

U.S. Bank Protect 360 FAQ

Contents

Premium subscription management.....	2
Credit monitoring services	3
Credit monitoring.....	3
Credit score forecast tool.....	4
Credit freezes	5
Data privacy services.....	7
Identity protection services.....	9

U.S. Bank Protect 360 FAQ

Premium subscription management

When is my billing cycle?

Your first billing cycle starts on the date you enrolled in U.S. Bank Protect 360 Premium. Each billing cycle will start on the same date each month.

If your billing cycle is set to renew on a date that doesn't exist in the current month, then it will be renewed on the last day of that month.

For example:

- You enroll on January 14. Your billing cycles will begin on the 14th every month.
- You enroll on January 31. Your billing cycle will begin on the last day of each month: February 28 or 29, March 31, April 30, and so on.

If I cancel before my billing cycle is over, do I get a partial refund?

No. Refunds are only issued when required by law, or if we're unable to provide the service because of things like system outages, data availability or third-party malfunctions.

When you cancel, you'll continue to have access to your premium features through the end of your billing cycle. After that, you'll be switched to the free essentials plan.

Why is my subscription more than \$9.99 each month?

Applicable sales tax is added to your subscription price where required by law.

How do I cancel my premium subscription?

You can cancel at any time online or by calling us at 800-USBANKS (872-2657).

To cancel online, go to your U.S. Bank Protect 360 summary page and select **Manage**, then **Cancel subscription**.

To avoid charges for the next billing cycle, cancel by 7:59 p.m. PT the day before your renewal date. If you cancel after this time, you may be charged for the next billing cycle.

U.S. Bank Protect 360 FAQ

Credit monitoring services

Credit monitoring

Why can I not see my credit score or report?

We rely on TransUnion to provide your credit score and report. If they don't provide your data, we can't display it.

If you're using premium and we can't retrieve your data for an extended period, we will notify you and will look into the issue to see if we can fix it. During this time, your premium subscription will remain active. If we cannot restore services and display your data, you may receive a refund.

What should I do if I see something inaccurate in my credit report or alerts?

If you don't recognize an account, inquiry or activity in your credit profile, you can file a dispute directly with the credit bureau that reported it.

To file a dispute:

1. Check your Protect 360 account to see which credit bureau reported the item.
2. Contact the bureau by letter, online or by phone:

Equifax

PO Box 740256
Atlanta, GA 30374
equifax.com
800-525-6285

Experian

PO Box 9554
Allen, TX 75013
experian.com/fraud
888-397-3742

TransUnion

PO Box 2000
Chester, PA 19016
transunion.com/fraud
800-680-7289

U.S. Bank Protect 360 FAQ

3. Tell the bureau which item you believe is incorrect and request a dispute.

Be prepared to provide identifying info and details about the item you're disputing. Each bureau has its own dispute process and may ask for supporting documentation.

Credit score forecast tool

How does the credit score forecast work?

The credit score forecast tool uses your current credit profile to show how specific changes could impact your score.

This won't actually affect your credit score. It just helps you understand what can happen before you make big financial decisions.

Are the credit score forecast changes guaranteed?

No. The credit score forecast tool simulates what one change could do to your credit score. But in reality, your score is affected by multiple factors, not just one change. This tool helps you understand each individual part of the whole picture.

What scoring model does the credit score forecast use?

The credit score forecast tool is based on VantageScore® 3.0 credit scores. Your score will be different based on the model you're currently using.

What happens if I make more than one important change to my credit at once?

The credit score forecast tool will help you understand how much impact one particular action can have on your credit score. That way, when your score changes, you'll have a better idea of how much each action is affecting your score.

How long do credit score changes usually last?

It depends. The type and number of changes that affect your score will determine how long the change might last. For example, a missed payment will affect your score longer than a hard inquiry will. However, it also depends on the number of events that happen at once.

U.S. Bank Protect 360 FAQ

Credit freezes

How does a credit freeze protect my credit?

To open a credit card or loan account, creditors usually need to see your credit report. A credit freeze stops this from happening. This helps prevent identity thieves from opening an account in your name.

If you want to apply for a credit card or loan yourself, you can always unfreeze your credit, then refreeze it once your account is opened.

Why should I freeze my credit?

Credit freezes prevent identity theft by making it more difficult for anyone to open a fraudulent account in your name.

What is the difference between locking my credit and a credit freeze?

Credit freezes and credit locks both prevent the use of your credit report to open a loan or credit account.

Some credit bureaus offer different features with credit locks, but these may come with a monthly fee. Freezing your credit is always free.

What's the best way to use a credit freeze to prevent identity theft?

Most creditors use one of the three major credit bureaus to run credit checks: Equifax, Experian and TransUnion. To maximize protection, many people choose to freeze their credit with all of them.

What does a credit freeze do? What does it not do?

A credit freeze will:

- Prevent most creditors from accessing your credit report without your consent

A credit freeze will not:

- Affect your ability to use a credit monitoring service
- Directly impact your credit score
- Stop you from receiving prescreened offers of credit lines
- Prevent you from using existing credit accounts

U.S. Bank Protect 360 FAQ

While your credit is frozen, the following people can still see your credit report:

- Your current lenders and card issuers, as part of their account management process
- Landlords and rental agencies that are screening you as a potential tenant
- Debt collectors attempting to collect a debt
- Credit card issuers that have prescreened you for credit offers
- Potential employers that you have authorized to conduct a background check
- Child support agencies
- Government agents who are executing a court order or warrant

U.S. Bank Protect 360 FAQ

Data privacy services

What does the data privacy service do?

The essentials service helps you remove personal, sensitive or unwanted info from the web. You can scan for your info on dozens of people search sites and data brokers.

With premium, we'll take care of the whole process, regularly scanning for your info on these sites and removing it.

What is a data broker?

According to the Federal Trade Commission (FTC), a data broker is a site or service that compiles info about consumers and resells it to advertisers and other third parties.

What is a people search site?

A people search site is a type of data broker that makes personal info publicly available, often without consent. This info can usually be found through a simple online search.

Why should I remove my info from data brokers and people search sites?

According to the Federal Trade Commission (FTC), nearly every U.S. consumer has personal info on data broker and people search sites. Your info appearing on these sites can make you vulnerable to serious threats like identity theft, hacks, robocalls, spam, doxxing, stalking and harassment.

How does the premium data privacy service work?

1. Search and find: We scour dozens of data brokers and people search sites to find where your info is being listed, including your phone number, email address, family members and government records.
2. Remove and opt out: We send deletion or opt out requests on your behalf. If a site won't allow third party requests, we'll streamline the process so you can easily delete or opt out yourself.
3. Monitor and track: We monitor these sites regularly to verify the info has been removed. Once your info is removed, a data broker can sometimes compile new

U.S. Bank Protect 360 FAQ

info about you. So we'll keep monitoring them and submit a new request to remove your info if it shows up again.

How long does it take to remove my info or opt out?

It varies. Some sites will remove your info in hours, but others will take months. With premium, we'll continue to recheck the site until your info has been removed. Once this is done, we'll show the record as **Done**.

Some sites require additional action from you to complete the process. We'll show these records as **Action required**.

Why are you showing me a record that isn't me, or has partially incorrect info?

Data brokers combine info from multiple sources, which can result in incomplete or incorrect records. We show what's actively promoted when someone searches for you, both accurate and inaccurate.

Will you find all of my info on the sites you search?

Our technology is extremely effective at finding references to your personal info, but we can't guarantee we'll find it all. There are a few reasons for this:

- The info submitted is incomplete or incorrect.
- A site is temporarily down or offline.
- A site has created a record about you after our most recent scan.
- A site does not show records due to security rules or other issues.

With premium, you can minimize these misses, because we will run scans regularly to make sure your info is found and removed.

Why does a record say removed when I can still find it on the data broker site?

Broker sites can have multiple records for the same person, or they may republish info after it was removed. If they change how they store or display data, this can also lead to them showing different results for the same search.

With premium protection, we regularly rescan these sites. If a record reappears or a new one surfaces, we'll usually find these records on your next scan and resubmit them for removal.

U.S. Bank Protect 360 FAQ

Identity protection services

What is identity theft?

Identity theft is a crime in which someone deliberately assumes your identity and uses your personal info, like your SSN or driver's license number, to commit fraud. They may use your identity to take out loans, open credit cards, rent an apartment, purchase a car, file for bankruptcy and more.

These actions can hurt your credit score and result in failed background checks, limiting your ability to get a loan, rent an apartment or get a job. It can even lead to you having a criminal record for crimes you didn't commit, possibly resulting in a wrongful arrest.

How does the identity protection service work?

This service continually monitors for:

- Your SSN being used to complete a financial or service application
- Your address being changed
- High spending and other financial thresholds set by you
- Signs that your social media account has been hacked
- Signs that you're receiving scam phone calls
- Significant changes to your home title

We also regularly scan thousands of websites and millions of data points for signs that your info is being shared or sold on the dark web. If we detect that your info is compromised, we let you know right away.

Where do we look for your info?

- Over 10,000 forums and websites
- Over 500 internet relay chat (IRC) channels
- Over 200 Twitter feeds
- Over 114 peer-to-peer (P2P) servers
- Over 80 hidden web services
- Over 100 command and control (C&C) servers and over 150,000 compromised hosts
- Over 320 torrent sources

U.S. Bank Protect 360 FAQ

What personal info can we look for?

- Names
- Dates of birth
- Social Security numbers
- Phone numbers
- Email addresses
- Addresses
- Bank account numbers (with premium)
- Credit card info (with premium)
- Passport info (with premium)
- Medical ID numbers (with premium)

How do identity thieves get my info?

Identity thieves can use any number of methods to get your personal info, including:

- Going through your trash at home or work to find bills and credit statements that contain sensitive info
- Stealing credit and debit card numbers with a special information storage device in a practice known as “skimming”
- Stealing your wallet or purse to get your driver's license, debit cards and credit cards
- Changing your address with the postal service, so that the identity thief receives your tax information and credit card statements
- Stealing your mail
- Using a phone camera to take a picture of your credit card or ID when you buy something or go to the bank in person
- Scamming info from you by posing as someone you will trust, like someone who works at a trusted institution or a government official
- Stealing records about you from an organization, either by being an employee, bribing an employee, conning info out of an employee or hacking into the organization's computers

U.S. Bank Protect 360 FAQ

How can I protect myself from identity thieves?

Minimize your risk by protecting and monitoring your info with an institution you trust. Early detection of fraud greatly reduces the financial, emotional and legal burden of identity theft.

Other tips to protect your identity

- Don't carry your Social Security card in your wallet or in your purse.
- Don't provide your SSN to just anyone. Only a few organizations can require your SSN, including motor vehicle departments, tax departments, welfare departments, and organizations that perform tax transactions like your employer, bank and other financial institutions. For anyone else, ask if they will accept an alternative proof of ID.
- Don't put your SSN on your driver's license or on personal checks.
- When exchanging personal info or making a payment, watch for people who may try to look over your shoulder, eavesdrop or take a picture.
- Shred mail and other documents with personal info on them, like credit card and bank statements, credit card offers, utility bills and tax documents.
- Use a locked mailbox to send and receive mail.
- Regularly check your public record profile to ensure all the info reported is correct.
- Regularly monitor your credit reports to ensure all the info listed is correct.
- Learn how to recognize “phishing” emails. Never give out your SSN, credit card numbers, user IDs or passwords via email.
- Learn how to recognize “vishing” phone calls. Don't give out sensitive info to someone on the phone unless you initiated the call and it's a legitimate institution.

U.S. Bank Protect 360 FAQ

How can I tell if I am a victim of identity theft?

Consistently monitor both your financial and public record info and look for:

- Unfamiliar addresses, criminal records, court records or bankruptcies
- Unfamiliar charges or withdrawals in your credit card or bank transactions
- Credit accounts that you didn't open on your credit report

Other signs that your identity has been compromised:

- You stop receiving bills and other mail. This may signal an identity thief has changed your address with the provider or the postal service.
- You're served court papers or arrest warrants for things you didn't do.
- You receive credit cards you didn't apply for.
- You're denied credit for no apparent reason.
- You receive calls or letters from debt collectors for debts that aren't yours.
- You receive calls or letters from businesses about something you didn't buy.

What should I do if I am a victim of identity theft?

With premium, our expert team will take care of the entire recovery process and cover up to \$1 million in eligible costs.

If you need help restoring your identity, call our specialists at 833-568-6249. We accept relay calls.

To file a reimbursement claim, or if you have questions about the identity theft insurance policy, call us at 866-237-5240. We accept relay calls.

With essentials, you still have options. Visit identitytheft.gov to report your identity theft to the federal government and get resources for recovery. Then, consider taking the following steps:

Report your identity theft to the Federal Trade Commission (FTC).

Complete the form at identitytheft.gov or call the FTC at 877-438-4338 to file a report. This report proves to businesses that someone stole your identity and grants you certain rights.

U.S. Bank Protect 360 FAQ

Contact creditors and other companies where you know your identity was used.

Call the fraud department or customer service. Explain that someone stole your identity. Depending on the type of account, ask them to change the account number, close the account or freeze the account. Get replacement cards with new account numbers. Ask them to put a passphrase or PIN on your account, so no one else will be able to access it. Consider changing your login info and PINs for your accounts.

You can also follow up on your phone conversations with a letter to the company that summarizes your request in writing.

Place a fraud alert with the major credit bureaus.

A fraud alert tells businesses that check your credit that they should contact you before opening a new account. Fraud alerts last one year.

You only need to contact one of the three major credit bureaus: Equifax, Experian or TransUnion. The one that you contact is responsible for contacting the other two on your behalf. You can find their phone numbers and websites at identitytheft.gov/creditbureaucontacts.

File a police report.

Go to your local police or sheriff's office with:

- A copy of your FTC Identity Theft Report
- Your government-issued photo ID
- Proof of your address, like a rental agreement, mortgage statement or utility bill
- Any other proof you have of the theft, like bills and IRS notices

Tell the police that someone stole your identity and you need to file a report. Ask for a copy of the police report. You may need it in the future to prove you are a victim.