Mastercard Asia/Pacific (Australia) Pty Ltd ("Mastercard") Transparency Report:
ID Network Government Personal Information Requests
January 1 - December 31, 2022

1. Introduction

Transparency is a key value at Mastercard. Mastercard believes individuals and our customers have a right to understand how their personal data is handled, and we consider it our responsibility to provide them with the most current and state of the art privacy and security protections available. Mastercard has prepared the following report to provide information regarding requests Mastercard received from government agencies worldwide with respect to Mastercard Australia's ID Network from January 1 through December 31, 2022. In addition, this report explains our information practices, our commitment to privacy, as well as to increase transparency about our business.

2. Mastercard ID Data

Mastercard ID Network provides a technology platform and operational service to allow the secure storage, transmission and use of verified digital identity information based on user consent. Mastercard ID Network processes the following kinds of information, collectively referred to as "**Personal Information**":

- **Identity Information** such as contact details (name, billing address, phone number), identification data (data that derive from identity documents like age or nationality, national identification number), biometric data used to securely access ID as well as to verify users' documents, device details (device IP address, device ID); and
- **Activity Information** such as logs which contain a system-generated unique identifier, the date and time of actions performed by a user (enrolment, document verification), logs of consents.

For more information on how we handle Personal Information, please refer to our ID Global Privacy Notice.

Mastercard has designed the ID Network such that it has limited access to Personal Information:
- We do not hold any Identity Information – this is encrypted and stored on the user's device, and stored for a limited time by Identity Verification Providers (IVPs) for troubleshooting and customer support purposes; and
- We encrypt and store Activity Information securely in our servers – this information is restricted to the people and processes necessary to carry out ID transactions.

3. Government Requests for Data

On occasion, Mastercard may receive requests from law enforcement and other governmental agencies to provide Mastercard Australia ID Network Personal Information. Mastercard responds to these requests by: educating the inquiring agency about our limited data set; we then may refer them to the appropriate ID Network participant, which has a more comprehensive data relationship with the ID Network user, where appropriate. In those instances where a law enforcement or governmental agency further pursues a request, Mastercard ensures that they follow the applicable legal process. If there is a question about the legitimacy or scope of the request, we challenge it. Only when we are satisfied that the legal process is valid and appropriate do we deliver the narrowest possible set of data required to be responsive to the request.

Period for Mastercard Australia's ID Network Transparency Report is January 1 through December 31 for 2022
Requests for Personal Information

Year	Requests Received	ID Network User Subjects	Requests where no Personal Information was Provided	Requests where Personal Information was Provided
2022	0	0	0	0

4. Commitment to Privacy & Data Protection

Mastercard builds privacy and data protection into the fabric of our business and has a longstanding commitment to privacy. The way we handle data is a vital part of our responsibility to our customers, cardholders and employees and is part of how we earn their trust.
- Culture – We believe that privacy and data protection are fundamental human rights, and this belief informs all our business decisions. Our corporate mission focuses the organization's efforts to make payments safe, simple and smart, and incorporates privacy into our business practices. We ensure privacy and data are protected and we regularly conduct training to assist this understanding.
- Board/Executive Oversight - Mastercard's commitment to privacy starts at the highest levels of the organization, with our Board of Directors and Chief Executive Officer. Mastercard has a Chief Privacy Officer and a Chief Data Officer and has created

a global team of professionals responsible for administering a comprehensive privacy program. On an annual basis, or more frequently if needed, the Chief Privacy Officer provides a comprehensive assessment of the program and the related risks to the Audit Committee of our Board of Directors. Additionally, Mastercard has a Data Protection Officer who leads our Global Compliance Assurance program to ensure that Mastercard continues to adhere to global General Data Protection Regulation Standards and local privacy requirements.

- Accountability – Mastercard holds itself accountable for how it collects, uses and discloses personal data. Mastercard clearly explains how we handle personal information in our Global Privacy Notice including our use of data to fight fraud and identity theft, which is complemented by specific notices for certain products and activities. On a bi-annual basis Mastercard's security, privacy and information practices are reviewed by United States financial regulators for compliance with the requirements of U.S. financial privacy laws.
- Privacy by Design - We design, develop and deliver our products and services by placing the individual at the center, protecting and respecting their privacy and personal information along the way. Our privacy program is dedicated to ensuring legal compliance with applicable laws, setting standards and policies and implementing best practices to ensure privacy is embedded throughout our product life cycle. We are committed to the responsible handling of personal information and we balance our product development activities with a commitment to transparency and non-discrimination.
- Policy Development – We regularly work with governments, regulators, policy makers and industry bodies across the globe to enact strong privacy protections for individuals, while still enabling businesses to operate globally and use data for responsible innovation.

We are committed to engagement and understanding what our stakeholders think of our approach, our reporting on information practices and our commitment to privacy. If you have any questions or comments about this report or our privacy practices, please email us at: privacyanddataprotection@mastercard.com.

5. Key Definitions

"**Authority**" means any national or regional public authority or government agency, including law enforcement, national intelligence and regulatory supervision agencies.
"**Government Request**" means any request from an Authority in any country for Personal Information that is processed by Mastercard Australia's ID Network on Mastercard or its customers' behalf or processed by a third party on Mastercard's behalf.
"**ID Network User Subjects**" means the total number of ID users that were subjects of the total number of legal requests. For example, a single subpoena could request information about two ID Network users.
"**Requests Received**" means the number of Government Requests that Mastercard received for Personal Information.
"**Requests where no Personal Information was Provided**" means the request resulted in Mastercard objecting to the request or without responsive Personal Information so that no Personal Information was shared.
"**Requests where Personal Information Provided**" means the request resulted in Mastercard providing the narrowest possible set of Personal Information in response to a valid legal request.