Compliance with Anti-Bribery Laws for additional information about complying with these laws.

Political Representations

You are free to express your political views, support candidates of your choice, run for elective office, or serve in an elective or government-appointed office on your own time and at your own expense. However, as noted above, political contributions to certain candidates by certain employees may be subject to special restrictions and must be pre-cleared. You may serve in an elective or government-appointed office as long as it does not interfere with job performance or service as a director, use Company time or resources, or present a conflict of interest. However, if you serve in an elective or government-appointed office or participate in a personal political activity, you may not indicate in any way that you are representing U.S. Bank.