



Your Guide to Benefit describes the benefit in effect as of 02/01/2021. Benefit information in this guide replaces any prior benefit information You may have received. Please read and retain for Your records. Your eligibility is determined by Your financial institution.

Visa Platinum Rewards® Card

Identity theft continues to evolve and so do NortonLifeLock™ solutions

No one can prevent all identity theft, so staying informed and knowing what to do when your identity is threatened can give you greater peace of mind. ID Navigator Powered by NortonLifeLock provides you with the tools to help keep you informed of potential threats to your identity so you can act quickly.

The dark web is continuously patrolled for information that may belong to you, and you're notified if it's found. Should large-scale data breaches occur, NortonLifeLock will keep you informed.

To help detect credit fraud, key changes to your credit file are monitored with One –Bureau 1 Credit Monitoring. And if your wallet is stolen, you'll receive guidance to help cancel or replace credit cards, insurance identification and other key documents.

Should you do become a victim of identity theft, a U.S.-based Identity Restoration Specialist will help guide you on the next steps to take to help resolve the issue.

As a Visa cardholder, you will also have access to special discounts on other NortonLifeLock™ products.

To confirm eligibility, visit www.cardbenefitidprotect.com. Once verified, you will be redirected to the offer page on Norton.com where ID Navigator enrollment is available.

Smart tools to help against the evolving threat of identity theft

How ID Navigator Powered by NortonLifeLock can help provide you with greater peace of mind:

- Dark Web Monitoring** continuously patrols the dark web and private forums looking for personal information that may belong to you. Should it be found, notifications are sent with suggested steps.
- Data Breach Notifications** sends notifications on large-scale breaches so you can act quickly should a breach affect your personal information.
- Stolen Wallet Assist** A stolen wallet can mean a lost identity. If your wallet is stolen you will receive guidance to help you cancel or replaced key documents like your credit cards, driver's licenses, Social Security cards, insurance cards and more.
- One-Bureau Credit Monitoring Alerts** helps you stay on-top of your credit to help

detect fraud more quickly, alerts are sent when key changes are made to your credit file with a major credit bureau.

- Credit, Bank & Utility Account Freezes** provides instructions and links so you can quickly freeze credit, bank and utility files with each consumer reporting company to help protect you against criminals opening unauthorized accounts in your name.
- Restoration Assist** US-based Identity Restoration Specialists are available Monday to Friday 6a.m. – 5p.m. PST with guidance and with next steps to assist you should you become a victim of identity theft or other suspicious activity. Note: Visa Cardholders will have access to special discounts if they are interested in purchasing a more robust identity theft offering that includes features such as the LifeLock Million Dollar Protection™ Package.
- US-based Member Services & Support** is available Monday to Friday 6 a.m. – 6 p.m. PST; and Saturday 7 a.m. – 1 p.m. PST.

No one can prevent all identity theft.

1-Two requirements must be met to receive the One-Bureau Credit Monitoring feature: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file that contains sufficient credit history information. If these requirements are not met you will not receive credit features from Equifax. You will receive Credit Features once the verification process is successfully completed. Any credit monitoring from Equifax will take several days to begin after your successful plan enrollment.

Below you will find answers to questions about the benefit:

Q: How is the personal data I enter for Dark Web Monitoring stored and managed?

How do I know my personal data shared with NortonLifeLock is secure?

A: Your personal data is stored and managed by an advanced secure cloud database which is encrypted and protected with multiple layers of security measures.

Q: How can I be sure the personal data I enter for Dark Web Monitoring is not used or sold by NortonLifeLock employees?

A: Any personal data you provide is encrypted. Only a few selected employees, who undergo training on how to handle personal data can access it. These employees must provide their own unique credentials every time they access personal data and are subject to monitoring by our Information Security and Compliance team. See the NortonLifeLock™ Global Privacy Statement for additional details.

Q: Can NortonLifeLock remove my personal data from the dark web?

A: Unfortunately no. The content on the dark web is not centralized and is owned by many different (usually anonymous) owners. Only the owner of the content could remove or modify the content.

Q: How does NortonLifeLock help if I receive a Dark Web Monitoring notification?

A: Within the notifications, advice is provided on next steps you can take to help protect your personal data, and when available, it will include links to additional resources. If you have additional questions, go to support.norton.com.

Q: How does NortonLifeLock help if my personal data was leaked in a data breach?

A: Notifications are sent that provide best practices and suggested next steps you can take to help protect your personal data at support.norton.com

Q: How do I enroll? What information will I need to provide?

A: Visa cardholders should visit www.cardbenefitidprotect.com, and complete the eligibility verification. Once verified, cardholders will be redirected to the offer page on Norton.com where ID Navigator enrollment is available. Enrollment in ID Navigator will require first name, last name, SSN, date of birth, address, phone number, and email address.

Q: What are some common triggers for dark web, credit, and data breach notifications?

A: Your personal information being detected on the dark web, a hard credit check, or an update to your credit file are a few examples. Data breach notifications are sent regarding large data breaches that may impact consumers

Q: I received an alert. What do I do next?

A: Each alert will include information about next steps. Specifics vary by type of alert.