Data Processing Agreement for Mastercard Identity Verification Services ("Data Processing Agreement")

Version March 6, 2024

1. Scope and Applicability

1.1. This Data Processing Agreement regulates the Processing of Personal Data by the Parties (as defined in the Principal Agreement) in the context of the provision of the Services specified in the Principal Agreement (defined below). Unless otherwise expressly stated in the Principal Agreement, this version of the Data Processing Agreement shall be effective and remain in force for the term of the Principal Agreement.

1.2. In addition, to the extent the Principal Agreement involves the Processing of Personal Data of individuals subject to European Data Protection Law, the Parties have agreed to the terms set forth in **Annex 2** of this Data Processing Agreement for the purpose of complying with European Data Protection Law (the "**European Addendum**"). To the extent the Principal Agreement involves the Processing of Customer Personal Data (as defined in Annex 3) by Mastercard of Consumers (as defined in Annex 3) subject to State Privacy Laws to provide the Services to Customer, Mastercard and Customer will comply with their respective obligations pursuant to the terms set forth in **Annex 3** of this Data Processing Agreement (the "**US Addendum**").

2. Obligations of the Parties. Each Party is responsible for the Processing of Personal Data for its own Business Purposes (as defined in the Principal Agreement) in the context of the Services specified in the Principal Agreement and each Party represents and warrants that, in relation to the Processing of Personal Data for its own Business Purposes in the context of the Services, it will:

2.1. comply with Privacy and Data Protection Law when Processing Personal Data in the context of the Services and performing their obligations under this Data Processing Agreement and be responsible for the compliance of their respective Affiliates and Users (Compliance with Laws);

2.2. cooperate with the other Party in good faith to fulfil their respective data protection compliance obligations under Privacy and Data Protection Law, including complying with individuals' requests to exercise their data protection rights and replying to investigations and inquiries from regulators as required under Privacy and Data Protection Law and notifying Personal Data Breaches and enter into additional terms to address any modifications, amendments, or updates to applicable statutes, regulations or other laws pertaining to privacy and information security (Cooperation and Assistance);

2.3. comply with the security requirements contained in **Annex 1** of this Data Processing Agreement and have implemented and maintain a comprehensive written information security program which includes appropriate technical, operational and organizational measures to protect from a Personal Data Breach. The appropriate measures must ensure a level of security appropriate to the risk, and as appropriate must include : (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing (Information Security Program);

2.4. notify the other Party, without undue delay, of a Personal Data Breach that relates to Personal Data Processed in the context of the Service and for which the other Party is a Controller (Notification of Personal Data Breaches);

2.5. inform the other Party without undue delay, in writing, of any request, question, objection, complaint, investigation or any other inquiry, received from any individual (including objections to processing and request for deletion), regulator or public authority of whatever jurisdiction, that relates to Personal Data Processed in the context of the Services, unless otherwise restricted by applicable law. Each Party will provide the other Party with a copy of any such requests within 48 (forty-eight) hours of receipt (i) for Mastercard, by email to TPRM@mastercard.com and SOC@mastercard.com; (ii) for Customer, by email to the email provided by Customer in the relevant Notice section of the Principal Agreement and will respond to such requests only in accordance with the other Party's prior written authorization, unless otherwise prohibited by applicable law (Notification Obligations). For clarity, this Section 2.5 does not apply to the fulfillment of Data Subject Rights requests submitted by Data Subjects to either Party in their roles as Controller under European Data Protection Law to the extent compliance with the European Data Protection

Law does not necessitate the notification of the other Party for the other Party's compliance with applicable Privacy and Data Protection Laws (Other Notification Obligations).

2.6. only disclose Personal Data to a third party in accordance with this Data Processing Agreement and Principal Agreement and will require such third party in writing to comply with Privacy and Data Protection Law applicable to the data being disclosed and with the same obligations as are imposed on each Party by this Agreement, as appropriate and relevant, unless it is not possible to do so, such as where the data recipient is a governmental authority (Data Disclosures).

3. Customer's Obligations.

3.1. **Customer's Privacy Policy.** Customer represents and warrants that Customer will provide Data Subjects with all notices in a timely manner and obtain from them all rights and consents necessary for the provision and transfer of such data to Mastercard in particular of the transfer and storage by Mastercard of their Personal Data outside the country in which it was collected (e.g., transfer to and storage in the United States) and the Processing of such data by or on behalf of Mastercard in accordance with Mastercard's privacy notice (which shall also be provided to the Data Subjects by the Customer via a link). As between Customer and Mastercard, Customer is solely responsible for providing such notice and obtaining such consent (Notice and Consents).

3.2. **Automated Decisions.** Should the Customer use the Services to make any automated decisions that produce legal effects on the Data Subjects or similarly significantly affect the Data Subjects, the Customer shall either:

3.2.1. implement at least a secondary measure in addition to the Services prior to making such automated decisions and ensure that the scores generated from the Services are not the strongest factor in the automated decision making; or

3.2.2. obtain the consent of the data subject for the automated decision to be carried out by Mastercard and provide a non-automated alternative if the Data Subject rejects the automated decision making.

3.3. **For 1-to-1 Profiling Authorized Use Cases.** To the extent and in the manner required by applicable Privacy and Data Protection Law, Customer represents and warrants that it will obtain any necessary consents, authorizations and permissions from Data Subjects on Mastercard's behalf for any Processing of Sensitive Data carried out by Mastercard in the context of the Services.

3.3.1. Customer will provide Mastercard with proof of each consent obtained on behalf of Mastercard in the form described in **Annex 4** ("**Proof of Consent**"). Customer will ensure that such Proof of Consent and any other information related to the consent is securely stored, and provided to Mastercard upon request, including but not limited to information allowing identification of the Data Subject that provided the consent, a copy of the consent capture form and a copy of the consent statement in force at the time consent was obtained.

3.3.2. Customer will ensure that consent is refreshed where required by Privacy and Data Protection Law applicable to either Party and without unreasonable delay.

3.3.3. Customer will further ensure that the Data Subjects can withdraw their consent in accordance with the valid consent requirements under applicable Privacy and Data Protection Law and in each instance where a Data Subject withdraws their consent, it shall inform Mastercard immediately in writing.

3.3.4. In addition, to the extent the Principal Agreement involves the Processing of Sensitive Data of individuals subject to European Data Protection Law, the Customer has agreed to the additional consent safeguards set forth in **Annex 4** ("**Additional Safeguards For 1-to-1 Profiling Authorized Use Cases**") of this Data Processing Agreement.

4. Definitions

"**1-to-1 Profiling Authorized Use Cases**" means any Authorized Use Case which involves the Processing of Sensitive Data. This includes but is not limited to the following: Continuous Validation with Behavioral Biometrics, NuDetect for Good User Validation, and NuDetect Behavioral Biometrics for Authentication. "**Binding Corporate Rules**", "**Controller**", "**Processor**", shall have the meanings given to them under applicable Data Protection Law to the extent such laws are applicable to the Personal Data being Processed.

"**Data Subject**" means a directly or indirectly identified or identifiable natural person whose Personal Data is Processed in the context of the Principal Agreement.

"**EEA Mastercard Binding Corporate Rules**" (or "**EEA Mastercard BCRs**") means the Mastercard Binding Corporate Rules as approved by the EEA data protection authorities and available at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.

"**EEA Personal Data**" means Personal Data to which the GDPR was applicable prior to its processing by the other Party.

"**European Data Protection Law**" means all of the following, each as amended and replaced from time to time: the EU General Data Protection Regulation 2016/679 ("**EU GDPR**") and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and their respective national implementing legislations; Swiss Federal Act on Data Protection ("**FADP**"); the Monaco Data Protection Act; the UK Data Protection Act 2018 and UK GDPR (together "**UK Data Protection Law**"); and the Data Protection Acts of the European Economic Area ("**EEA**") countries; each as applicable.

"**Personal Data**" (or "**Personal Information**") means any information relating to an identified or identifiable individual or as those terms are defined in applicable Privacy and Data Protection Law.

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, access to, or other unauthorized Processing of Personal Data transmitted, stored or otherwise Processed.

"**Principal Agreement"** means a written services agreement, an Order, an enrollment form, or any other relevant agreement entered into by the Parties which involves the Processing of Personal Data of Data Subjects subject to Privacy and Data Protection Law.

"**Privacy and Data Protection Law**" means any law, statute, declaration, decree, legislation, enactment, order, ordinance, regulation or rule (as amended and replaced from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which the Parties are subject, including but not limited to European Data Protection Law; the State Privacy Laws; the U.S. Gramm-Leach-Bliley Act; the Brazil General Data Protection Act; the Argentina Personal Data Protection Act 25.326; the South Africa Protection of Personal Information Act; laws regulating unsolicited email, telephone, and text message communications; security breach notification laws; laws imposing minimum security requirements; laws requiring the secure disposal of records containing certain Personal Data; laws governing the portability and/or cross-border transfer of Personal Data; and all other similar international, federal, state, provincial, and local requirements; each as applicable.

"**Processing of Personal Data**" (or "**Processing/Process**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, including any operation defined as "Processing" under applicable Privacy and Data Protection Law.

"**Protected Area**" means: in the case of EEA Personal Data, the members states of the European Union and the European Economic Area and any country, territory, sector or international organization in respect of which an adequacy decision under Art.45 GDPR is in force; in the case of UK Personal Data, the United Kingdom and any country, territory, sector or international organization in respect of which an adequacy decision under United Kingdom adequacy regulations is in force; and, in the case of Swiss Personal Data, any country, territory, sector or international organization which is recognized as adequate under the laws of Switzerland.

"**Sensitive Data**" means any Personal Data considered to be sensitive according to applicable Privacy and Data Protection Law and may include data revealing racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, or trade union

membership, criminal records, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

"**Standard Contractual Clauses**" means: in respect of EEA Personal Data, the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission under Commission Implementing Decision (EU) 2021/914, in accordance with clause 1.3 of the European Addendum ("**EU SCCs**"); in respect of UK Personal Data, the International Data Transfer Addendum issued by the UK Information Commissioner in accordance with s.119A of the UK Data Protection Act 2018 but, as permitted by clause 17 of such Addendum, the parties agree to change the format of the information set out in Part 1 of the Addendum in accordance with clause 1.4 of the European Addendum; and, in respect of Swiss Personal Data, the EU SCCs, provided that any references in the EU SCCs to the GDPR shall refer to the FADP.

"**State Privacy Laws**" means, collectively, all UNITED STATES state privacy laws and their implementing regulations, as amended or superseded from time to time, that apply generally to the processing of individuals' Personal Data and that do not apply solely to specific industry sectors (e.g., financial institutions), specific demographics (e.g., children), or specific classes of information (e.g., health or biometric information). State Privacy Laws include but are not limited to the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (California Civil Code §§ 1798.100 to 1798.199) ("**CPRA**"); Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("**ColoPA**"); Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("**CPOMA**"); Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("**UCPA**"); Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("**VCDPA**").

"**Swiss Personal Data**" means Personal Data to which the FADP was applicable prior to its processing by the other Party;

"**UK Mastercard Binding Corporate Rules"** (or "UK Mastercard BCRs") means the Mastercard Binding Corporate Rules as approved by the UK data protection authority and available at https://www.mastercard.us/content/dam/mccom/en-us/documents/mastercard-bcrs-february-2017.pdf.

"**UK Personal Data**" means the processing of personal data to which Privacy and Data Protection Law of the United Kingdom was applicable prior to its processing by the other Party.

Other capitalized terms have the meaning given to them in the Principal Agreement.

ANNEX 1

TECHNICAL AND ORGANIZATIONAL MEASURES

The Parties will, as a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, include:

- Establishing security areas, restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management, card-keys procedures;
- Door locking (electric door openers etc.);
- Security staff, janitors;
- Surveillance facilities, video/CCTV monitor, alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons include:

- User identification and authentication procedures;
- ID/password security procedures (special characters, minimum length, change of password);
- Automatic blocking (e.g. password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Creation of one master record per user, user master data procedures, per data processing environment.

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, include:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access Personal Data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure.

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, include:

- Tunneling
- Logging
- Transport security

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, include:

- Logging and reporting systems;
- Audit trails and documentation.

6. Availability control

Technical and organizational measures to ensure that Personal Data are protected against accidental destruction or loss (physical/logical) include:

- Backup procedures;
- Mirroring of hard disks (e.g. RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

7. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately include:

- Separation of databases;
- “Internal client” concept / limitation of use;
- Segregation of functions (production/testing);
- Procedures for storage, amendment, deletion, transmission of data for different purposes.

ANNEX 2
EUROPEAN DATA PROCESSING ADDENDUM

Customer, Mastercard, and Mastercard Europe agree that the terms and conditions set out below are added as a European Data Processing Addendum ("**European Addendum**") to, and form an integral part of, the Data Processing Agreement to which it is attached. This European Addendum regulates the Processing of Personal Data subject to European Data Protection Law. In the event of a conflict between the terms of this European Addendum and the Data Processing Agreement with respect to the subject matter of this European Addendum, the terms of this European Addendum will control to the extent of such conflict.

1. **Roles of the Parties**. Each Party agrees that, in relation to the Processing of Personal Data for its own Business Purposes in the context of the Services, it acts as a Controller.

2. **Additional Safeguards For 1-to-1 Profiling Authorized Use Cases.** Subject to section 3.3 of the Data Processing Agreement, Customer represents and warrants that prior explicit consent will be obtained from Data Subjects on Mastercard's behalf for any Processing of Sensitive Data carried out by Mastercard in the context of the Services using the consent statement provided by Mastercard in **Annex 4**, as may be updated from time to time ("**Mastercard Consent Statement**"). In addition, Customer represents and warrants that it will provide to Mastercard upon request a copy of the Mastercard Consent Statement in force at the time consent was obtained and will ensure that consent is refreshed whenever Mastercard provides an updated version to Customer of the Mastercard Consent Statement.

3. **International Data Transfers**.

   3.1. Mastercard and Customer may transfer either directly or via onward transfer the Personal Data Processed in connection with the Services outside of Protected Area in accordance with European Data Protection Law.

   3.2. Mastercard represents and warrants that it will abide by the EEA or the UK Mastercard BCRs when Processing Personal Data for its own Business Purposes in the context of the Services.

   3.3. By signing this DPA, Mastercard and Customer conclude Module 1 (Controller-to-Controller) of the SCCs, which is hereby incorporated by reference and completed as follows: the "data exporter" is Mastercard; the "data importer" is Customer; the optional docking clause in Clause 7 is implemented; the optional redress clause in Clause 11(a) is struck; Option 1 of Clause 17 is implemented and the governing law is the law of Belgium; the courts in Clause 18(b) are the Courts of Brussels, Belgium; Annex I and II to the SCCs are Annex 1 and Schedule 1 to this European Addendum respectively. For International Data Transfers of Swiss Personal Data the Swiss Data Protection Authority ("FDPIC") shall also be a competent supervisory authority and the term 'member state' must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the EU SCCs.

   3.4. By signing this DPA, Mastercard and Customer conclude the UK Addendum which is hereby incorporated and applies to International Data Transfers of UK Personal Data. Part 1 of the UK Addendum is completed as follows: (i) in Table 1, the "Exporter" is Mastercard and the "Importer" is Customer, their details are set forth in this European Addendum and the DPA; (ii) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 4.3 of this Europe Addendum; (iii) in Table 3, Annexes 1 (A and B), and II to the "Approved EU SCCs" are Annex 1 and Schedule 1 to Annex II of the DPA (with no requirement for signature). For the purposes of UK Addendum the governing law is the law of England and Wales and the governing courts are the courts of England and Wales.

   3.5. If either Party's compliance with European Data Protection Law is affected by circumstances outside of either Party's control, including if a legal instrument for transfers is invalidated, amended, or replaced, then the Parties will inform one another promptly and work together in good faith to reasonably resolve such non-compliance.

SCHEDULE 1 to ANNEX II- DETAILS OF PROCESSING

This table provides the details of processing required for Annex I of the Standard Contractual Clauses

EKATA SERVICES

Categories of Data Subjects whose personal data is transferred	Categories of personal data transferred	Special Categories of Data transferred	Frequency of the Transfer	Nature of the Processing	Purpose of data transfer and further processing	Retention Period	International Transfer basis/ Module of the SCCs	List of Parties	
								Disclosing Part(ies)	Receiving Part(ies)
End Users of the Customer	Contact information. For example, Name (including first, last, middle initial and any combination thereof), IP address, Address, Phone Number.	Not Applicable	The Personal Data will be transferred on a continuous basis.	Personal Data may be Processed pursuant to the Principal Agreement for the performance of the Services. For example, storing, matching, and analyzing to create fraud signals for the Customer.	Mastercard transfers Personal Data to Customer pursuant to the Principal Agreement for the performance of the Services. For example, to deliver fraud risk scores and insights to the Customer for the Customer.	Personal Data may be Processed and stored for the period necessary to fulfill the agreed Business Purposes pursuant to and for the duration of the Principal Agreement and to comply with applicable privacy and data protection laws and regulations.	SCCs – Module 1 transfer to the United States	Mastercard Europe (Controller)	Customer or its Affiliates based outside of the Protected Area (Controller)

NUDETECT SERVICES

Categories of Data Subjects whose personal data is transferred	Categories of personal data transferred	Special Categories of Data transferred	Frequency of the Transfer	Nature of the Processing	Purpose of data transfer and further processing	Retention Period	International Transfer basis/ Module of the SCCs	List of Parties	
								Disclosing Part(ies)	Receiving Part(ies)
End Users of the Customer	Unique Identifiers such as account id, username, email, phone number etc., device information such as device fingerprint, device id, IP address etc., applications information such as account identifier, session identifier.	Passive biometrics. For example, timing between keystrokes, window scroll position time and location of mouse clicks.	The Personal Data will be transferred on a continuous basis.	Personal Data may be Processed pursuant to the Principal Agreement for the performance of the Services. For example, storing, matching, and analyzing to create fraud signals for the Customer.	Mastercard transfers Personal Data to Customer pursuant to the Principal Agreement for the performance of the Services. For example, to deliver fraud risk scores and insights to the Customer for the Customer.	Personal Data may be Processed and stored for the period necessary to fulfill the agreed Business Purposes pursuant to and for the duration of the Principal Agreement and to comply with applicable privacy and data protection laws and regulations.	SCCs – Module 1 transfer to the United States	Mastercard Europe (Controller)	Customer or its Affiliates [based outside of the Protected Area] (Controller)

ANNEX 3
UNITED STATES State DATA PROCESSING ADDENDUM

This UNITED STATES State Data Processing Addendum (the "US Addendum") forms part of the Principal Agreement to which it is attached. This US Addendum regulates the Processing of Personal Data of Consumers subject to the State Privacy Laws. If there's a conflict between this US Addendum and the Principal Agreement regarding the subject matter of this US Addendum, the terms of this US Addendum will prevail in that conflict. The terms used in this US Addendum have the meaning set forth in Section 1. Except as modified below, the terms of the Principal Agreement remain in full force and effect. Exhibit 1 forms an integral part of this US Addendum.

NOW, THEREFORE, the Parties agree as follows:

1. Applicability and Roles.

1.1. **Applicability.** This US Addendum applies only to: Mastercard's Processing of Customer Personal Data for the nature, purposes, and duration set forth in Exhibit 1a; and Mastercard's Sale of Mastercard Personal Data to Customer for the purposes set forth in Exhibit 1b.

1.2. **Roles of the Parties.** For the purposes of the Principal Agreement and this US Addendum:

1.2.1. Customer Personal Data. Customer is the Party responsible for determining the purposes and means of Processing Customer Personal Data as the Controller and appoints Mastercard as a Processor to Process Customer Personal Data as set forth in **Exhibit 1a**; and

1.2.2. Mastercard Personal Data. Mastercard is the Party responsible for determining the purposes and means of Processing Mastercard Personal Data as the Controller and Customer is the Third Party to whom Mastercard Personal Data is Sold for the limited and specific purposes set forth in **Exhibit 1b** and pursuant to the obligations set forth in Section 6.

2. Compliance.

2.1. **Compliance with Obligations**. Mastercard, its employees, and agents, with respect to the Processing of Customer Personal Data understand and shall comply with this US Addendum and upon the reasonable request of Customer, Mastercard shall make available to Customer all information in Mastercard's possession necessary to demonstrate Mastercard's compliance with this subsection.

2.2. **Compliance Assurance.** Customer has the right to take reasonable and appropriate steps to ensure that Mastercard uses Customer Personal Data consistent with Customer's obligations under applicable State Privacy Laws.

2.3. **Compliance Monitoring.** With respect to the Processing of Customer Personal Data, Mastercard shall, with Customer's consent, arrange for a qualified and independent assessor to conduct an assessment, at least annually and at Mastercard's expense, of Mastercard's policies and technical and organizational measures in support of the obligations under this US Addendum using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Mastercard shall provide a report of such assessment to Customer upon request.

2.4. **Compliance Remediation.** Mastercard shall promptly notify Customer if it determines that it can no longer meet its obligations under applicable State Privacy Laws with respect to Mastercard's Processing of Customer Personal Data. Upon receiving notice from Mastercard in accordance with this subsection, Customer may direct Mastercard to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

3. Restrictions on Processing.

3.1. **Limitations on Processing.** Mastercard will Process Customer Personal Data as instructed in the Principal Agreement, this US Addendum, and as permitted by the State Privacy Laws. Except as expressly permitted by the State Privacy Laws, Mastercard is prohibited from (i) Selling or Sharing Customer Personal Data, (ii) retaining, using, or disclosing Customer Personal Data for any purpose other than for the specific purpose of performing the services specified in Exhibit 1a, (iii) retaining, using, or disclosing Customer Personal Data outside of the direct

business relationship between the Parties, and (iv) combining Customer Personal Data with Personal Data obtained from, or on behalf of, sources other than Customer.

3.2. **Subcontractors; Sub-processors**. Mastercard's current subcontractors and sub-processors are set forth in Exhibit 2. Mastercard shall notify Customer of any intended changes concerning the addition or replacement of subcontractors or sub-processors. Further, Mastercard shall ensure that Mastercard's subcontractors or sub-processors who Process Customer Personal Data on Mastercard's behalf agree in writing to the same or equivalent restrictions and requirements that apply to Mastercard in this US Addendum and the Principal Agreement with respect to Customer Personal Data, as well as to comply with the applicable State Privacy Laws.

3.3. **Right to Object**. Customer may object in writing to Mastercard's appointment of a new subcontractor or sub-processor on reasonable grounds by notifying Mastercard in writing within 30 calendar days of receipt of notice. In the event Customer objects, the Parties shall discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution.

3.4. **Obligations at Termination.** Upon termination of the Principal Agreement except as set forth therein or herein, where required by State Privacy Laws, Mastercard will discontinue Processing and delete Customer Personal Data in its possession without undue delay and shall direct its subcontractors and sub-processors to do the same. Mastercard may retain Customer Personal Data to the extent required by law but only to the extent and for such period as required by such law and always provided that Mastercard shall ensure the confidentiality of all such Customer Personal Data.

4. Consumer Rights.

4.1. Mastercard shall provide commercially reasonable assistance, where required under the State Privacy Laws, to Customer for the fulfillment of Customer's obligations to respond to Consumer Requests.

4.2. Customer shall inform Mastercard of any Consumer Request that Mastercard must comply with under State Privacy Law. Customer shall provide Mastercard with the information necessary for Mastercard to comply with the request.

5. Definitions.

"**Consumer**", "**Sale**," "**Selling**," and "**Sold**" have the meanings defined in the State Privacy Laws.

"**Controller**" means "Controller" or "Business" as those terms are defined in the State Privacy Laws.

"**Customer Personal Data**" means Personal Data provided by Customer to, or which is collected on behalf of Customer by, Mastercard to provide services to Customer pursuant to the Principal Agreement.

"**Mastercard Personal Data**" means the Personal Data of California residents subject to the CPRA that is Sold to Customers by Mastercard to provide services to Customer pursuant to the Principal Agreement.

"**Processor**" means "Processor," "Service Provider," or "Contractor" as those terms are defined in the State Privacy Laws.

"**Share**", "**Shared**", "**Sharing**" and "**Third Party**", have the meaning defined in the CPRA.

Other capitalized terms have the meaning given to them in the Principal Agreement. In the event of a conflict in the meanings of defined terms in the State Privacy Laws, the meaning from the law applicable to the state of residence of the relevant Consumer applies.

Exhibit 1a - Customer Personal Data Processing Details

Nature and Purpose of the Processing	Processing Customer Personal Data to create Insights and algorithmic models to provide the Services.
Types of Customer Personal Data Subject to Processing	The types of Personal Data included in the Customer Personal Data that Mastercard Processes for Processor Services Purposes are the following: For Ekata: First and last name, address, email address, IP address and phone number For NuDetect: Unique Identifiers such as account id, username etc., device information such device id, IP address etc., applications information such as account identifier, session identifier etc., behavior based interactions such as timing between keystrokes, time and location of mouse clicks etc..
Processing Duration	Customer Personal Data will only be Processed for as long as necessary to provide the Services.

Exhibit 1b - Mastercard Personal Data Processing Details

Purpose(s) of Processing	Customer Processes Mastercard Personal Data to detect and prevent fraud.

Exhibit 2 - Sub-Processor Details

To support delivery of Mastercard's services, Mastercard may engage and use third parties as sub-processors to Process certain Customer Personal Data. This Exhibit 2 provides information about the identity, location, and role of each sub-processor.

Name and address of Sub-Processor	Location(s) where Personal Data are stored or from which Personal Data are accessed by the Sub-Processor	Description of Processing (including a clear delimitation of responsibilities in case several Sub-Processes are authorized)
Amazon Web Services 410 Terry Avenue North Seattle, WA 98109	USA, Germany, Ireland, Singapore, Australia	Cloud hosting services for NuDetect & Ekata Services
Sumo Logic 305 Main St., Redwood City, CA 94063	USA	Logging service and storage
NetNumber 650 Suffolk Street, Lowell, MA 01854	USA	Processing limited to append additional information to be passed back to Customer
Neustar 1906 Reston Metro Plaza Suite 500, Reston, VA 20190	Co-located with API endpoints, USA	Processing limited to append additional Personal Information to be passed back to Customer
GoodData Corporation	USA	Processing limited to the provisions of the NuDetect Dashboard to enable customers to visualize analytics on their platform.

ANNEX 4 - Additional Safeguards For 1-to-1 Profiling Authorized Use Cases

PROOF OF CONSENT

1. **Proof of Consent**

   Proof of consent will be provided in the form of a unique reference number for each Data Subject and timestamp of the consent.

MASTERCARD CONSENT STATEMENT

2. **Mastercard Consent Statement**

   "I hereby consent to the processing by Mastercard Europe SA of my behavior-based data (such as keystroke timing, scroll position, and mouse-location) to uniquely identify me for purposes of ensuring my account security in accordance with the NuDetect Privacy Notice at https://www.mastercard.com/global/en/nudata-privacy-notice.html. You can withdraw your consent at any time by visiting the consent management platform of [Customer]