TCF Online Privacy and Security Policy

Effective Date 5/29/2015

At TCF Bank and its banking and non-banking affiliates and subsidiaries ("we," "us," "our," and "TCF"), we know that your financial information is important to you. We remain committed to protecting the privacy of that information. This Online Privacy and Security Policy describes how TCF treats information that you provide or that we collect through a) our website(s) and TCF-branded social media sites or pages ("Site"), or b) any of our online or mobile banking services and applications ("Online Services"). By using the Site or Online Services, you agree to all the terms of this Policy.

Respecting Your Privacy

Types of Information We Collect

When you visit and browse the Site or Online Services, we are able to collect information that could be reasonably used to indirectly identify you individually, such as your physical location, the device you are using and the Internet Service Provider (ISP) you are using. We can also record the date, time, and pages visited while you are at our site and the type of web browser and operating system you use. We do this to determine how individuals use our Site so that we can enhance the individual user's experience and make the Site more useful for our customers and potential customers.

When you request information or make an application for, or use, the Online Services, we collect personally identifiable information that you provide to us directly, such as by completing an online form, application, field, or survey. "Personally Identifiable Information" or "PII" means information that directly identifies you, or can be used to directly identify you, individually. Examples of PII may include your name, physical address, email address, telephone number, social security number, date of birth, or account information. If you are enrolled for the Online Services, you can review and make changes to your online account preferences, personal preferences, or email address by signing in to TCF Online Banking and clicking on "Preferences."

We may also collect information to help us understand your financial needs so that we can offer you products and services. For example, if we know that you own a home, we may offer you a home equity loan. We do this by collecting identifying information (such as your name and address), information from your application (such as your assets), transaction information (such as your loan repayment history) and information to comply with applicable laws and regulations. We may also collect information to design new products or services, or modify existing products or services, in order to meet the needs of our customers.

When you use the Online Services, you also may be required to enter information we believe is necessary to safely process your transactions, such as your online banking Login ID and password.

How We Use Your Information

We may use your personally identifiable information to, among other things:

- Open an account for you, enroll you for Online Services, or complete your transactions;
- Respond to your requests for information and otherwise communicate with you;
- Provide you with information about products and services that we, or third parties with whom we do business, offer or make available;
- Send you notices or alerts concerning your account or account transactions;
- Detect and prevent activities that may violate our policies or be illegal; and
- Comply with our legal and regulatory obligations.

We may also use aggregate personally identifiable information from you and other users of the Site and Online Services to develop and implement marketing strategies, improve our current products and services and develop new ones, and enhance the Site and Online Services.

We may share your personally identifiable information as described in the TCF Privacy Policy, which you can access at tcfbank.com by clicking on the Customer Service tab and clicking the link under the Disclosures and Agreements heading. The TCF Privacy Policy applies to online and offline information we collect only for accounts intended to be used primarily for personal, family or household purposes. The TCF Privacy Policy also describes how you can prevent TCF from sharing certain personally identifiable information, or "opt-out."

We may also use information that we collect through the Site and Online Services to optimize and improve user experiences when using the services, as further described below under "Online Tracking."

Online Tracking

We and our service providers may collect information about your usage of the Online Services and other Internet activities using tracking technologies, including but not limited to:

- **Browser Cookies** – HTML, or "browser" cookies are small text files stored directly on your device. They allow us to recognize your device and store user preferences for when you return to our website. Cookies may be temporary, called "session cookies." Session cookies expire at the end of your browsing session or within 24 hours. Or they may stay on your device for longer periods until their expiration date, called "persistent cookies." Cookies may be used to collect information about your Internet service provider, Internet protocol (IP) address,

Internet browser and operating system, the time spent using the Online Services, the Site or applications you visit, account preferences, and other non-personally identifiable information. The Online Services do not use cookies to capture your unencrypted personally identifiable information.

- **Flash Cookies** – Similar to browser cookies, local shared objects, or "flash cookies," are also used to recognize your device and store user preferences for when you return to our website. Flash cookies can be shared across browsers on the same device.
- **Pixel Tags** – Pixel tags, also called web Beacons or clear GIF's, and similar technologies are typically small blocks of code embedded in images shown in the Online Services or certain e-mails we send you. They may involve the transmission of information directly to us or to third parties on our behalf. We may use these technologies to bring together information we collect about you.
- **Location Tracking** – Certain applications may transmit information to us about your location when you request information from them.

We may use cookies and other tracking technology to:

- Help us maintain security and verify your information when using the Online Services as you navigate from page to page. This enables you to avoid having to re-enter your information each time you enter a new page.
- Help us recognize you as a unique user when you return to use the Online Services so that you do not have to re-enter your information multiple times as you move between our pages or services.
- Remember your preference settings when using the Online Services.
- Optimize your usage of the Site and//or Online Services, for example, by recognizing if your browser supports specific technology features.
- Otherwise enhance and personalize your experience when using the Site and/or Online Services.
- Enable us, and third parties with whom we do business, to tailor advertising and promotional activities to products and services that may be of interest to you.
- Collect and compile aggregated information for statistical and evaluation purposes to help us understand how the Online Services are used. This helps us enhance the Online Services, enhance other products and services and develop new ones, and develop marketing and promotion strategies.

You have the ability to disable browser cookies, generally by changing your Internet software browsing settings. It may also be possible to configure your browser to accept specific browser cookies or to notify you each time a new cookie is about to be stored on your device, thereby enabling you to decide whether to accept or reject the cookie. Changing your browser settings does not disable flash cookies. However, you can disable or delete the data stored by flash cookies or similar technologies by managing your browser's "add-on settings" or visiting the manufacturer's website. If you refuse cookies, you will not have access to many features that make your user experience more efficient and some of the Online Services will not function properly.

E-mail

If you provide your e-mail address to us, or if we obtain it from another source, we may use it to respond to or update you on your inquiries, to contact you about your accounts or to let you know about products and services that may be available to you. If we send you an e-mail, the primary purpose of which is for advertisement or promotional purposes, it will include instructions on how to opt-out of receiving such e-mails in the future. If you elect to opt-out of receiving e-mail advertisements and promotions, we may still send you e-mails about your account relationships with us.

Linked Websites

The Site and Online Services may contain links to third-party websites owned or controlled by third parties not affiliated with TCF. Some of these sites may share a similar "look and feel" to TCF's website. The privacy policies applicable to your use of those websites are determined by the third party, and not TCF. TCF is not responsible for the privacy or security of those websites. We encourage you to read the privacy policies provided by other websites before you provide personal information to them.

Children's Privacy

We do not use the Site or Online Services to knowingly solicit data from or market to children under the age of thirteen without parental consent. Parents or guardians who become aware that their child has provided us with information without their consent should promptly contact us and we will delete the information from our files. For additional information regarding the Children's Online Privacy Protection Act ("COPPA"), please visit the Federal Trade Commission's website at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy.

Access to Customer Information

TCF has policies and procedures intended to reasonably protect your customer information from illegal access or use.

TCF emphasizes to employees the importance of maintaining the confidentiality of customer information. We do so through staff training, day-to- day management and enforcement of TCF's Code of Ethics. Employees are expected to follow our confidentiality standards. Disciplinary measures are taken when appropriate to enforce these standards.

We review these policies and procedures on an ongoing basis and work to update them as needed to accommodate changing business environments and new products and services.

Protection Against Inappropriate Use Of Customer Information

To help protect you, TCF may gather and ask for certain information, so that we can identify you as a legitimate account holder when transacting

business. We may request identifying information, such as a social security number, account number, or ask you for identification, such as your driver's license to help guard against unauthorized use of your account.

System Security to Protect Customer Privacy

TCF maintains system security to help protect against any unauthorized access to customer information. These systems are intended to reasonably guard against unauthorized access and use of customer information by unauthorized individuals. TCF works to upgrade these practices and procedures on an ongoing basis.

Sharing of Information Within TCF

We share information with other TCF companies. In doing so, we follow all TCF security standards and policies, as well as any applicable laws or regulations regarding the sharing of such information.

Sharing of Information With Third Parties

TCF may share some information about our customers with other companies. We also share information when necessary to protect against fraud or other financial abuse, or in connection with credit reporting. TCF may also release information about you or your account, or transactions involving your account, to third parties if it is necessary to complete a transaction, or to verify the existence of the account or availability of funds for a third party. We may also provide information to law enforcement or other government agencies or to another third party (for example, in response to a subpoena) when legally required to do so. We also sometimes contract with outside agents or service providers to print checks, provide audit services, enter or calculate transactions and balances, or provide other materials or services on our behalf. We will seek to make sure that these agents, service providers, and third-party product providers agree to safeguard our information about you, your products and services with us, and to abide by applicable law.

We also occasionally decide to sell business assets or a business line, such as mortgage servicing rights. In these cases, we may transfer to the purchaser the related customer information. There may be other circumstances where it becomes necessary to disclose information in order to conduct our business.

To assist in offering you new products and services of interest you, TCF sometimes provides customer information to parties outside TCF. Of course, you may accept or decline any of these product offerings, with no impact to your relationship with TCF.

Maintaining Accurate Customer Information

Maintaining accurate customer information is as important to us as it is to you. TCF has policies and procedures in place to help us collect and maintain accurate information. If customers inform us that they believe some of our information is inaccurate, we will investigate and take steps to correct the information where necessary. Of course, customers should notify TCF as quickly as possible of any information maintained or reported by TCF that they think is incorrect.

At TCF we value our relationship with you, our customer. We use your customer information only in connection with business purposes that we believe are appropriate and to develop better products and services to meet your financial needs.

Internet Security

The security of your online banking transaction depends upon a partnership between you and TCF.

While we have numerous security measures intended to reasonably protect the confidentiality of your online banking transactions, you are also responsible for maintaining security.

Your Responsibility

You are responsible for keeping your banking information confidential. This means you should not share your password, account numbers, personal identification information , or other account data with anyone, including any other companies or services providers. You should also safeguard this information so unauthorized persons cannot find it.

You are also responsible for inputting or entering correct information and for notifying us about lost or stolen information or suspected fraudulent activity. Entering incorrect information into an online banking website can expose your information to unauthorized access and cause errors in processing your transactions.

You are also responsible for logging out when your online banking session is complete, to prevent unauthorized persons from using the Online Services.

Except as otherwise provided by law, we are not responsible for your errors or negligent use of any services provided by this website and will not be responsible for or cover losses due to:

- Misuse of any services;
- Input errors;
- Unauthorized access to your account(s) resulting from your negligence, such as sharing your password, writing down your password, entering your password when others may see you;
- Leaving your computer unattended while transacting on-line banking;
- Failure to report unauthorized account access within two business days from the date it became known to you; and

- Viruses. Viruses cannot get into your computer unless you let them by downloading programs, opening emails or attachments, or sharing diskettes. There are numerous virus-protection programs available commercially to help you reduce, but not eliminate, this risk.

Your Browser

In order to use the Online Services, your browser must support the Secure Sockets Layer (SSL) protocol. SSL helps provide a secure channel to send and receive data over the Internet. Our online banking site is viewed best with Microsoft Internet Explorer version 10 and above, or current versions of Chrome, Firefox or Safari. Other browsers may work but the display and printing of pages may not be ideal and certain functionality may not be available.

Trusted Operating System

The trusted operating system helps protect customer information by containing privilege and authorization codes to control access. The system also contains audit controls to track requests and navigation in order to identify suspicious activities.

Surveillance

We constantly monitor attempts to break into our security systems. This helps us to identify possible system vulnerabilities.

Individual User Name and Password

You authorize and authenticate your online banking transaction by entering your user name and password, which are encrypted when they are transmitted to us. You should safeguard your user name and password and keep them a secret. We strongly recommend that you do not use your Social Security number as a username or password.

Timed Log-Off

TCF's online banking system will automatically log you off after 20 minutes of inactivity. This reduces the risk of others accessing your information from your computer while it is unattended.

Encryption

"Encryption" means we will scramble the data. We encrypt your personal data, including your password, when it is in transit. We do this to help prevent third parties from accessing your information.

You can generally determine if encryption is being used if the padlock icon on your browser is locked. If the padlock icon is unlocked, encryption is not being used. Any web address beginning with "https://..." indicates the page you are viewing uses encryption.

Routers and Firewalls

We use a series of routers and firewalls to help prevent unauthorized persons from obtaining your account information.

The first component is a router, which determines who has access to designated Internet banking components by verifying the source and destination of each transmission, and determines whether or not to let the transmission pass.

A firewall tracks each request, the source of the request, when the request was made and the destination of each request. The firewall changes the "address" of the request to deliver it to the appropriate site. These precautions are used to determine whether the request is granted and helps protect our internal networks from unauthorized access.

You authorize and authenticate your online banking transaction by entering your password, which is encrypted when it is transmitted to us.

Please safeguard your password and keep it confidential at all times.

Additional Security Measures

TCF employs a layered approach to online banking security that goes beyond trusted operating system controls, surveillance, unique usernames and passwords, timed log-offs, encryption, and routers and firewalls. Certain information security-related events may trigger additional security measures. For example, if we are suspicious of any online activities, we may restrict online access to accounts or prevent certain kinds of transactions. Further proof of identity may be required before we restore online access.

Alternative Risk Control Mechanisms

If you are a business customer, TCF recommends that you periodically perform a risk assessment and evaluate your controls as they relate to your online banking activities. You should also consider the following alternative risk control mechanisms to mitigation your own risk. For instance, consider assigning separate user identification names or numbers to each of your employees having access to your online accounts, rather than letting several employees share a single name or number. Each employee should have his or her own password, and these should change every 30 days.

Accuracy of Information

We know that maintaining accurate customer information is just as important to you as it is to us. TCF Bank has policies and procedures in place to help us collect and maintain accurate information about your accounts.

If you believe that some of our information regarding your accounts is inaccurate, please notify us and we will investigate to take steps as soon

as possible to correct the information.

Of course, you should contact us as quickly as possible about any information maintained or reported by TCF that you think is incorrect.

How To Protect Yourself

TCF will never ask you to provide your online banking sign-in I.D., online banking password, or secret code by email, phone or pop-up message. Use the following tips for preventing email fraud and identity theft.

General Fraud Prevention Tips

- Never provide personal information in response to an unsolicited request (including from someone claiming to be from TCF), whether it is in an email or over the phone or on the Internet. Emails and Internet pages created by phishers may look exactly like the real thing. They may even have a fake padlock icon that ordinarily is used to denote a secure site. If you do not initiate the communication, do not provide any information.
- If you are unsure whether a contact is legitimate, contact us. You can find phone numbers and websites on the monthly statements you receive from TCF. The key is that you should be the one to initiate the contact, using information that you have verified yourself.
- Never provide your account information, online banking password over the phone or in response to an unsolicited Internet request. TCF would never ask you to verify your account information or confirm a password online. Thieves armed with this information and your account number can help themselves to your money.
- Review account statements regularly to ensure all charges are correct. If your account statement is late in arriving or does not arrive, phone TCF to find out why. Check your account activity online regularly to catch suspicious activity.

Online Banking Safety

- Do not leave your computer unattended after you have signed in to online banking at TCF.
- Always exit your online banking session when you have completed your transactions.
- Safeguard your online banking password and keep it private. Never give your online banking password to others or allow others to access your online banking records.
- If you access your account information from any computer other than your own (such as your computer at work) be sure the system is private (not shared).
- Avoid accessing your account from Internet cafes, airports or other public Internet locations where the security of a wireless network is unknown.

Telephone Banking Safety

- TCF employees will never ask you to tell them your online banking password over the telephone. If someone calls you claiming to be a TCF representative and asks for your password, do not give it out. Ask them for identification and call TCF immediately to report the incident.

TCF Check Card Safety

- As soon as you get your new card, call TCF to activate it, and sign the back of the card.
- Review your monthly statement or your account activity online to confirm all transactions are yours. Report any errors or unknown charges immediately.
- After you have handed your card to a merchant for a purchase, make sure that the card is actually yours when it is given back (and not the card of someone else). Keep your charge slip and destroy any carbons.
- If you lose your card, report it to TCF immediately.

ATM Safety

- We want your experience at TCF ATMs to be convenient and safe. To ensure your safety when using any ATM, follow these important tips:
- Look around and observe your surroundings – if the ATM is poorly lit or is in a hidden area, use another location.
- Have your card ready. Don’t go through your wallet or purse to find your card while stopped at the ATM.
- Don’t leave your keys or valuables in your car when using an ATM, and don’t leave your car engine running.
- Make sure people waiting behind you to use the ATM can’t see you entering your PIN or transaction amount.
- If you are using an indoor ATM that requires your card to open the door, look inside before entering. Don’t let anyone come in with you who you do not know.
- Lock the car doors and roll up the other windows when you use a drive-through ATM.
- Cancel your transaction and leave immediately if you see anything suspicious. Verify as soon as possible with TCF Bank that the transaction was canceled.
- Don’t count your cash while standing at the ATM! Put your cash, card, and receipt away immediately.
- Never leave your receipt behind. Always take it with you. Compare your ATM receipts to your monthly statement. It is the best way to guard against fraud and it makes record keeping easier for you.
- If you lose your TCF check card or your ATM card, contact TCF Bank immediately.

Your Card and PIN

- Protect your ATM card from damage by keeping it in a safe place – don't allow it to bend or be scratched.
- Memorize your PIN. If you must write down your PIN, don't keep it in your wallet, purse, or on the card itself.
- When selecting a PIN, avoid numbers and letters that can be easily identified or associated with you. Don't use your initials, birth date, telephone number, or home address.
- In case you lose your card – be sure to know the emergency phone numbers for TCF Bank.

Identity Theft

Identity theft means a fraud was committed or attempted using identifying information of another person without authority. Thieves steal your name, date of birth, account numbers, passwords, Social Security Number, or other confidential information to use your financial accounts or run up bills on your credit cards. They can take out loans, obtain credit cards and even get a driver's license in your name. They can do damage to your financial history and personal reputation that can take years to unravel.

How to Fight Identity Theft

- Never provide personal financial information, including your Social Security number, account numbers or passwords over the phone or the Internet, if you did not initiate the contact. Choose an online banking password that others cannot guess.
- Never click on the link provided in an e-mail you think is fraudulent. In addition to stealing your personal information, the link may contain a virus that can contaminate your computer.
- Do not be intimidated by an email or caller who suggests dire consequences if you do not immediately provide or verify financial information.
- If you are unsure whether a contact is legitimate, go to the company's website by typing in the site address or using a page you have previously book marked, instead of using a link provided by the email.
- If you fall victim to identity theft, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.
- Learn more about how to keep your banking activity safe.

What to Do If You Are a Victim

- Contact us immediately to alert us of the situation.
- Close accounts you think have been tampered with or opened fraudulently. Phone the security or fraud department of each associated company or financial institution. Follow-up in writing and supply copies of supporting documents.
- Notify credit card companies and financial institutions in writing. Send your letters by certified mail, return receipt requested, so you can document when and what the company received. Keep copies of your correspondence or enclosures.
- Report all suspicious contacts to the Federal Trade Commission through the Internet here, or by phoning 1-877-IDTHEFT (1-877-438-4338).
- Check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number, or check www.naag.org for a list of state Attorneys General.
- File a report with local police or police in the community where the identity theft took place. Get a copy of the police report or the report number. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report.
- Contact one of the major credit bureaus listed below to place a fraud alert on your file. A fraud alert will help prevent thieves from opening a new account in your name.

  Equifax
  P.O. Box 740250
  Atlanta, GA 30374
  (800) 525-6285
  www.equifax.com

  Experian
  P.O. Box 1017
  Allen, TX 75013
  (888) 397-3742
  www.experian.com

  TransUnion
  P.O. Box 6790
  Fullerton, CA 92634
  (800) 680-7289
  www.transunion.com

- To learn more about keeping your money safe, visit MyMoney.gov

Online Banking & Email Fraud

TCF Bank will never ask you to provide your Online Banking sign-in ID, Online Banking password or PIN by email, phone, or pop-up message. Learn about online banking and email fraud below.

FDIC Fraudulent Correspondence Alert

Fraudulent TCF Bank look-alike emails asking for personal and confidential information have been sent to some TCF customers. These emails are not from TCF Bank. Do not respond to these emails or click on any links or attachments contained within them. TCF Bank will never ask you to provide your Online Banking sign-in ID or Online Banking password by email.

Access the downloads below to see examples of fraudulent emails sent to TCF customers.

How to Report Email Fraud

If you believe you have received a fraudulent email, please forward the email immediately to emailfraud@tcfbank.com and then delete the email.

If you have already responded to an email you believe is fraudulent, please contact a TCF representative immediately to report your card as stolen.

If you call after business hours, please follow the voice prompts for reporting your card as stolen. Your call will be answered by a Visa® automated processing system.

Email Fraud Examples

- Subject: Online Banking Update Notice
- Subject: Online Banking Alert. Reconfirm your Billing Information
- Subject: Message Alert - You Have 1 Important Message
- Subject: Unauthorized Login Access Denied
- Subject: Your TCF Account Has Been Suspended
- Subject: TCF Privacy Policy: Re-Confirm Your Online Banking Activities
- Subject: Online Banking Notice (February 2008)
- Subject: Important Notice (February 2008)
- Subject: Security Notice Alerts(Online Banking Security Access)
- Subject: Update Your TCF Online Banking.
- Subject: TCF Bank Security Update Notification
- Subject: You have 1 new secure message
- Subject: TCF Debit Card Alert
- Subject: TCF National Bank Security Message
- Subject: Important Online Banking Alert
- Subject: TCF Bank Verification Required
- Subject: Confirm Your Identity
- Subject: Dear TCF customer
- Subject: Important Action Required
- Subject: TCF Bank e-mail verification

TCF employees will never ask for your account PIN or online banking password or ask that you write your PIN or password for them. If someone phones you claiming to be a TCF Bank representative and asks for your PIN or password, do not give it out. Ask for identification and contact us immediately to report the incident.

It is very important that you keep your PIN and password secure to prevent unauthorized use of your account. If you feel that your PIN or password is no longer secure, contact us immediately.

Tips to keep your PIN and password secure:

- Choose a PIN and password that others cannot guess
- Do not tell anyone else your PIN or password
- Never send a PIN or password by email
- Consider changing your PIN and password regularly
- Do not leave your PIN or password where someone else can find it. Keep it safe.

FDIC Fraudulent Alerts

- New – FDIC Fraudulent Email Special Alert.
- FDIC Fraudulent Correspondence Alert.

To display downloaded PDFs, you will need Adobe Reader. Get it now for free.

Changes to the Online Privacy and Security Policy

TCF may make changes to this Policy from time to time by posting the changes on this website. Users are encouraged to review the Policy periodically. If we make changes to the Policy, we will update the "Effective Date" posted at the bottom of the Policy to reflect the effective date of the change. Any such changes will become effective when posted on this website. By continuing to use the Online Services following such changes, you are agreeing to accept the terms of the revised Policy.