Frequently Asked Questions

Below you will find answers to questions about the benefit.

Q: How is the personal data cardholders enter for Dark Web Monitoring stored and managed? How do cardholders know their personal data shared with NortonLifeLock is secure?

Personal data is stored and managed by an advanced secure cloud database, which is encryptedand protected with multiple layers of security measures.

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

Any personal data 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 NortonLifeLockTM Global Privacy Statement for additional details.

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

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 can remove or modify the content.

Q: How does NortonLifeLock help cardholders who receive a Dark Web Monitoring notification?

Within the notifications, advice is provided on next steps they can take to help protect their personal data. When available, it will include links to additional resources. If cardholders have additional questions they can go to support.norton.com.

Q: How does NortonLifeLock help if a cardholder's personal data is leaked in a data breach?

Notifications are sent that provide best practices and suggested next steps they can take to help protect their personal data. Plus, they can visit support.norton.com.

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

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

Q: If a cardholder receives an alert, what should they do next?

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