

Know more about Mastercard ID Theft Protection – Lite

Here are some Frequently Asked Questions to assist end customers:

What is ID Theft Protection - Lite?

ID Theft Protection – Lite is an identity monitoring and alerts solution. It provides proactive monitoring and alerts of identity theft threats on all sources of identification that you register into the ID Theft Protection portal.

What is identity monitoring and why is it important?

Identity monitoring continually monitors for suspicious activity that endangers your personal information and alerts them via email whenever activity is found that requires you to take action. ID Theft Protection scour the deepest corners of the internet, searching for compromised credentials and potentially damaging use of your personal information, detecting fraud at its inception, and alerting you so you can take immediate action. You will see an alert if we detect:

- Compromised credentials such as your username, email address, or passwords within a corporate data breach, malicious third-party botnets, or criminal forums.
- Black Market activity related to your personal information such as your name, address, date of birth, or information that you provide on your portal for monitoring such as your debit/credit cards, insurance information, driver's license, and more.

By proactively monitoring for fraud, you can easily detect and stop fraud before more damage is done. ID Theft Protection is predictive and can detect when your identity is at an elevated risk for identity theft – this allows you to take necessary precautions and immediate preventative measures to minimize damages.

Limitation: ID Theft Protection-Lite is provided as a tool to protect your personal information and identity; however, the product does not offer a guarantee of information and identity protection. There are a lot of ways that criminals can get hold of someone's credit card number and or personal information without it being part of a breach and/or appearing on the dark/deep web. For example, RFID readers can capture credit card signals; pickpockets can steal physical credit cards; individuals can put credit card readers on gas pumps or ATMs to scan cards. All this information can be shared with criminals without the data being placed on the deep and dark web. ID Theft Protection provides industry-leading and verified alert notifications, by matching the data on the deep and dark web to individual customer profiles, as we strive to minimize false positives and duplicate records that exist in the market.

Does ID Theft Protection – Lite work on a mobile device?

Yes, ID Theft Protection portal is optimized to work on any browser-enabled smartphone, tablet or other mobile device.

How does ID Theft Protection – Lite work?

- You will first have to activate your account by entering your 16-digit Mastercard card number/phone number/promo code and fill up required fields on email address
- You will receive an email or SMS to complete activation by registering other necessary fields
- Once activation is completed, you can input all your personal identifiable information in the portal
- All personal identifiable information input in the portal will be monitored via scans in the deep, dark, surface webs
- Should there be any identity theft threats, you will receive email alerts on the cases and can view them in the alerts tab in the portal
- You can obtain the self-service resolution kit to view best practices and suggestions on how to prevent and act upon a case of identity theft

What are the steps required for me to register for access to ID Theft Protection portal?

- You can access [ID Theft Protection South Asia portal](#)
- **For first-time users:** You must activate your account by entering your 16-digit Mastercard card number/phone number/promo code and fill up required fields on email address
 - You will receive an email to complete activation by registering other necessary fields
 - Once activation is completed, you can input all your personal identifiable information in the portal
- **For returning users:** You can login directly at login page with your registered email address and password

How do I input personal identifiable information on ID Theft Protection portal?

In the dashboard, you can click on “Add Monitoring Items” under monitoring as illustrated in the screenshot below:

Your Recent Alerts
View your alerts and take action to keep your identity safe.
This summarizes the last 30 days of activity.
[View All Alerts](#)

Recommended Next Steps:
Add monitoring items to enhance your protection

Identity Monitoring
12 Items

Essentials
Email, Phone, Home

Financial Well-Being
Credit, Debit, Prepaid, Loyalty & Frequent Flyer, Bank Accounts

Identity, Cards & Documents
Passports, Driver's License

Insurance Documents

[Add Monitoring Items](#)

Resources
Visit our Resources to read articles and learn more about how to safeguard your identity.
[View](#)

Help Center
Visit our Help Center to answer common questions about your portal and services.
[View](#)

Add Items to Monitor
The online monitoring dashboard is the primary interface for consumers. It serves as a repository of all the PII data the consumer wants to monitor. Tracks and displays items being monitored.

By clicking on “Add”, you will be navigated to the identity monitoring page where you can input your personal identifiable information. Screenshots below for reference:

Identity Monitoring

Essentials
Identity thieves can do a lot of damage with your essential information. Add these essential items, the most critical items to check.

Financial Well-Being
Don't let thieves spend your money. For added security, we only require partial information.

Identity, Cards & Documents
Your identification documents and cards are prime targets for identity theft and fraud. Add these items to prevent an identity thief from becoming you.

Add Driver's Licenses

This item will be added to Identity Monitoring.

Nickname

License Number

Request

[Start Monitoring](#)

Monitored
It looks like you haven't yet added any Driver's Licenses. Add your information to get started.

Why is it important?
Thieves can use this information to verify your identity to create online and financial accounts in your name.

Alerts
An always-on service that monitors the results of an alert to decide if action is needed.

Date Received	Monitoring Type	Source of Exposure	Reason
1/11/2023	Identity	Dark Web	Phishing
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Phishing
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Unknown
1/11/2023	Identity	Dark Web	Unknown

Alerts Explained
"Date Received" is the date we discovered the activity. We sometimes receive notices or patterns, such as the presence of your name on a list, that are not specific to you.
If the activity that gives action to your item, you will receive email and/or SMS notification.
"Dark Web" is the place where stolen information is sold. It is not a specific place, but a collection of places where stolen information is sold.
"Phishing" is the act of trying to get you to give up your information by pretending to be someone you know or a trusted organization.

What does this mean?
Your information was found in a known data breach.

What should I do?
• One or more pieces of your personal or account information may have been exposed. The exposure is that you gave attention to your account and we may have any information exposed to the public.
• If your username and/or password was found, immediately change the password for this account and for any other accounts that use the same password. Also, verify that no changes were made to your security settings in the compromised area.
• Review your account information and verify that it is correct. If you are unsure, contact your account provider for assistance.
• Review your personal information to ensure that it is correct. If you are unsure, contact your account provider for assistance.

What this Exposure
Username, Email, User ID, Social Security Number, Email Address

What is included in the list of personal identifiable information that I can input on ID Theft Protection portal to have it monitored?

The list below reflects the personal identifiable information that you can input in the portal:

ALERT	Drivers Licenses
	Passport Numbers
	Email Addresses
	Debit/Credit Cards
	Bank Account Numbers
	Username, Social Media Handles
	Mother's Maiden Name
	Address
	Phone numbers
	Gamer Tag
	IP Address
	Insurance Cards
	Loyalty/Frequent Flyer Cards

Can I input credit/debit cards from other brands on ID Theft Protection portal to have it monitored?

You can input credit/debit cards from other brands in the ID Theft Protection portal, to have them monitored.

Are there any restrictions (i.e., number of addresses, etc.) to the personal identifiable information that I can input to monitor?

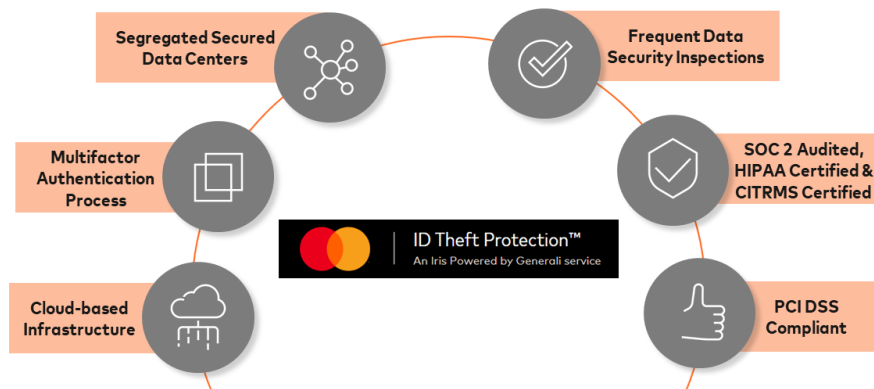
Please refer to the list below for the restrictions per monitoring item

ALERT	Drivers Licenses	Limit to 10
	Passport Numbers	Limit to 10
	Email Addresses	Limit to 10
	Debit/Credit Cards	Limit to 10
	Bank Account Numbers	Limit to 10
	Username, Social Media Handles	Limit to 10
	Mother's Maiden Name	Limit to 1
	Address	Limit to 10
	Phone numbers	Limit to 10
	Gamer Tag	Limit to 10
	IP Address	Limit to 10
	Insurance Cards	Limit to 10
	Loyalty/Frequent Flyer Cards	Limit to 10

How are my personal identifiable information secured on the ID Theft Protection portal?

Your actual personal identifiable information is never stored in Mastercard/GGA systems. When you enter your personal identifiable information, a random string of text (a unique ID, called hashing) is generated to represent the data before it is contained.

All information is stored in a private cloud-based infrastructure. All incoming traffic to Mastercard/GGA's networks is encrypted from browsers to Application Load Balances (ALB) via HTTP/TLS. The ID Theft Protection portal is the only public component of our infrastructure, and it is guarded by a web application firewall that can detect and prevent network intrusion/XSS attacks/DDoS attacks.

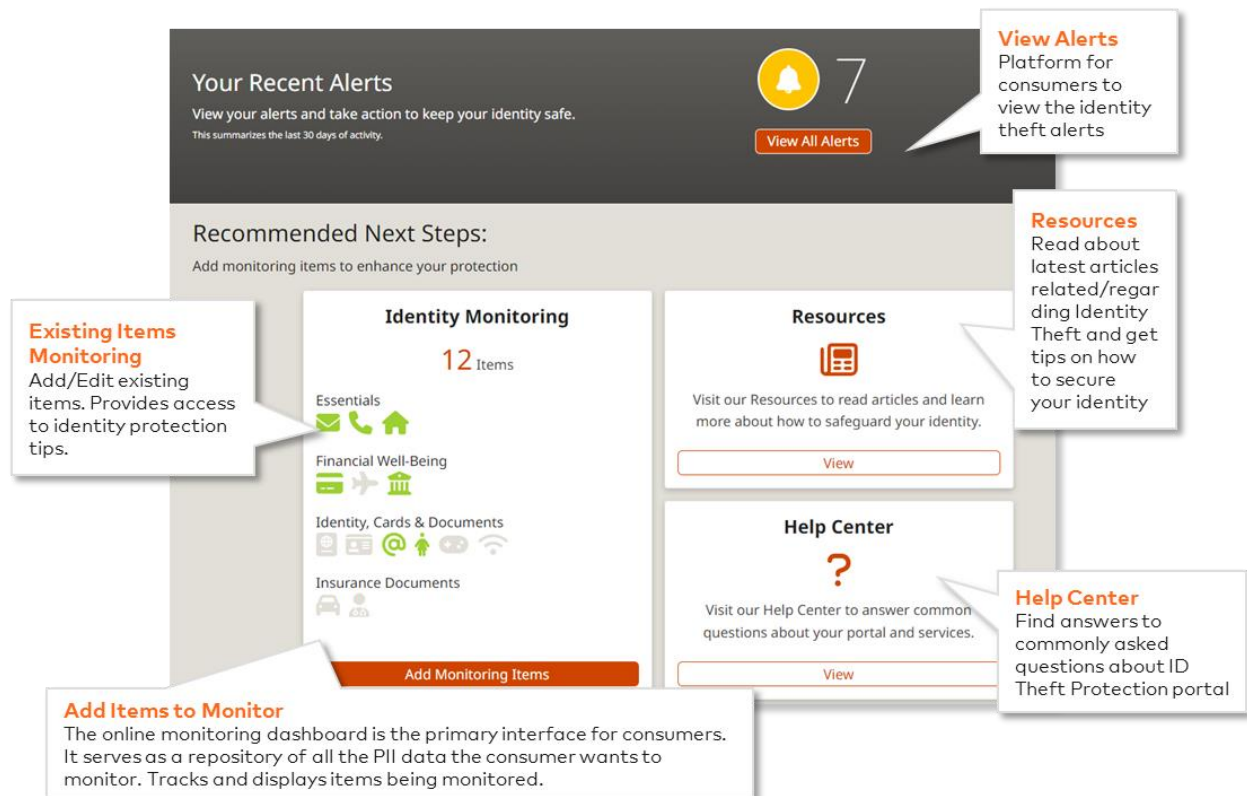


How can I be assured that Mastercard/GGA will not sell my data?

Personal information is not shared with third-party vendors, except if use of personal information is necessary to provide a service that has been requested, such as identity monitoring services. Except in such special circumstances, information will not be shared with any third-party, unless required by law to do so.

What is reflected on the ID Theft Protection dashboard?

You can get a quick view of the number of alerts you have received and the number of personal identifiable information being monitored on the dashboard page. You can also navigate to the identity monitoring page from the dashboard to register more data to be monitored or click into the alerts page to view past and current alerts. Screenshot of the dashboard included below for reference:



Your Recent Alerts
View your alerts and take action to keep your identity safe.
This summarizes the last 30 days of activity.

View Alerts
Platform for consumers to view the identity theft alerts

Recommended Next Steps:
Add monitoring items to enhance your protection

Existing Items Monitoring
Add/Edit existing items. Provides access to identity protection tips.

Identity Monitoring
12 Items

- Essentials
- Financial Well-Being
- Identity, Cards & Documents
- Insurance Documents

Add Monitoring Items

Add Items to Monitor
The online monitoring dashboard is the primary interface for consumers. It serves as a repository of all the PII data the consumer wants to monitor. Tracks and displays items being monitored.

Resources
Visit our Resources to read articles and learn more about how to safeguard your identity.

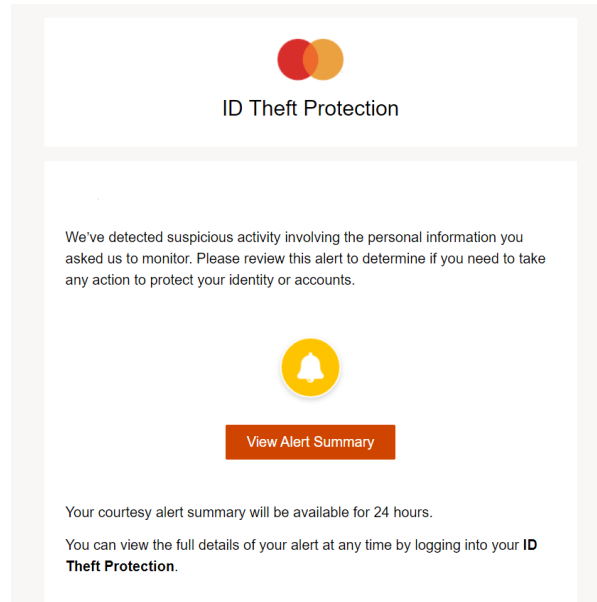
Resources
Read about latest articles related/regarding Identity Theft and get tips on how to secure your identity

Help Center
Visit our Help Center to answer common questions about your portal and services.

Help Center
Find answers to commonly asked questions about ID Theft Protection portal

How will I be alerted of any case of identity breach?

Upon a case of identity breach, you will be alerted via an email notification from ID Theft Protection. The email alert prompts the you to view the details of the breach on the ID Theft Protection portal. Screenshot of email alert included below for reference:



Will there be historical information of cases of identity breach related to the personal identifiable information registered?

Yes, the alerts section of the dashboard will also include historical data breaches where any registered personal identifiable information is found.

What should I do upon a case of identity breach?

If an identity breach is identified there will be additional instructions and recommendations in the details of the alert in the View Alerts page depending on what information was involved in the breach.

How do I access the Self-service ID Resolution Kit?

The Self-service ID Resolution Kit can be found in the Helpful Links section of the Profile page under “My Account”. It can be viewed online as well as downloaded.

What is the information available in the Self-service ID Resolution Kit?

The Self-service ID Resolution Kit includes best practices that guide end consumers on how to protect your identity/prevent a case of identity breach.

If I face a technical issue on ID Theft Protection portal, who should consumers reach out to?

To report a technical issue, please submit the form under Contact Us with details of what technical issue is occurring.