CYBERSOURCE RESELLER DATA PROCESSING AGREEMENT

Updated: August 28, 2024

This Data Processing Agreement ("DPA") is an agreement between you and the entity you represent ("Reseller" or "you"), on the one hand, and Cybersource Corporation and/or any other applicable affiliated Cybersource contracting entity(ies) ("Cybersource"), on the other hand. It forms part of any written or electronic agreement between you and Cybersource (each, an "Agreement") under which Cybersource Processes Personal Information on behalf of Reseller's customers ("Customer Personal Information"), except with respect to any Agreement under which you and Cybersource have entered data processing terms that address the subject matter hereof.

1 **Responsibility of Reseller's customers**. For the avoidance of doubt, Reseller shall ensure that its customers comply with any and all obligations, responsibilities and requirements in this DPA specified as belonging to Reseller's customers.

2 **Processing of Customer Personal Information**. The parties acknowledge and agree that under Applicable Data Protection Law, that Cybersource may act in various data processing roles. To enable each party to comply with its obligations under Applicable Data Protection Law, each party further agrees to comply with any required provisions of Schedule A: California Consumer Privacy Act and/or Schedule B: General Data Protection Regulation, each, to the extent applicable.

2.1 **GDPR**. Where the General Data Protection Regulation (Regulation (EU) 2016/679 (the "GDPR") applies to Reseller's customers use of Cybersource Services or if Applicable Data Protection Law imposes a comparable requirement, the parties acknowledge and agree that with respect to the Customer Personal Information that Cybersource Processes, that:

2.1.1 Reseller's customers are controllers (or equivalent term pursuant to Applicable Data Protection Laws), Reseller is a data processor, and Cybersource is a "sub-processor" engaged by Reseller to carry out specific processing activities for Reseller's customers or such equivalent term under Applicable Data Protection Law, if any (referred to as "Sub-Processor" for purposes of this DPA) for the "Sub-Processor Services". Such Sub-Processor Services include, by way of example and for illustrative purposes the Processing detailed on Details of Processing (Exhibit 2, section 1); and

2.1.2 both Reseller's customers and Cybersource are "joint controllers", or such equivalent term under Applicable Data Protection Law, if any, for the "Controller Services". Such Controller Services include the Processing detailed on Details of Processing (Exhibit 2, section 2).

2.2 **Other Applicable Data Protection Law**. Where section 1.1 does not apply, the parties acknowledge and agree that Cybersource is a Sub-Processor for all Cybersource Services engaged by Reseller to carry out specific processing activities for Reseller's customers.

3 **Compliance with law**. Cybersource, in its provision of Cybersource Services to Reseller, and Reseller and its customers in their use of the Cybersource Services, shall Process Customer Personal Information in accordance with Applicable Data Protection Law.

4 **Privacy Notice**. With respect to the Cybersource Services, Reseller shall ensure that its customer shall provide their End-User(s) with all privacy notices, information and any necessary choices and shall obtain any necessary consents to enable the parties to comply with Applicable Data Protection Law with respect to the Cybersource Services.

5 **Sub-Processor obligations**

5.1 **Authorization to Process**. Where Cybersource is acting as a Sub-Processor, it will Process Personal Information on behalf of Reseller's customers to provide such Cybersource Services, and Reseller, on behalf of its customers, authorizes Sub-Processor to Process Customer Personal Information solely in connection with the following activities:

5.1.1 In accordance with the applicable Agreement(s), including, without limitation, any exhibits, schedules, and applicable price schedule(s), to provide the Cybersource Services, and any Processing required under applicable law or regulations;

5.1.2 Based on the instructions of Reseller and in its use of the Cybersource Services, Sub-Processor transfers Personal Information to acquiring banks, issuing banks, payment processors providing services on behalf of acquiring banks, credit/debit card companies, or service providers performing payer authentication services used by Customer, such as Verified by Visa and MasterCard Identity Check (ID Check); and

5.1.3 As reasonably necessary to enable Sub-Processor to comply with any other directions or instructions provided by Reseller.

5.2 **Data Subject Rights**. Sub-Processor will, to the extent legally permitted, provide reasonable assistance to Reseller to respond to requests from its customers' End-Users to exercise their rights under Applicable Data Protection Law (e.g., rights to access or delete Personal Information) in a manner that is consistent with the nature and functionality of the Cybersource Services. Reseller shall submit such requests for assistance to the Business Center. Where Sub-Processor receives any such request, it shall advise the End-User that the applicable Reseller's customer is responsible for handling such requests by an End-User in accordance with Applicable Data Protection Law.

5.3 **Engaging with Sub-Sub-Processors**. Sub-Processor shall ensure that when engaging with another data processor including any Affiliates (a "Sub-Sub-Processor") for the purposes of carrying out specific Processing activities on behalf of Reseller's customers, there is a written contract in place between Sub-Processor and the relevant Sub-Sub-Processor. Such written contracts, to the extent applicable to the nature of the Cybersource Services provided by the relevant Sub-Sub-Processor will provide at least the same level of protection for Customer Personal Information as set out in this DPA.

5.4 **Staff**. Sub-Processor shall ensure that persons authorized to Process Customer Personal Information have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.5 **Security of Processing**. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Sub-Processor shall implement technical and organizational measures to ensure a level of security appropriate to that risk. In assessing the appropriate level of security, Sub-Processor shall, in particular, take into account the sensitivity of the Personal Information and the risks that are presented by the Processing, in particular from unauthorized or unlawful Processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Information transmitted, stored or otherwise Processed. Sub-Processor shall provide reasonable assistance to Reseller in ensuring it meets its own compliance obligations with respect to these same security measures. Cybersource, Reseller and its customers shall also comply with PCI-DSS as set out in the Agreement.

6 **Security Breach**. The applicable party, Cybersource, Reseller or its customer, shall promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of Customer Personal Information. In the event of an actual Security Breach (defined below) affecting Customer Personal Information Cybersource, Reseller and Reseller's customer shall cooperate and assist one another in

good faith as needed to comply with Applicable Data Protection Laws including as applicable, notifying a Supervisory Authority of the Security Breach and communicating the Security Breach to the relevant Data Subjects.

6.1.1 In the event of an actual Security Breach affecting Customer Personal Information contained in:

6.1.1.1 Cybersource's systems, Cybersource shall notify Reseller of the Security Breach without undue delay and continue to keep Reseller informed on a regular basis of the progress of investigation and remediation efforts. Notice in accordance with this section shall be made by sending an email and/or text message to the email address and/or mobile phone number registered by Reseller in the Business Center. For Controller Services, Reseller and its customer impacted by the Security Breach shall cooperate and assist Cybersource as necessary for Cybersource to communicate the Security Breach to the relevant Supervisory Authorities.

6.1.1.2 Reseller or Reseller's customer's systems, the Reseller may elect to notify Cybersource of the Security Breach, and such notice should be made by sending an email to vsirt@visa.com. Cybersource shall cooperate and assist the Reseller as necessary for Reseller to communicate the Security Breach to the relevant Supervisory Authorities.

6.1.2 Reseller or its applicable customer shall be responsible for communicating any Security Breach to End Users if notice is required under Applicable Data Protection Laws.

6.1.3 Except as required by applicable law or regulation the parties, including Reseller's customers, will not make (or permit any third party to make) any statement concerning the Security Breach that directly or indirectly references the other party, unless the other party provides its explicit written authorization.

6.1.4 To the extent that a Security Breach was caused by Reseller, Reseller's customers or End Users, Reseller shall be responsible for the costs arising from the Sub-Processor's provision of assistance under this section 6.

7 **Deletion and Retention**. Sub-Processor shall, at the choice of Reseller, delete or return all Customer Personal Information upon termination of the Agreement and delete existing copies unless storage is required by applicable law.

8 **Miscellaneous**. The terms of this DPA shall apply only to the extent required by Applicable Data Protection Law. To the extent not inconsistent herewith, the applicable provisions of the Agreement(s) (including without limitation, indemnifications, limitations of liability, enforcement, and interpretation) shall apply to this DPA. In the event of any conflict between this DPA and the terms of an applicable Agreement, the terms of this DPA shall control solely with respect to data processing terms where required by Applicable Data Protection Law, and, in all other respects, the terms of the applicable Agreement shall control. Notwithstanding any term or condition of the DPA, the DPA does not apply to any data or information that does not relate to one or more identifiable individuals under Applicable Data Protection Law, such as data that has been aggregated, de-identified or anonymized, or to the extent that Cybersource and you have entered separate data processing terms that address the subject matter hereof.

9 **Definitions**. Unless otherwise defined in the Agreement (including this DPA), all terms in this DPA shall have the definitions given to them in Applicable Data Protection Law.

"Applicable Data Protection Law"	means any law or regulation pertaining to data protection, privacy, and/or the Processing of Personal Information, to the extent applicable in respect of a party's obligations under the Agreement and this DPA. For illustrative

purposes only, Applicable Data Protection Laws include, without limitation, and to the extent applicable, the General Data Protection Regulation (Regulation (EU) 2016/679 (the “GDPR”), the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (”CCPA”), Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (“PIPEDA”), UK Data Protection Laws, Swiss DP Laws and any associated regulations or any other legislation or regulations that transpose, supersede or are deemed substantially similar to the above.

“EEA Standard Contractual Clauses” means the Standard Contractual Clauses set out in the European Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as amended or replaced from time to time by a competent authority under the Applicable Data Protection Law, including the Swiss amendments to the EU Standard Contractual Clauses required by the Swiss Federal Data Protection Information Commissioner (the “Swiss Addendum”) to the extent applicable.

“End-User(s)” means any person that purchases goods or services of Reseller’s customers, whose information is submitted by Reseller or its customers to Cybersource during the course of using the Cybersource Services hereunder.

“Personal Information” means all data or information, in any form or format, that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer (“Data Subject”) or household or that is regulated as “personal data,” “personal information,” or otherwise under Applicable Data Protection Law. For the avoidance of doubt, this includes any information relating to an End-User as defined in the Agreement. For the avoidance of doubt, this includes data relating to legal entities, if and as long as they are protected under the Swiss DP Laws as well as any information relating to an End-User as defined in the Agreement.

“Process” or “Processed” or “Processing” means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, such as access, collection, recording, organization, storage, adaptation or alteration, retrieval, disclosure or otherwise making available, duplication, transmission, combination, blocking, redaction, erasure or destruction.

“Security Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information. A Security Breach includes a “personal data breach” (as defined in the GDPR), a “breach of security of a system” (as defined in any US law), a “breach of security safeguards” (as defined in PIPEDA) or similar term (as defined in any other applicable privacy laws) as well as any other event that compromises the security, confidentiality or integrity of Personal Information.

“Swiss DP Laws” means the Federal Act on Data Protection of June 19, 1992 (as updated, amended and replaced from time to time), including all implementing ordinances. In this DPA, in circumstances where and solely to the extent that the Swiss DP Laws apply, references to the GDPR and its provisions shall be construed as references to the Swiss DP Laws and their corresponding provisions.

“Transfer”

means to transmit or otherwise make Customer Personal Information available across national borders in circumstances which are restricted by Applicable Data Protection law.

“UK Data Protection Laws”

means the GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("UK GDPR"), together with the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and other data protection or privacy legislation in force from time to time in the United Kingdom. In this DPA, in circumstances where and solely to the extent that the UK GDPR applies, references to the GDPR and its provisions shall be construed as references to the UK GDPR and its corresponding provisions.

“UK IDTA”

means the International Data Transfer Addendum to the EEA Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

SCHEDULE A
CALIFORNIA CONSUMER PRIVACY ACT

This CCPA Schedule applies in addition to any terms set forth in the body of the DPA (and is incorporated therein) when the CCPA applies to your use of Transaction Services or if Applicable Data Protection Law imposes a comparable requirement outlined under Schedule A. Capitalized terms not defined herein have the meaning assigned to them under the DPA. To the extent there are any conflicts between this CCPA Schedule and the DPA, this CCPA Schedule shall prevail.

1 Cybersource shall not:

(i) sell, or share for cross-contextual behavioral advertising, Customer Personal Information;

(ii) combine Customer Personal Information with personal information obtained from different sources;

(iii) retain, use, or disclose Customer Personal Information other than for the specific purposes set forth in the body of the DPA; or

(iv) where applicable, use any Sensitive Personal Information received from Customer other than to assist the Customer in purposes authorized by Customer instruction;

in each case, except as required to perform a business purpose defined in this Agreement or as permitted by Applicable Data Protection Law.

2 To the extent required by Applicable Data Protection Law, this CCPA Schedule constitutes its certification to the Processing restrictions herein to enable Customer to:

(i) ensure Customer Personal Information is used consistent with Applicable Data Protection Law;

(ii) stop and remediate unauthorized use of Customer Personal Information, and

(iii) to conduct reasonable assessments of Cybersource's policies and technical and organizational measures. Cybersource grants Customer the rights set forth in Schedule B, Section 4 for the purposes of Section 2(iii) of this Schedule.

3. Sub-processor obligations pursuant to the CCPA shall be governed by Section 4.3 of the DPA.

3 Each of Cybersource and Customer shall comply with applicable provisions of the CCPA, including, in the case of the Customer, to provide required notices and disclosures with respect to the obligations of the business under the CCPA; and in the case of Cybersource, to notify Customer promptly (and, in any event, within any period required by law) upon making a determination that it can no longer meet its obligations with respect to Customer Personal Information under the CCPA.

SCHEDULE B

GENERAL DATA PROTECTION REGULATION

This GDPR Schedule applies in addition to any terms set forth in the body of the DPA (and is incorporated therein) when the GDPR applies to Reseller's use of Cybersource Services or if Applicable Data Protection Law imposes a comparable requirement outlined under Schedule B. Capitalized terms not defined herein have the meaning assigned to them under the DPA. To the extent there are any conflicts between this GDPR Schedule and the DPA, this GDPR Schedule shall prevail.

1 **Processing of Customer Personal Information**. Sub-Processor shall Process Customer Personal Information only on documented reasonable instructions from Reseller (including instructions with respect to transfers of Customer Personal Information to a third country, if applicable) unless Sub-Processor is required to otherwise Process Customer Personal Information by Applicable Data Protection Law. In such circumstances, Sub-Processor shall inform Reseller of that legal requirement before Processing, unless prohibited from doing so by applicable law, on important grounds of public interest. Sub-Processor shall immediately inform Reseller if, in Sub-Processor's opinion, Reseller's instructions would be in breach of Applicable Data Protection Law. Reseller agrees that Sub-Processor shall be under no obligation to take actions designed to form any such opinion.

2 Use of Sub-Sub-Processor

2.1 Reseller provides authorization for Sub-Processor to engage with the Sub-Sub-Processors listed in the Business Center. Sub-Processor reserves the right to maintain its Sub-Sub-Processor list through means such as publication of its Sub-Sub-Processor list online.

2.2 Sub-Processor shall inform Reseller of any intended changes concerning the addition or replacement of other Sub-Sub-Processors to give Reseller's clients a reasonable opportunity to object to such changes. If a client of Reseller objects to Processor's change or addition of a Sub-Sub-Processor ("Objecting Client"), Reseller shall promptly notify Sub-Processor of objections in writing within 10 business days after receipt of Sub-Processor's notice of such change or addition.

2.3 Sub-Processor may, at its option, undertake reasonable efforts to make available to Reseller's Objecting Client a change in the Cybersource Services or recommend a commercially reasonable change to the Objecting Client's configuration or use of the Cybersource Services to avoid Processing of Customer Personal Information by the objected-to new Sub-Sub-Processor. If Sub-Processor is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Reseller may, at its client's request, terminate the Agreement for the Objecting Client with respect to only those aspects of the Cybersource Services which cannot be provided by Sub-Processor without the use of the objected-to new Sub-Sub-Processor by providing written notice to Sub-Processor.

2.4 Sub-Processor agrees not to impose a penalty for any termination under section 2 of this GDPR Schedule on Reseller.

3 Data Protection Impact Assessments and Prior Consultation with Regulator. Sub-Processor shall provide reasonable assistance to Reseller with any legally required (i) data protection impact assessments; and (ii) prior consultations initiated by Reseller with its regulator in connection with such data protection impact assessments. Such assistance shall be strictly limited to the Processing of Customer Personal Information by Sub-Processor on behalf of Reseller's under the Agreement taking into account the nature of the Processing and information available to the Sub-Processor**.**

4 Demonstrating Compliance with this DPA

4.1 Sub-Processor shall make available to Reseller all information necessary to demonstrate compliance with its obligations under this DPA and allow for (and contribute to) audits, including inspections conducted by Reseller or another auditor under the instruction of the Reseller for the same purposes of demonstrating compliance with obligations set out in this DPA.

4.2 Reseller's right under section 4 of this GDPR Schedule is subject to the following:

4.2.1 If Sub-Processor can demonstrate compliance with its obligations set out in this DPA by adhering to an approved code of conduct, by obtaining an approved certification or by providing Reseller with an audit report issued by an independent third party auditor (provided that Reseller will comply with appropriate confidentiality obligations as set out in the Agreement and shall not use such audit report for any other purpose), Reseller agrees that it will not conduct an audit or inspection under this section 4;

4.2.2 In acknowledgement of the time, expense and disruption to business associated with performing audits and inspections involving interviews and onsite visits, Reseller agrees to only conduct such audits and inspections on condition that Reseller can demonstrate such audit or inspection is necessary beyond the information made available by Sub-Processor under section 4 above. Such audits and inspections, shall be at reasonable intervals (but not more than once per year) upon not less than 60 days' notice and at a date mutually agreed by the Parties, provided that the audit will (i) not disrupt Sub-Processor's business; (ii) be conducted during business hours and at the Reseller's expense; (iii) not interfere with the interests of Sub-Processor's other customers; and (iv) not exceed a period of two successive business days.

5 **Cross-Border Transfers for Sub-Processor Services**. Sub-Processor shall comply with Reseller's documented instructions concerning the Transfer of Customer Personal Information to a third country. Sub-Processor shall only Transfer any Customer Personal Information outside the Reseller's customer's applicable jurisdiction or the End-User's resident jurisdiction, including, without limitation, outside the European Economic Area ("EEA"), the UK or Switzerland, in compliance with the Applicable Data Protection Law. Reseller agrees and acknowledges that Sub-Processor Transfers and stores certain Customer Personal Information (including relating to individuals located in the EEA) in the United States.

5.1 **Transfers subject to the GDPR, UK GDPR or Swiss DP Laws:** Module 3 (Transfer processor to processor) of the EEA Standard Contractual Clauses shall apply with respect to any Transfer of Customer Personal Information from the EEA, UK or Switzerland to Cybersource and any of its affiliated entities in the United States or other third countries ("Cybersource Entities"). The parties acknowledge and agree that Module 3 (Transfer processor to processor) of the EEA Standard Contractual Clauses is hereby incorporated by reference and;

5.1.1 Reseller shall be deemed to be the "data exporter" and the Cybersource Entities shall be the "data importer";

5.1.2 Clause 7 – *Docking clause* shall apply;

5.1.3 Clause 9 – *Use of subprocessors* Option 2 shall apply and the "time period" shall be 10 business days;

5.1.4 Clause 11(a) – *Redress* the optional language shall not apply;

5.1.5 Clause 13(a) – *Supervision*

5.1.5.1 Where the data exporter is established in an EU Member State the following shall apply: *"The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C , shall act as competent supervisory authority."*

5.1.5.2 Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of the GDPR the following shall apply: *"The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority."*

5.1.5.3 Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of the GDPR in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of the GDPR, the following shall apply: *"The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose* *behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority."*

5.1.6 Clause 17 – *Governing law* Option 1 shall apply and the "Member State" shall be Ireland;

5.1.7 Clause 18 – *Choice of forum and jurisdiction* the Member State shall be Ireland; and

5.1.8 the information in Exhibit 1 (Table 1) of this GDPR Schedule is incorporated into Annexes 1, 2 and 3 of the EEA Standard Contractual Clauses.

5.1.9 **Transfers subject to the UK GDPR:** where the Transfer is subject to the UK GDPR, the EEA Standard Contractual Clauses and Clause 5.1 of this Schedule B shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA. For the purposes of Table 4 in Part 1 (Tables) of the UK IDTA, the parties select the "neither party" option. ~~, and~~ Otherwise, the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in Exhibit 1. If there is any conflict or inconsistency between a term in the body of this DPA, an Agreement and a term in Module 3 (Transfer processor to processor) of the EEA Standard Contractual Clauses , incorporated into this DPA, the term in Module 3 (Transfer processor to processor) of the EEA Standard Contractual Clauses () shall take precedence.

5.1.10 **Transfers subject to Swiss DP Laws**: Where the Transfer is subject to the Swiss DP Laws, the EEA Standard Contractual Clauses and Clause 5.1 of this Schedule B shall be read in accordance with section 13.4 of Schedule B to this DPA.

6 **Joint Controller Obligations**. The obligations in this DPA, including those set out below in this GDPR Schedule, shall constitute the written arrangement allocating responsibilities between joint controllers required under Article 26 of the GDPR with respect to the Controller Services.

7 **Reasonable Assistance**. With respect to the Controller Services, Cybersource and Reseller's customers shall assist one another as reasonably required, in meeting any regulatory obligations in relation to data security, notification of a Security Breach, and data protection impact assessments for the Controller Services.

8 **Notice**. For the avoidance of doubt, with respect to the Controller Services, Reseller's Customer shall provide its End-User(s) with all privacy notices, information and any necessary choices and shall obtain any necessary consents to enable the parties to comply with Applicable Data Protection Law with respect to the Cybersource Services.

9 **Data Subject Rights.** Reseller's customer shall be the designated point of contact for the Data Subject with respect to Data Subject Rights requests for Controller Services, and Cybersource shall reasonably cooperate with and assist Reseller's customers in the execution and fulfilment of their obligations under Applicable Data Protection Laws in relation to such requests.

10 **Supervisory Authority**. Cybersource and Reseller's customers shall without undue delay notify each other upon receipt of any correspondence from a Supervisory Authority in respect of the Controller Services where and to the extent permitted by applicable law.

11 **Security of Processing.** Cybersource and Reseller's customers shall each be responsible for ensuring adequate security in respect of processing of Personal Information for Controller Services that takes place within that party's own systems.

12 **Security Breach**. For the avoidance of doubt, in the event of a Security Breach related to Controller Services, the section 6 of the body of the Agreement shall govern.

13 **Cross border transfers for Controller Services**

13.1 Transfers subject to the GDPR, UK GDPR or Swiss DP Laws: Module 4 (transfer processor to controller) of the EEA Standard Contractual Clauses shall apply with respect to any Transfer of Customer Personal Information from the EEA, UK or Switzerland to Cybersource Corporation in the United States, solely when Cybersource Corporation is acting as a controller for the purposes of the Controller Services. The parties acknowledge and agree that Module 4 (transfer processor to controller) of the EEA Standard Contractual Clauses is hereby incorporated by reference and;

13.1.1 Reseller shall be deemed to be the "data exporter" and the Cybersource Entities shall be the "data importer";

13.1.2 Clause 7 – *Docking clause* shall apply;

13.1.3 Clause 11(a) – *Redress* the optional language shall not apply;

13.1.4 Clause 17 – *Governing law* the country shall be Ireland;

13.1.5 Clause 18 – *Choice of forum and jurisdiction* shall be the courts of Ireland;

13.1.6 the information in Exhibit 1 (Table 1) of this GDPR Schedule is incorporated into Annexes 1, 2 and 3 of the EEA Standard Contractual Clauses.

13.2 Transfers subject to the UK GDPR: where the Transfer is subject to the UK GDPR, the EEA Standard Contractual Clauses and Clause 13.1 of this Schedule B shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK IDTA. For the purposes of Table 4 in Part 1 (Tables) of the UK IDTA, the parties select the "neither party" option. Otherwise, the Parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in Exhibit 1.

13.3 if there is any conflict or inconsistency between a term in the body of this DPA, an Agreement and a term in Module 4 (transfer processor to controller) of the EEA Standard Contractual incorporated into this DPA, the term in the EEA Standard Contractual Clauses shall take precedence.

13.4 Transfers subject to the Swiss DP Laws: to the extent the Swiss DP Laws are applicable to a data export under the EEA Standard Contractual Clauses set forth in this DPA, the Parties agree on the following amendments to the EEA Standard Contractual Clauses and Clause 13.1 of this Schedule B:

13.4.1 The term "Member State" according to Clause 18 (c) of the EEA Standard Contractual Clauses shall not be interpreted in a such a way that data subjects in Switzerland are excluded from exercising their rights, if any, at their place of habitual residence;

13.4.2 The supervisory authority pursuant to Clause 13 of the EEA Standard Contractual Clauses is the Swiss Federal Data Protection and Information Commissioner;

13.4.3 The law applicable to the EEA Standard Contractual Clauses pursuant to Clause 17 of the EEA Standard Contractual Clauses shall be Swiss DP Laws;

13.4.4 The place of jurisdiction under Clause 18 (b) of the EEA Standard Contractual Clauses shall be the courts of the city of Zurich;

13.4.5 Where the EEA Standard Contractual Clauses include references to the GDPR, such references shall be understood as references to the Swiss DP Laws.

EXHIBIT 1
INFORMATION REQUIRED FOR THE EEA STANDARD CONTRACTUAL CLAUSES AND THE UK IDTA AND SWISS DP LAWS

Table 1: Information to be incorporated into the EEA Standard Contractual Clauses	
ANNEX I A. List of Parties	
Data EXPORTER identity and contact details	
Name	Reseller
Address	To be provided on request
Contact person's name, position and contact details:	To be provided on request
Activities relevant to the data transferred under these Clauses:	As set out in the table in Exhibit 2 under "Nature and Purpose of the Processing".
Role (controller/processor):	Processor
Data IMPORTER identity and contact details	
Name	Cybersource Entities
Address	900 Metro Center Boulevard Foster City, CA 94404 U.S.A.
Contact person's name, position and contact details:	privacy@visa.com
Activities relevant to the data transferred under these Clauses:	As set out in the table in Exhibit 2 under "Nature and Purpose of the Processing".
Role (controller/processor):	Module 1: Controller Module 2: Processor
ANNEX I B. Description of Transfer	
Categories of data subjects whose personal data is transferred	As set out in the table in Exhibit 2 under "Categories of Data Subjects".
Categories of personal data transferred	As set out in the table in Exhibit 2 under "Types of Personal Information".

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.	Not Applicable
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	Continuous
Nature of the processing	As set out in the table in Exhibit 2 under "Nature and Purpose of the Processing".
Purpose(s) of the data transfer and further processing	As set out in the table in Exhibit 2 under "Nature and Purpose of the Processing".
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Personal data will be retained in accordance with Cybersource's retention policies, for only as long as is required to meet Cybersource's legal, regulatory and operational requirements and as necessary to perform services.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing	As set out in the table in Exhibit 2 under "Nature and Purpose of the Processing".
Annex I C. Competent Supervisory Authority	
Competent supervisory authority/ies	To be provided by the data exporter on request.
ANNEX II Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data	
Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.	Cybersource Corporation is certified as compliant with all standards established by the Payment Card Industry Data Security Standards (together with any successor organization thereto, "PCI DSS") that are applicable to Cybersource Corporation and its affiliates (such standards, the "PCI Standards"). As evidence of compliance, Customer may access Cybersource Corporation's current Attestation of Compliance signed by a Payment Card Industry Qualified Security Assessor through Visa Online. Cybersource Corporation maintains and enforces commercially reasonable information security and

	physical security policies, procedures and standards, that are designed (i) to insure the security and confidentiality of Customer's records and information, (ii) to protect against any anticipated threats or hazards to the security or integrity of such records, and (iii) to protect against unauthorized access to or use of such records or information which could result in substantial harm (the "Visa Information Security Program"). At a minimum, the Visa Information Security Program is designed to meet the standards set forth in ISO 27002 published by the International Organization for Standardization, as well as any revisions, versions or other standards or objectives that supersede or replace the foregoing. Cybersource Corporation engages its independent certified public accountants to conduct a review of Cybersource Corporation's operations and procedures at Cybersource Corporation's cost. The accountants conduct the review in accordance with the American Institute of Certified Public Accounts Statement on Standards for Attestation Engagements No. 18 SOC I Type II ("SSAE 18") and record their findings and recommendations in a report to Cybersource Corporation. Upon request, and subject to standard confidentiality obligations, Cybersource Corporation will provide its most recent SSAE 18 and, in Cybersource Corporation's reasonable discretion, additional information reasonably requested to address questions or concerns regarding the SSAE 18's findings.
For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter	In respect of Cybersource Services: initiatives, products, processes and supporting technology are assessed from a data privacy perspective, allowing Cybersource to embed privacy controls to mitigate risks at early stages (privacy by design). Cybersource has a robust privacy risk assessment framework (including privacy impact assessments), embedding this process in our change vehicles across the business, to ensure that both new and changed personal data processing activities are reviewed. Where Customer requires specific assistance, Customer may submit such requests for assistance to the Business Center.

ANNEX III LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

As listed in the Business Center.

EXHIBIT 2
DETAILS OF PROCESSING CUSTOMER PERSONAL INFORMATION

1 Details of Processing in respect of the Sub-Processor Services

The table below includes certain details of the Processing of Customer Personal Information in respect of the Sub-Processor Services as required by Article 28(3) of the GDPR. Each of the service descriptions below apply to the extent that Customer uses such service under the Agreement.

Service	Nature and purpose of the processing	Types of personal information	Categories of data subjects to whom the personal information relates to
Payment gateway service	Gateway services for bank transfers, direct debits, credit/debit card authorisation, settlement, authentication and credit, including processing, provision of customer support.	Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address.	End-Users as defined under the Agreement (including Credit card holders, bank transfer users, direct debit users, all End-Users whose cardholder or bank account data is submitted to Sub-Processor for processing).
Tokenization	Tokenization is a Data Security technology which helps customers facilitate a safe transfer and storage of sensitive information. Cybersource Tokenization service replaces sensitive payment data with a unique identifier or token. This simplifies customer operations and removes sensitive data from their environment. The actual payment data is securely stored in Visa data centers within the customers token vault.	If the Customer enrolls for the Tokenization service, they can choose which Customer data to store. Cybersource can support data such as account numbers, name, billing address, shipping address, phone number, e-mail address, etc.	

Payer Authentication	Payer Authentication, also called 3D Secure, provides Customer with risk management and authentication services. Payer Authentication facilitates the exchange of data between Customer and a card issuer to authenticate a cardholder by routing data to Payer Authentication programs, such as Visa Secure, Mastercard Identity Check (ID Check), American Express SafeKey and JCB J/Secure. Payer Authentication helps to minimize costly fraudulent transactions by adding an extra layer of protection to the payment process, helping to increase authorization approval rates as well as reduce the risk of fraud.	If the Customer opts to use the Authentication service, the service may use Cardholder and banking information, including, without limitation, card numbers, bank account numbers, names, addresses, phone numbers, and e-mail addresses as a part of processing the authentication request with the issuer.	
Order Screening	Order Screening provides customers risk management and order review services. Customer Personal Information is used to evaluate the potential for fraud and mark those transactions with recommendations for the client.	Order Screening leverages the Customer's data available in the Decision Manager service. This data includes Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address, as well as cardholder's device that is used to complete Customer's transactions (such as device fingerprint if the customer elects to use ThreatMetrix).	
Performance Monitoring	Performance Monitoring provides a Customer with an expert risk analyst for consultative purposes in the fraud management space,	Performance Monitoring leverages the Customer's data available in the Decision Manager service.	

	specifically related to using Decision Manager.	This data includes Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address, as well as cardholder’s device that is used to complete Customer’s transactions (such as device fingerprint if the customer elects to use ThreatMetrix).	
Alternative payments	Alt Pay services for Online Banks Transfers, eWallets, Buy Now Pay Later and Cash based payments	Name, address, email address, Phone Number, IBAN (optional), BIC/SWIFT (optional)	
Recurring Billing	Recurring billing is a payment model that enables business owners to charge their customers at predefined frequencies (weekly, monthly, annually, or custom intervals), for the products or services they purchase. Recurring Billing stores customer data securely, with seamless integration into Account Updater ensuring customer data is up to date.	This data includes Cardholder and banking information, including, card numbers, bank account numbers, name, address, phone number, e-mail address. The data is stored in a TMS customer vault. Recurring Billing knows the customer only by their token ID and First and Last name	
Invoicing	Invoicing enables business owners to create and send invoices digitally via the online portal (Enterprise Business Center) or API. Business owners send their customers the link to a digital invoice, and they pay it online. Customer information is used by Visa to process payments per standard card network and other digital payment processing rules, prevent fraudulent payment activity and by the business owners to reconcile with other	Data collected includes business owners' customer information, including, card numbers, bank account numbers, name, address, phone number, e-mail address.	

	systems used for business operations.		

2 Details of Processing in respect of the Controller Services

The table below includes certain details of the Processing of Customer Personal Information in respect of the Controller Services. Each of the service descriptions below apply to the extent that Customer uses such service under the Agreement.

Service	Nature and purpose of the processing	Types of personal information	Categories of data subjects to whom the personal information relates to
Decision Manager	Decision Manager provides the Customer with risk management and fraud mitigation services. Customer Personal Information is used to support the creation and enhancement of security and fraud prevention tools and models for use by Customer and any other customer of Cybersource. These models ensure that scoring in Fraud Services is kept up-to-date.	Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address, as well as cardholder's device that is used to complete Customer's transactions (such as device fingerprint if the customer elects to use ThreatMetrix).	End-Users as defined under the Agreement (including Credit card holders, bank transfer users, direct debit users, all End-Users whose cardholder or bank account data is submitted to Cybersource for processing).
FME (Fraud Management Essentials)	Fraud Management Essentials provides the Customer with risk management and fraud mitigation services. Customer Personal Information is used to support the creation and enhancement of security and fraud prevention tools and models for use by Customer and any other customer of Cybersource. These models ensure that scoring in Fraud Services is kept up-to-date.	Cardholder and banking information, including, without limitation, card numbers, bank account numbers, name, address, phone number, e-mail address, as well as cardholder's device that is used to complete Customer's transactions (such as device fingerprint if the customer elects to use ThreatMetrix).	