

U.S. Bank Protect 360 Terms of Use

WELCOME

The U.S. Bank Protect 360 Terms of Use (“TOU”) includes important disclosures related to your use of the U.S. Bank Protect 360 services. This TOU is in addition to the Digital Services Agreement and any other agreements and disclosures that apply to your account(s)/relationship. If there is a conflict between this TOU and other agreements (or terms of use) that specifically reference the U.S. Bank Protect 360 services features described herein, this TOU will control in resolving those inconsistencies.

This TOU is revised periodically, and it may include changes from earlier versions; the most current version is the controlling version of this TOU. In accordance with your communication preferences, you will receive an electronic notification of material changes in advance of the effective date of such changes. **By continuing to use the U.S. Bank Protect 360 services after the effective date of the change, you are reaffirming your acceptance of the most recent version of this TOU.**

SUBSCRIPTION SERVICES PURCHASE, BILLING AND AUTOMATIC RENEWAL TERMS

Services

As part of our Digital Services, we make available basic credit monitoring and identity protection services at no charge called U.S. Bank Protect 360 Essentials (“Essentials”) and advanced credit monitoring and identity protection services that require payment of a monthly subscription fee called U.S. Bank Protect 360 Premium (“Premium”). The specific features included in the Essentials and the Premium services (collectively, the “Protect 360 Services”) are disclosed at the time of enrollment and generally described below. **We may modify the features, functionality, availability, pricing, or billing terms of any of the Protect 360 Services from time to time as permitted by law.** If a change materially affects your subscription to Premium, we will provide notice within the timeframe required by applicable law, and the change will generally take effect at the next monthly renewal. By enrolling in the Protect 360 Services, you consent to receive all notices and disclosures electronically and agree that your electronic consent and transactions satisfy any legal requirements for written agreements.

The Protect 360 Services rely on third-party data processing and monitoring that may not be continuous. Monitoring services are informational and do not prevent identity theft, fraud, or unauthorized use of personal information. We do not provide monitoring, restoration, or process claims for identity theft or fraud that occurred prior to enrollment in the Protect 360 Services.

Eligibility and Availability

Enrollment in the Protect 360 Services is available only if you are a Digitally Engaged U.S. Bank customer. To enroll in Premium, you must be an Essentials customer with a U.S. Bank method of payment on file which is associated with one of your Digitally Engaged accounts.

The Protect 360 Services are only available if your personal information can be verified with certain credit databases. If we cannot properly verify your information, you will not be able to use the Essentials service or enroll in the Premium service.

You may cancel enrollment in the Protect 360 Services at any time online by logging into the U.S. Bank website or mobile app and navigating to the Protect 360 summary section, or by calling customer support at 1-800-USBANKS (872-2657), or speaking with a banker at your local branch.

Authorization to obtain credit information and consent to share information

By enrolling in the Protect 360 Services, you provide your written instructions and authorization under the Fair Credit Reporting Act (“FCRA”) and other applicable federal and state laws for U.S. Bank, its Service Providers, and consumer reporting agencies (including Equifax, Experian, and TransUnion), to access your credit files on an ongoing basis, obtain information about you, and exchange information with such parties

for purposes of verifying your identity and providing the Protect 360 Services. Your information will be treated with respect to our Privacy Policy available [here](#).

Data processing

You authorize U.S. Bank, and its agents, servicers, and employees, to act on your behalf to submit opt-out requests to data broker sites, including to obtain and submit your personal information, communicate with data broker sites and other third parties, agree to applicable terms, execute required documents, and take other actions reasonably necessary to process opt-out requests or provide you with the Protect 360 Services. Submitting opt-out requests will limit data that can be used to provide you with the Protect 360 Services and may reduce or terminate your access to the Protect 360 Services.

Subscription Services term

Your Premium subscription begins on the date you successfully complete enrollment and payment ("Enrollment Date") and continues to auto-renew on a monthly basis ("Billing Cycle") until terminated by you or us as described below.

Billing

Billing authorization

By enrolling in Premium and selecting the applicable payment option, you authorize us, and our third-party payment processors, to charge your selected payment method for the initial subscription fee and for each automatic renewal, unless you cancel in accordance with these terms. You also authorize us to store your payment information for recurring billing purposes and to receive and use updated payment credentials from your card issuer to avoid interruptions to your subscription. All payment transactions are subject to the applicable account and card agreements, as well as the Digital Services Agreement.

- For payments from checking, savings/money market accounts: You authorize us to initiate ACH transfers every month by debiting your account. If you fail to add funds to your checking or savings account, your account may be overdrawn and could incur overdraft fee(s).
- For debit card payments: If your account does not have sufficient funds, you may be overdrawn and could incur overdraft fee(s).
- For credit card payments: If your selected card fails, your payment will not be processed, and your Premium service will be canceled. In the event the transaction exceeds your credit limit, you may be subject to over credit limit fees from your credit card issuer.

Subscription fees and taxes

Subscription fees are disclosed at the time of purchase and are listed in U.S. dollars. Applicable sales tax will be added where required by law. Upon enrollment, you will be charged the full monthly subscription fee for the applicable billing period. Subscription fees are not prorated based on the enrollment date or the number of days remaining in a month upon cancellation. You will not be charged a subscription fee if we are unable to process your enrollment in the Premium Service.

Billing cycle and renewal

Subscription fees, plus applicable taxes, are billed monthly on the anniversary of the Enrollment Date ("Renewal Date"). If a renewal month does not contain the corresponding calendar day, the subscription will renew on the last day of that month. Fees are charged in full and are not prorated for partial months, shortened months, or adjusted renewal dates.

Examples

- If you enroll on the 15th day of the month, your Renewal Date will occur on the 15th day of the next month.
- If you enroll on the 31st day of a month and a subsequent month has fewer than 31 days, your Renewal Date will occur on the last day of that month.

- If you enroll on February 29 in a leap year, your February Renewal Date in nonleap years will occur on February 28.

Billing disputes

If you believe you have been billed in error for Premium, you must notify us immediately by contacting customer support at 1-800-USBANKS (872-2657) and providing the following required information:

- Your name and account number (if any).
- The error or issue in question and why you believe it is an error or why you need additional information.
- The dollar amount of the suspected error.

We will investigate and respond within 10 business days after receiving your inquiry and will correct any error promptly.

Automatic renewal

Your Premium subscription will automatically renew for successive one-month terms unless your enrollment is canceled or terminated as described below.

You may cancel at any time online by logging into the U.S. Bank website or mobile app and navigating to the Protect 360 summary section, or by calling customer support at 1-800-USBANKS (872-2657), or speaking with a banker at your local branch.

If you do not cancel your subscription by 7:59 p.m. P.T. at least one (1) calendar day before the Renewal Date to avoid being charged for the next Billing Cycle, you expressly authorize us to charge the applicable monthly subscription fee plus any applicable tax to your payment method on file at the start of each renewal term.

SUBSCRIPTION CANCELLATION, TERMINATION, AND REFUNDS

Cancellation

Your enrollment in Premium will continue until canceled. You may cancel at any time online by logging into the U.S. Bank website or mobile app and navigating to the Protect 360 summary section, or by calling customer support at 1-800-USBANKS (872-2657), or by speaking with a banker at your local branch. You must cancel your Premium subscription by 7:59 p.m. P.T. at least one (1) calendar day before the Renewal Date to avoid being charged for the next Billing Cycle. If a cancellation request is submitted after this time, you may be charged for the subsequent Billing Cycle. Upon cancellation, your subscription will remain active until the end of the current paid Billing Cycle and will not renew. After the canceled Billing Cycle has ended, you will have access to Essentials only, and your access to Premium will cease. Historical alerts or reports may no longer be accessible, even if you decide to re-enroll in Premium at a later time.

Termination

We may terminate your enrollment if we are unable to provide you with any of the Protect 360 Services. We may also terminate your enrollment if you delete your U.S. Bank digital profile, close underlying eligible accounts, or no longer have access to Digital Services. Your enrollment may also be terminated for failed payments, fraud or misuse, or legal/regulatory requirements. If your enrollment is terminated, we will contact you.

Identity verification

Protect 360 Services may require identity verification. If we are unable to verify your identity or determine your eligibility, we may deny, suspend, or terminate access to Protect 360 Services in accordance with this TOU and applicable law.

Unable to obtain data

In order to provide you with the Protect 360 Services, we rely on information provided by the three major credit bureaus: Equifax, Experian, and TransUnion. There may be times when your information cannot be obtained from one or more of the bureaus. In these cases, you may be unable to receive credit reports, monitoring and/or credit scores.

If a Premium Service feature, such as credit monitoring is unavailable for more than 48 hours due to a technical issue, you may be eligible for a prorated refund until the feature is restored. Your Premium service will remain active while we investigate, unless you choose to cancel.

Failed payments and suspension

If a Premium subscription payment cannot be processed, we may attempt to reprocess the payment, request updated payment information, or suspend or terminate the Premium service. You are responsible for any related bank fees for reprocessing payments.

Refund policy

Except as expressly stated in these Terms or required by applicable law, Premium subscription fees are non-refundable, including for partial subscription periods, unused services, or early cancellation. Nothing in this TOU limits any statutory refund or cancellation rights you may have. Refunds may be issued at our discretion under certain circumstances.

If your monthly enrollment in Premium is canceled or terminated, you will not receive a refund except as expressly stated in this TOU or required by law. However, you may continue to use Premium through the end of the Billing Cycle. After cancellation, you will have access to Essentials only, and you will not be billed for any additional months after cancellation/termination. You may choose to cancel Premium at any time online by logging into the U.S. Bank website or mobile app and navigating to the Protect 360 summary section, or by calling customer support at 1-800-USBANKS (872-2657) or by speaking with a banker at your local branch.

FEATURES OF THE PROTECT 360 SERVICES

Essentials

Credit Score

Provides access to your credit score based on the VantageScore® 3.0 model using data from TransUnion. The score reflects a snapshot in time and may not reflect the most current information in your credit file. Accounts not reported to or removed from TransUnion are not included. In addition, you will receive up to 12 months of score history, refreshed weekly, enabling you to track changes over time and better understand your credit standing.

Accessing your credit score through this service does not affect your credit score. The service does not maintain or modify your credit report.

Credit Report

Provides access to your credit report from one credit bureau (TransUnion). The report is refreshed weekly.

Each credit bureau maintains separate credit files and information may differ across bureaus. Data may not include accounts not reported to that bureau or accounts that have been deleted. The Protect 360 Services cannot make corrections or changes to your credit report. Viewing your report through the Protect 360 Services does not constitute credit repair.

Credit Alerts

Monitors credit activity across one major credit bureau (TransUnion) and sends alerts for certain key credit file changes to help detect potential fraud.

Monitoring does not prevent fraud or unauthorized account activity. It may not alert you if information about you (including your name, address or Social Security Number) is contained in the credit file of another person and will not provide you with any information contained in another individual's credit file. Alerts are not guaranteed and may be delayed or incomplete.

Debt Analysis

Summarizes reported debt balances and estimated monthly obligations and calculates a debt-to-income (DTI) ratio to help you understand how debt impacts your financial profile.

Debt data is derived solely from your TransUnion credit report. Accounts not reported to TransUnion are not included. Debt-to-income calculations rely in part on self-reported income. Calculations are estimates only and may be incomplete or inaccurate. This feature is not financial, credit, or budgeting advice.

Score Factors

Explains the primary factors influencing your credit score and provides personalized educational insights and tips to help you better understand your credit profile.

Score factors are informational and do not guarantee score improvement. Insights are based only on data available from the applicable credit bureau. Educational tips are not predictive and should not be relied upon as financial advice.

Score Forecast

Provides hypothetical scenarios showing how certain credit behaviors (such as paying down balances or opening accounts) might impact your credit score.

Forecasted scores and changes are estimates only. Actual credit score outcomes may differ, materially or entirely. No guarantee is made that forecasted results will occur. Results should not be relied upon to take or refrain from taking any action.

Credit Freeze Guide

Designed to help you protect your credit by guiding you on how to place or remove credit freezes with Equifax, Experian, and TransUnion, including direct links and step-by-step guidance.

This service does not place a freeze on your behalf. Credit freeze effectiveness and availability are controlled by the credit bureaus, and you remain responsible for managing freezes directly with each bureau.

Dark Web Monitoring (Essentials)

Scans 100,000+ websites, 35,000+ chat rooms, forums, and message boards on the dark web for your exposed information. Detects usernames, passwords, IP addresses, NPI numbers, and more. Monitored items include one: Email, phone number, address, name, DOB, and SSN.

Monitoring does not include all illicit sites or private forums and is limited to specific data elements. Detection does not mean misuse has occurred, and absence of alerts does not mean data has not been exposed. Removal of exposed data is not included with this feature.

Data Broker Scans

Scans data broker and people-search sites every 90 days to identify exposed personal information and provides instructions for manual removal.

Removal depends on third-party site cooperation. The Protect 360 Services do not guarantee complete or permanent removal. Scans are conducted periodically, not continuously.

[Premium \(includes all features of Essentials\)](#)

Credit Alerts

Monitors credit activity across all three major credit bureaus (Equifax, Experian, and TransUnion) and sends alerts for certain key credit file changes to help detect potential fraud.

Monitoring does not prevent fraud or unauthorized account activity. It may not alert you if an item of identifying information about you (including your name, address or Social Security Number) is contained in the credit file of another person and will not provide you with any information contained in another individual's credit file. Alerts are not guaranteed and may be delayed or incomplete.

SSN Alerts

Monitors if your SSN is used to apply for a financial or service account such as credit, banking, employment, healthcare, tax, or service applications and sends alerts of suspicious activity.

Monitoring is based on available data sources and may not detect all misuse. Alerts do not confirm fraud, only potential activity.

Change of Address Alerts

Uses United States Postal Service (USPS) and National Change of Address (NCOA) data to alert you when address changes are detected that may indicate identity fraud.

Monitoring is limited to data provided by USPS/NCOA systems. The Protect 360 Services do not prevent fraud or unauthorized mail redirection. Address changes identified may occur for legitimate reasons.

Dark Web Monitoring (Premium)

Checks a broader range of sensitive information than the Essentials service and expands dark web monitoring to include financial, government, and medical identifiers such as bank accounts, credit cards, driver's licenses, medical IDs, and passports. Provides alerts if exposed data is found.

Monitoring does not include all illicit sites or private forums and is limited to specific data elements. Detection does not mean misuse has occurred, and absence of alerts does not mean data has not been exposed. Removal of exposed data is not included with this feature.

High Spending Alerts

Allows you to set personalized financial thresholds and receive alerts when defined spending or asset limits are exceeded.

The Protect 360 Services do not monitor all financial accounts and do not prevent fraud. It is not intended to provide financial advice. Threshold alerts are informational only.

Social Media Protection

Monitors linked social media accounts (Facebook, Instagram, LinkedIn, Twitter, and YouTube) for unexpected profile changes, suspicious posts on public forums, and potentially fraudulent activity.

Monitoring applies only to linked accounts. To enable monitoring, you must link your social media accounts to the Premium service. The Protect 360 Services cannot access private content beyond platform permissions. Detection does not prevent third-party use of posted content.

Phone Monitoring

Monitors for signs of spoofing or vishing activity associated with your phone number and alerts you to suspicious patterns that may indicate fraudulent activity. Spoofing refers to the practice of deliberately altering caller ID information displayed on a person's device to disguise the caller's true identity. Vishing ("voice" + "phishing") is a type of phishing attack where phone calls or voice messages, sometimes using recognizable voices are used to trick users into revealing sensitive personal, financial, or login information.

Phone Monitoring does not block calls or prevent scams. It does not access call content, phone location, or device activity. The service detects when your phone number appears in a potential fraud event, as

identified by our Service Provider, and sends you an alert. Available data is limited to your phone number, associated mobile carrier, and the event timestamp. Not all spoofing or vishing activity can be detected.

Identity Theft Insurance + Identity Restoration

Provides identity restoration assistance through our Service Provider and up to \$1 million in identity theft insurance for eligible out-of-pocket costs, subject to confirmation and policy terms. Identity theft insurance may reimburse you for certain losses for unauthorized electronic funds transfers and expenses related to identity theft, including replacement of documents, traveling expenses, loss of income, child/elderly care expenses (incurred as a result of identity restoration), and legal costs. If you believe you have experienced identity theft and need assistance with identity restoration services, please contact 1-833-568-6249 to open a restoration case.

If you would like to obtain a copy of the insurance policy, have questions regarding identity theft insurance coverage, or wish to file a claim under the policy, please contact our insurance Service Provider at 1-866-237-5240.

The information provided here is a summary and is solely intended for informational purposes and may not include all terms, conditions, and exclusions of the policies described. Coverage may not be available in all jurisdictions. Cancellation or termination of your Premium subscription will result in immediate termination of policy coverage. Please refer to the actual policy for terms, conditions, qualifications, and exclusions of coverage.

Home Title Monitoring

Monitors property records to detect changes such as liens, ownership transfers, refinances, or new claims that may indicate title fraud.

Monitoring relies on public and third-party property record sources. Alerts do not prevent fraudulent filings. The Protect 360 Services do not provide legal or title insurance protections.

Data Broker Scans and Automatic Removal

This service scans data broker and people-search sites every 90 days and automatically submits and tracks removal requests on your behalf.

Not all sites honor removal requests. Reposting of personal information by third parties may occur.

[Delivery of alerts and notifications](#)

We can not guarantee the delivery of alerts and notifications and can not guarantee that the Protect 360 Services will detect all possible instances of identity theft and/or potentially fraudulent or improper use of your information.

As a condition for using and receiving alerts, you acknowledge and agree that you will keep any personal information required to enable the applicable alert accurate and current, including without limitation, your name, address, date of birth, email address, telephone number, social security number, driver's license number, and financial account numbers (e.g. credit or debit card numbers, etc.).

[Right to receive a free credit report](#)

A "consumer disclosure" is a complete account of all the information on your credit report, as mandated by consumer reporting legislation. A consumer disclosure lists all inquiries made to your credit file, including account management inquiries, non-credit-related inquiries and your own inquiries. The credit and personal information provided to you as part of the Protect 360 Services does not constitute a consumer disclosure for the purposes of applicable consumer reporting legislation. By law, you are entitled to receive a free copy of your consumer disclosure from each of the national credit reporting agencies by contacting them directly.

[Credit freeze](#)

A credit freeze (also called a security freeze or a credit lock) can be placed on your accounts and it restricts access to your credit report, preventing identity thieves from opening new accounts in your name. It does not affect your credit score or stop you from using existing credit cards. You must contact all three major bureaus - Equifax, Experian, and TransUnion - to freeze your credit.

ADDITIONAL TERMS OF USE

[Links to other internet sites and third-party services](#)

The Protect 360 Services may contain links to other websites and services provided, owned or operated by third parties. These links do not imply our endorsement or approval of material on any third-party website. The linked websites are not under our control, and we are not responsible for the availability, content, products, services, advertising, or other materials available on third-party websites. The privacy policies of third-party websites may provide less security than our websites, so we strongly encourage you to read the third party's privacy policy before sharing any information with that third party.

All matters concerning third-party websites and services provided or operated by third parties are solely between you and the third party. We make no warranties or representations whatsoever regarding any third-party website or service and we are not responsible or liable to you for any damages, losses, or injuries of any kind arising out of your use of any third-party website.

[Intellectual property rights](#)

Content connected with the Protect 360 Services includes proprietary content in addition to your customer data. Proprietary content is the exclusive intellectual property of us, our licensors, and/or Service Providers and it may be protected by copyrights and other intellectual property rights. You are permitted to use the proprietary content delivered to you through the Protect 360 Services only for your personal use. You may not copy, reproduce, distribute, or create derivative works from proprietary content. Further, you agree not to reverse-engineer or reverse-compile any technology, including any software or other content associated with the Protect 360 Services.

The trademarks, logos, and service marks displayed in connection with the Protect 360 Services are the registered and unregistered trademarks of us, our Service Providers, or other third parties. Under no circumstances may you use, copy, imitate, alter, modify, or change these trademarks. Nothing contained on, in, or otherwise connected with the Protect 360 Services should be construed as granting (by implication or otherwise) any license or right to use any trademark without the express written permission of us or the third party, which has rights to such trademark.

All messages, suggestions, ideas, notes, concepts, know-how, techniques, data, applications, mail, and other information you may send to us through or regarding any of the Protect 360 Services shall be considered an uncompensated contribution of intellectual property to us and shall become our exclusive intellectual property. By submitting any of these materials to us, you automatically grant (or warrant that the owner of such materials has expressly granted) to us a perpetual, royalty-free, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, translate, publicly perform and display, create derivative works from and distribute such materials or incorporate such materials into any form, medium, or technology now known or later developed, and you warrant that all so-called "moral rights" in those materials have been waived, and you warrant that you have the right to make these warranties and transfers of rights.

[No warranties](#)

NEITHER WE, NOR SERVICE PROVIDERS, REPRESENTS OR WARRANTS THE ACCURACY, ADEQUACY, COMPLETENESS OR TIMELINESS OF THE PROTECT 360 SERVICES, OR THE ERROR FREE USE OF THE PROTECT 360 SERVICES. ALL PROTECT 360 SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT AND FREEDOM FROM A COMPUTER VIRUS.

IN THE EVENT OF A SYSTEM FAILURE OR INTERRUPTION, YOUR DATA MAY BE LOST OR DESTROYED. YOU ASSUME THE RISK OF LOSS OF YOUR DATA DURING ANY SYSTEM FAILURE OR INTERRUPTION AND THE RESPONSIBILITY TO VERIFY THE ACCURACY AND COMPLETENESS OF ANY TRANSACTIONS SO AFFECTED.

Limitation of liability; indemnification

IN NO EVENT WILL WE OR ANY SERVICE PROVIDERS BE LIABLE UNDER ANY CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHER CLAIM FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA, OR OTHER INTANGIBLE LOSSES (EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), WHETHER CAUSED BY OR RESULTING FROM (1) THE USE OR THE INABILITY TO USE THE PROTECT 360 SERVICES; (2) ANY FAILURE OF PERFORMANCE, ERROR, OMISSION, INTERRUPTION, DELAY IN OPERATION OR TRANSMISSION, COMPUTER VIRUS, LOSS OF DATA, THEFT, DESTRUCTION, OR UNAUTHORIZED ACCESS TO YOUR INFORMATION; (3) ERRORS, INACCURACIES, OMISSIONS, OR OTHER DEFECTS IN INFORMATION OR CONTENT PROVIDED BY, CONTAINED WITHIN, OR OBTAINED THROUGH ANY OF THE PROTECT 360 SERVICES, OR (4) ANY OTHER FAILURE, ACTION, OR OMISSION.

YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD US AND OUR SERVICE PROVIDERS HARMLESS FROM ANY AND ALL THIRD-PARTY CLAIMS, ACTIONS, LIABILITY, DAMAGES AND/OR COSTS (INCLUDING, BUT NOT LIMITED TO, REASONABLE ATTORNEY'S FEES) ARISING FROM (1) A THIRD-PARTY CLAIM, ACTION OR ALLEGATION OF INFRINGEMENT, MISUSE OR MISAPPROPRIATION BASED ON INFORMATION, DATA, FILES OR OTHER MATERIALS SUBMITTED BY YOU TO OR THROUGH ANY OF THE PROTECT 360 SERVICES; (2) ANY FRAUD, MANIPULATION OR OTHER BREACH OF THIS TOU BY YOU; (3) ANY THIRD-PARTY CLAIM, ACTION OR ALLEGATIONS BROUGHT AGAINST US ARISING OUT OF OR RELATING TO A DISPUTE WITH YOU OVER THE TERMS AND CONDITIONS OF AN AGREEMENT OR RELATED TO THE PURCHASE OF SALE OF ANY GOODS OR SERVICES; (4) YOUR VIOLATION OF ANY LAW OR RIGHTS OF A THIRD PARTY; OR (5) USE OF ANY OF THE PROTECT 360 SERVICES OR USE OF YOUR ACCOUNT BY ANY THIRD PARTY. WE RESERVE THE RIGHT, AT OUR OWN EXPENSE, TO ASSUME THE EXCLUSIVE DEFENSE AND CONTROL OF ANY MATTER OTHERWISE SUBJECT TO INDEMNIFICATION BY YOU, IN WHICH EVENT YOU WILL COOPERATE WITH US IN ASSERTING ANY AVAILABLE DEFENSES. YOU WILL NOT SETTLE ANY ACTION OR CLAIMS ON OUR BEHALF WITHOUT OUR PRIOR WRITTEN CONSENT.

Arbitration and class action waiver

YOU AGREE THAT ANY ARBITRATION/CLASS ACTION WAIVER PROVISION DESCRIBED WITHIN YOUR UNDERLYING ACCOUNT/RELATIONSHIP AGREEMENT ALSO APPLIES TO ANY CONTROVERSIES OR DISPUTES ARISING OUT OF OR RELATING TO YOUR USE OF DIGITAL SERVICES AND THIS TOU.

Governing law

Your use of the Protect 360 Services and the interpretation of this TOU is governed by all applicable Federal laws of the United States of America and the laws of the State of Minnesota (without regard to any choice of law provisions thereof).

DEFINITIONS

The following definitions apply in this TOU:

The words **“we,” “our,”** and **“us”** mean **U.S. Bank National Association (“U.S. Bank”)** and its respective affiliates, employees, successors, and assigns.

The words **“you”** and **“your”** mean each account owner and anyone else with access to receive the Protect 360 Services covered in this TOU. If there is more than one owner, then these words mean each account owner separately and all account owners jointly.

“Active Digital Consumer Account” means a demand deposit (checking), savings, or other consumer asset account (including Private Banking accounts) established primarily for personal, family, or household purposes that is enabled for digital banking services and has exhibited customer-initiated online activity

(including transactions or other account interactions) within the past year. Prepaid card accounts are not considered Consumer Accounts.

“Consumer” means a natural person, and does not include a sole proprietor, corporation, limited liability company, or other entity.

“Digital Services” means the digital financial services described in the Digital Services Agreement that we and our Service Providers make available to you on our secure online and mobile banking platforms.

“Digitally Engaged” means a consumer with an Active Digital Consumer Account; or a consumer credit card or consumer lending account enabled for Digital Services.

“Service Provider” means any processor or other third party that we have engaged to provide services in connection with the Protect 360 Services. This includes any agent, independent contractor, or subcontractor of any of the foregoing.

CONTACT US

If you have any questions, concerns, or complaints, you may contact us at a branch, or by contacting us as described below. Keep in mind that we may not immediately receive electronic messages you send, and we will not take action based on your electronic message until we actually receive it and have a reasonable time to act.

We accept relay calls.

U.S. Bank 24-Hour Banking Customer Support: 1-800-USBANKS (872-2657)

September 2026

© U.S. Bank