3DS Product Terms and Conditions: Mastercard

These 3DS Product Terms and Conditions shall apply to the extent a Counterparty is consuming or reselling 3DS Services from FreedomPay. For purposes of these terms and conditions, "Counterparty" shall mean a Client, Reseller, or Customer of a Reseller, as such terms are defined in an applicable agreement.

A. Fees: Fees for 3DS are set forth on an applicable Order or Agreement. Fees are charged for 3DS per request ("3DS Request Fee)." The 3DS Request Fee is charged for each request to FreedomPay's 3DS merchant plug in (a "3DS Request"). 3DS Requests may come directly from the Counterparty, from an ISV, be part of a defined flow, or be part of a hosted payment link transaction flow. For the avoidance of doubt, 3DS Requests are distinct from Transactions and the 3DS Request Fee is billed separately from transaction fees.

B. Counterparty Obligations:

1. Consumer Consents: Counterparty acknowledges and agrees that it shall be solely responsible for obtaining any and all consumer consents needed in connection with the 3DS services as required by applicable law, including but not limited to local law in any applicable jurisdiction.

2. Intellectual Property: 3DS service is provided and made available for Counterparty's non-transferable, non-exclusive use, without right to sub-license. Counterparty must not remove any copyright or other proprietary notices on or in the 3DS services. No right, title, or interest in the 3DS services, or any Intellectual Property Rights in the 3DS services, is transferred to Counterparty.

3. Privacy and Data Protection: In addition to any privacy or data protection provisions in the Agreement, the terms available herein shall apply to the 3DS services if the third party 3DS provider is Mastercard.

C. Indemnification: Counterparty will defend, indemnify and hold harmless the FreedomPay Indemnitees from and against any Losses arising from or in connection to any Claim arising out of FreedomPay's provision of 3DS Services, or Counterparty's receipt, use, misuse, or failure to use 3DS services, including but not limited to (i) any Claims arising out of the unauthorized transfer of the personal information of a claimant or other individual; (ii) access to the personal information of a claimant associated with Counterparty's use of 3DS Services, whether such unauthorized access occurs to FreedomPay's systems, or Counterparty's systems , (iii) any Claims arising out of breach of Counterparty's systems, including all costs of notification and remediation; (iv) any claims that any charges to a consumer's payment card were not authorized; (v) use, alteration, or modification by Counterparty of the 3DS Services in a manner that violates this Addendum or the instructions given to by FreedomPay or Mastercard, (vi) the combination, operation or use of the 3DS Services with equipment, devices, software or data not supplied by FreedomPay or Mastercard, if a claim would not have occurred but for such combination, operation or use; or (vii) Counterparty's failure to implement any modifications, upgrades, replacements, or enhancements to the 3DS Services, if a claim would not have occurred if such modifications, upgrades, replacements, or enhancements had been implemented.

D. WARRANTY: THE 3DS SERVICES IS PROVIDED AND MADE AVAILABLE ON AN "AS IS" AND "AS AVAILABLE" BASIS WITH ALL FAULTS KNOWN AND UNKNOWN. TO THE FULLEST EXTENT PERMITTED BY LAW, FREEDOMPAY MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE 3DS SERVICES, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

E. ACKNOWLEDGEMENT OF RESPONSIBILITY FOR POSSIBLE CARD BRAND DATA INTEGRITY FEES. Counterparty hereby acknowledges that it understands the card brands and issuers define data points required for 3DS authentication and FreedomPay is not accountable for authentication failures due to missing data points. In the event Counterparty implementations are missing required data points, "data integrity fees" may be imposed by the applicable card brands directly or passed down to the Counterparty from FreedomPay or the acquirer. Counterparty further acknowledges that it has been informed and fully understands that:

1. FreedomPay is not liable for any fees or service interruptions that may be levied by the card brands or acquirers as a result of not meeting minimum data requirements to perform 3DS.

2. By failing to collect and pass through the minimum required data points, Counterparty is fully responsible for payment of any imposed "data integrity fees" from the applicable card brands that may be passed down through FreedomPay or the Counterparty's acquiring bank.

3. Review or approval by FreedomPay of Counterparty's systems or processes does not constitute a representation or warranty by FreedomPay of Counterparty system effectiveness or suitability and shall not be deemed to transfer risk or liability to FreedomPay.

F. LIMITATION OF LIABILITY. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THE AGREEMENT, FREEDOMPAY SHALL HAVE NO LIABILITY UNDER THIS ADDENDUM OR IN ANY WAY RELATED TO 3DS SERVICES FOR ANY DIRECT,

INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR ANY LOST DATA, LOST BUSINESS, LOST REVENUE OR OPPORTUNITY COST OR DAMAGE TO REPUTATION OR GOODWILL, HOWSOEVER ARISING (WHETHER FORESEEABLE OR NOT, OR WITHIN THE CONTEMPLATION OF EITHER PARTY) WHETHER ARISING IN CONTRACT OR TORT (INCLUDING NEGLIGENCE AND BREACH OF STATUTORY OR OTHER DUTY) OR OTHER FORM OF EQUITABLE OR LEGAL THEORY. COUNTERPARTY ACKNOWLEDGES THAT FREEDOMPAY SHALL NOT BEAR ANY LIABILITY OR RESPONSIBILITY FOR FAULTS, ERRORS OR ERRONEOUS RECOMMENDATIONS PROVIDED ON THE BASIS OF UNTIMELY, INCOMPLETE, INACCURATE, FALSE OR MISLEADING INFORMATION PROVIDED BY COUNTERPARTIES.

3DS SERVICES PRIVACY AND DATA PROTECTION

The terms contained in Schedule 4, including Annex 1 and Annex 2, attached to this Exhibit B, 3DS Services Privacy and Data Protection, are required by Mastercard and shall be incorporated into the3DS Product Terms and Conditions in their entirety. The following definitions apply:

"3DS Smart Interface" has the same meaning as "3DS Services."
"Customer" means FreedomPay.
"Customer Client(s)" means "Counterparty".
"Mastercard" means FreedomPay's third party supplier of 3DS Services.

Any capitalized term used and not defined in this Addendum will have the meaning ascribed to such term in (a) the Value-Added Services Rules set forth under chapter 18 of the *Mastercard Rules* manual (as be amended from time to time, the "Value-Added Services Rules"); (b) the EMV® 3-D Secure Protocol and Core Functions Specification and applicable clarifications, bulletins, and Errata (the "Protocol and Core Functions Specifications"); and (c) all other applicable technical specifications, implementation user documentation, product guides associated with the 3DS Smart Interface, as may be amended from time to time ((b) and (c) together, the "Documentation").

SCHEDULE 4

Privacy & Data Protection
This Schedule 4 applies to the Processing of Personal Data of Data Subjects subject to Applicable Data Protection Law in the context of the 3DS Smart Interface and supplements the privacy and data protection terms set forth in Section 18.6 of the Value-Added Services Rules and the Enrollment Form. In the event of a conflict, the provisions in this Schedule 4 will prevail to the extent of the conflict. The terms used in this Schedule 4 have the meaning sets forth in the definitions section of this Schedule. Capitalized terms not otherwise defined herein have the meaning given to them in the Value-Added Services Rules or this Enrollment Form.

1. Definitions. The following terms have the meanings set out below for this Schedule:
1.1. "Controller" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.
1.2. "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and their national implementing legislations; the Swiss Federal Data Protection Act (as amended and replaced from time to time); the Monaco Data Protection Act (as amended and replaced from time to time); the UK Data Protection Act (as amended and replaced from time to time); and the Data Protection Acts of the European Economic Area ("EEA") countries (as amended and replaced from time to time).
1.3. "Europe" means the EEA, Switzerland, Monaco and the United Kingdom.
1.4. "Information Security Incident" means any actual or suspected unauthorized Processing, loss, use, disclosure, or acquisition of or access to any Personal Data Processed in connection with Customer's use of the 3DS Smart Interface.
1.5. "Mastercard Binding Corporate Rules" (or '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/global/documents/mastercard-bcrs.pdf.
1.6. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
1.7. "Processor" means the entity which processes Personal Data on behalf of a Controller.
1.8. "Sub-Processor" means the entity engaged by Mastercard or any further sub-contractor to process Personal Data on behalf of and in accordance with the instructions of Customer.

2. Use of Personal Data by Mastercard. Mastercard will be provided data which may include Personal Data to make the 3DS Smart Interface available to Customer. Customer acknowledges and agrees that Mastercard may Process Personal Data for the purpose of operating and providing the 3DS Smart Interface, including for product development, support and maintenance, and for any purpose listed in Section 18.6.10 of the Value-Added Services Rules, including internal research, fraud, security and risk management in accordance with Applicable Data Protection Law. Notwithstanding anything to the contrary set forth in this Schedule, the Enrollment Form or in Section 18.6 of the Value-Added Services Rules, Mastercard will not Process any Personal Data provided by Customer to Mastercard pursuant to the terms of this Enrollment Form for the purpose outlined at paragraph 7 of Section 18.6.10 of the Value-Added Services Rules.

3. Legal Ground and Notice. Customer must rely on a valid legal ground, and must ensure that Data Subjects are properly informed in accordance with Applicable Data Protection Law relating to the collection, use, disclosure, transfer or otherwise Processing of Personal Data by Customer and Mastercard in the context of the 3DS Smart Interface. In particular, Customer confirms and warrants that it will contractually require Customer Clients to obtain consent for the collection, use, disclosure, transfers and any other Processing of Personal Data by Customer and Mastercard in the context of the 3DS Smart Interface, to the extent and in the manner required by Applicable Data Protection Law. If Customer uses transaction data from another processing entity or a Mastercard competitor in connection with the 3DS Smart Interface, Customer will contractually require Customer Clients to obtain all applicable consents required to provide such transaction data to Mastercard. Upon request from Mastercard, Customer must demonstrate that it relies on a valid legal ground for the Processing, including consent, where applicable.

4. Data Subject Requests. Customer represents and warrants that it will contractually require Customer Clients to comply with Applicable Data Protection Laws in handling requests from Data Subjects. Customer Clients will be solely responsible for handling requests from Data Subjects to withdraw their consent, access, rectify, restrict or erase their Personal Data, exercise their right to data portability with regard to any Personal Data, object to the Processing of any Personal Data, or exercise their rights related to automated decision-making and profiling in connection with the 3DS Smart Interface. Customer will contractually require Customer Clients to handle such requests on Customer's and Mastercard's behalf. Mastercard will notify Customer of any such requests that Mastercard receives.

5. Information Security Incident. To the extent required by Applicable Data Protection Law, each Party will inform the other Party in writing of any Information Security Incident involving Personal Data Processed in connection with the 3DS Smart Interface in a commercially reasonable time frame, and in any event, no later than the time period required under Applicable Data Protection Law. Such Information Security Incident notice must describe, in reasonable detail, the nature of the Information Security Incident, the data elements involved, the identities of the affected individuals (if known), and the corrective action taken or to be taken to remedy the Information Security Incident. Customer will be solely responsible for any filings, communications, notices, press releases, or reports related to any Information Security Incident involving Personal Data processed in the context of the delivery of the 3DS Smart Interface pursuant to this Enrollment Form. Mastercard shall reasonably cooperate with Customer to support Customer's filings, communications, notices, press releases, or reports related to any Information Security Incident involving Personal Data Processed by Mastercard in the context of Mastercard's delivery of the 3DS Smart Interface to the Customer, where such Information Security Incident occurs within Mastercard's systems. Customer must obtain Mastercard's approval prior to the publication or communication of any filings, communications, notices, press releases or reports related to any Information Security Incident that expressly mentions Mastercard or its affiliates.

6. Governmental Requests for Personal Data. Except to the extent prohibited by applicable laws, each Party will promptly inform the other Party in writing if any competent authority, regulator or public authority of any jurisdiction requests disclosure of, or information about, Personal Data that has been Processed in connection with the 3DS Smart Interface. Each Party will, without limiting its rights under applicable laws, cooperate with the other Party as reasonably necessary to comply with any direction or ruling made by such authorities.

7. EU Data Protection Law. This Section 7 of Schedule 4 to the Enrollment Form regulates the Processing of Personal Data subject to EU Data Protection Law by the Parties in the context of the 3DS Smart Interface. This Section 7 of Schedule 4 supplements the privacy and data protection terms contained in this Enrollment Form, the Value-Added Services Rules or otherwise agreed between the Parties, to the extent they pertain to the Processing of Personal Data subject to EU Data Protection Law. In case of a conflict, the provisions of this Section 7 will prevail to the extent of the conflict.

7.1. **Roles of the Parties.** For the purpose of this Section 7 of Schedule 4, the Parties acknowledge and confirm that:
7.1.1. Customer Clients are the Controller, Customer is the Processor and Mastercard acts as Customer's Sub-Processor for the Processing of Personal Data for the Purposes (as defined in Annex 1) in the context of the 3DS Smart Interface.
7.1.2. Through its Customer Clients, Customer authorizes Mastercard to Process, as a Controller Personal Data for the purposes listed in Section 18.6.10 of the Value-Added Services Rules, including for internal research, fraud, security and risk management, but not for the purpose of administering sweepstakes, contests, or other marketing promotions. Mastercard represents and warrants that it will process Personal Data for these purposes in compliance with EU Data Protection Law, the Mastercard BCRs and the Value-Added Services Rules.
7.2. **Obligations of Customer and Customer Clients.** Customer represents and warrants that, in relation to the Processing of Personal Data for the Purposes in the context of the 3DS Smart Interface, it acts as a Processor pursuant to the lawful instructions of Customer Clients, the Controllers, and that it and/or its Customer Clients will:
7.2.1. Comply with EU Data Protection Law in respect of Processing of Personal Data, and only give lawful instructions to Mastercard.
7.2.2. Rely on a valid legal ground under EU Data Protection Law for each Purpose, including obtaining Data Subjects' appropriate consent if required or appropriate under EU Data Protection Law.
7.2.3. Provide appropriate notice to the Data Subjects regarding (1) the Processing of Personal Data for the Purposes, in a timely manner and at the minimum with the elements required under EU Data Protection Law; and (2) as applicable, the existence of Processors located outside of Europe and of the Mastercard BCRs, including the Data Subjects' right to enforce the Mastercard BCRs as third party beneficiaries (by linking to the Mastercard BCRs).
7.2.4. Take reasonable steps to ensure that Personal Data is accurate, complete and current; adequate, relevant and limited to what is necessary in relation to the Purposes for which they are Processed; and kept in a form which permits identification of Data Subjects for no longer than is necessary for the Purposes for which the Personal Data are Processed unless a longer retention is required or allowed under applicable law.
7.2.5. Implement appropriate technical and organizational measures to ensure, and to be able to demonstrate, that the Processing of Personal Data is performed in accordance with EU Data Protection Law, including, as appropriate, appointing a data protection officer, maintaining records of processing, complying with the principles of data protection by design and by default and, where required, performing data protection impact assessments and conducting prior consultations with supervisory authorities.
7.2.6. Respond to Data Subject requests to exercise their rights of or related to (a) access, (b) rectification, (c) erasure, (d) data portability, (e) restriction of Processing, (f) objection to the Processing, and (g) automated decision-making and profiling, in accordance with EU Data Protection Law.
7.2.7. Cooperate with Mastercard to fulfil its and/or their respective data protection compliance obligations in accordance with EU Data Protection Law.

7.2.8. Comply with any applicable requirements under EU Data Protection Law if it and/or they engage(s) in automated decision-making or profiling in the context of the 3DS Smart Interface.
4
7.3. **Obligations of Mastercard.** Mastercard will comply with the Mastercard BCRs and EU Data Protection Law when Processing Personal Data for the Purposes in connection with the 3DS Smart Interface, and it will:
7.3.1. Only Process Personal Data in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in Annex 1, Clause 7.1, the Value-Added Services Rules, or as otherwise agreed by both Parties in writing. Notwithstanding anything to the contrary set forth in this Schedule, the Enrollment Form or in Section 18.6 of the Value-Added Services Rules, Mastercard will not Process Personal Data provided by Customer to Mastercard pursuant to the terms of this Enrollment Form for the purpose outlined at paragraph 7 of Section 18.6.10 of the Value-Added Services Rules.
7.3.2. Promptly inform Customer if, in its opinion, the Customer's instructions infringe EU Data Protection Law, or if Mastercard is unable to comply with the Customers' instructions.
7.3.3. Cooperate with Customer in its role as Processor and Customer Clients in their roles as Controllers, to fulfil its own data protection compliance obligations under EU Data Protection Law, including by providing all information available to Mastercard as necessary to demonstrate compliance with the Customer's own obligations and where applicable to help Customer conducting data protection impact assessments or prior consultation with supervisory authorities.
7.3.4. Keep internal records of Processing of Personal Data carried out as a Sub-Processor on behalf of Customer.
7.3.5. Assist Customer in fulfilling Customer Clients' obligation to respond to Data Subjects' requests to exercise their rights as provided under EU Data Protection Law and specified under Clause 7.2.6, and notify Customer about such requests if Mastercard receives them directly from the Data Subject.
7.3.6. Notify Customer when local laws prevent Mastercard (1) from fulfilling its obligations under this Enrollment Form or the Mastercard BCRs and have a substantial adverse effect on the guarantees provided by this Enrollment Form or the Mastercard BCRs, and (2) from complying with the instructions received from the Customer via the Enrollment Form, except if such disclosure is prohibited by applicable law, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.
7.3.7. When the Enrollment Form expires or upon termination of the Enrollment Form or upon a request to delete or return Personal Data by Customer, except for any Personal Data which Mastercard Processes as a Controller pursuant to section 7.1.2 of this Schedule 4, Mastercard will, at the choice of Customer, delete, anonymize, or return such Personal Data to Customer, and delete or anonymize existing copies unless applicable law prevents it from returning or destroying all or part of the Personal Data or requires storage of the Personal Data (in which case Mastercard will protect the confidentiality of the Personal Data and will not actively Process the Personal Data anymore).
7.4. **Data Transfers**. Customer authorizes Mastercard to transfer the Personal Data Processed in connection with the 3DS Smart Interface outside of Europe in accordance with the Mastercard BCRs or with any other lawful data transfer mechanism that provides an adequate level of protection under EU Data Protection Law. Mastercard represents and warrants that it will abide by the Mastercard BCRs when Processing Personal Data for the Purposes in the context of the 3DS Smart Interface.
7.5. **Sub-Processing.** Without prejudice to Section 18.6.6 of the Value-Added Services Rules, Mastercard represents and warrants that when sub-processing the Processing of Personal Data in the context of the 3DS Smart Interface, it:
7.5.1. Remains liable to the Customer for the performance of its Sub-Processors' obligations.
7.5.2. Commits to provide a list of Sub-Processors to Customer upon request.
7.5.3. Will inform Customer of any addition or replacement of a Sub-Processor in a timely fashion so as to give Customer an opportunity to object to the change or to terminate the Enrollment Form before the Personal Data is communicated to the new Sub-Processor, except where the 3DS Smart Interface cannot be provided without the involvement of a specific Subprocessor.
7.6. **Security of the Processing; Confidentiality; and Personal Data Breach.**
7.6.1. The Parties must implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which includes at the minimum the security measures listed in Annex 2 and as appropriate: (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. In assessing the appropriate level of security, the Parties must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing of Personal Data as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects and the risks that are presented by the Processing of Personal Data, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.
7.6.2. The Parties must take steps to ensure that any person acting under their authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation, and if applicable Process Personal Data in accordance with the Controller's instructions.
7.6.3. The Parties must notify a Personal Data Breach that relates to Personal Data Processed in the context of the 3DS Smart Interface to the other Party, without undue delay, and no later than 72 hours after having become aware of a Personal Data Breach. Mastercard will provide reasonable assistance to Customer in complying with its obligations to notify a Personal Data Breach. Where required under EU Data Protection Law, Customer will notify such Personal Data Breach, without undue delay and, where feasible, not later than 72 hours after having become aware of it, to the competent supervisory authority. When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects or upon the competent supervisory authority's request to do so, Customer must communicate the Personal Data Brach to the affected Data Subjects without undue delay, where required under EU Data Protection Law.

7.6.4. The Parties will use their best efforts to reach an agreement on whether and how to notify a Personal Data Breach, and must document all Personal Data Breaches, including the facts relating to the Personal Data Breach, its effects and the remedial action taken.
7.7. **Data Protection Audit.** Upon prior written request by Customer, Mastercard agrees to cooperate and within reasonable time provide Customer with: (a) a summary of the audit reports demonstrating Mastercard's compliance with EU Data Protection Law obligations under this Enrollment Form and Mastercard BCRs, after redacting any confidential and commercially sensitive information; and (b) confirmation that the audit has not revealed any material vulnerability in Mastercard's systems, or to the extent that any such vulnerability was detected, that Mastercard has fully remedied such vulnerability. If the above measures are not sufficient to confirm compliance with EU Data Protection Law and Mastercard BCRs or reveal some material issues, subject to the strictest confidentiality obligations, Mastercard allows Customer to request an audit of Mastercard's data protection compliance program by external independent auditors, which are jointly selected by the Parties. The external independent auditor cannot be a competitor of Mastercard, and the Parties will mutually agree upon the scope, timing, and duration of the audit. Mastercard will make available to Customer the result of the audit of its data protection compliance program.
7.8. **Liability towards Data Subjects.** The Parties agree that they will be held liable for violations of EU Data Protection Law towards Data Subjects as follows:
7.8.1. Customer will be liable for the damage caused by the Processing only where it has not complied with (a) obligations of EU Data Protection Law specifically directed to Sub-Processors, (b) the Enrollment Form or (c) where it has acted outside of or contrary to Customer Clients' lawful instructions.
7.8.2. When Mastercard acts as a sub-Processor, it will be liable for the damage caused by the Processing only where it has not complied with obligations of EU Data Protection Law specifically directed to sub-Processors or where it has acted outside of or contrary to Customer's lawful instructions. In that context, Mastercard will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.
7.8.3. Where the Parties are involved in the same Processing and where they are responsible for any damage caused by the Processing, both Customer and Mastercard may be held liable for the entire damage in order to ensure effective compensation of the Data Subject. If Mastercard paid full compensation for the damage suffered, it is entitled to claim back from Customer that part of the compensation corresponding to Customer's part of responsibility for the damage.
7.9. **Applicable Law and Jurisdiction**. The Processing of Personal Data under this Section 7 of Schedule 4 will be governed by Belgian law. Any disputes between the Parties relating to the Processing of Personal Data under this Enrollment Form will be subject to the exclusive jurisdiction of the courts in Brussels, Belgium.

Annex 1 to Schedule 4: Description of the processing activities
This Annex 1 describes the Processing of Personal Data in the context of the 3DS Smart Interface.
Subject-matter of the Processing
The Parties will Process Personal Data to provide and operate the 3DS Smart Interface.
Nature and Purpose of the Processing ("Purposes")
 Customer will provide cardholders' Personal Data to Mastercard to operate and benefit from the 3DS Smart Interface
 Mastercard will process Personal Data, on behalf of Customer, to provide the 3DS Smart Interface for channeling requests to cardholder authentication programs
Types of Personal Data
The Parties will Process the following types of Personal Data:
- Cardholder device data (i.e., data related to cardholder's device, such as device name, device fingerprint);
- Cardholder transaction data (such as PAN, merchant name, transaction amount, currency, transaction ID, authentication status and value, card expiry, address information, date);
- Cardholder location data (i.e., location information derived from cardholder's IP address, browser IP Address).
Categories of Data Subjects
The Parties will Process Personal Data relating to cardholders.
Duration of the Processing
Mastercard will Process Personal Data as a Sub-Processor only for as long as necessary to provide the 3DS Smart Interface and to comply with applicable laws, and as permitted by the Enrollment Form.

Annex 2 to Schedule 4: Security 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. Control of instructions

Technical and organizational measures to ensure that Personal Data are processed solely in accordance with the Instructions of the Controller include:

- Unambiguous wording of the contract;
- Formal commissioning (request form);
- Criteria for selecting the Processor.

7. 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.

8. 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