CARDINAL CONSUMER AUTHENTICATION
DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is an agreement between you and the entity you represent ("Customer" or "you"), on the one hand, and CardinalCommerce Corporation and/or any other applicable affiliated CardinalCommerce contracting entity(ies) ("Cardinal" or "CardinalCommerce"), on the other hand. It forms part of any written or electronic agreement between you and Cardinal under which Cardinal Processes Personal Information on your behalf (each, an "Agreement"), except with respect to any Agreement under which you and Cardinal have entered data processing terms that address the subject matter hereof. Each of Cardinal and Customer may be referred to herein as a "party" and collectively as the "parties."

1 **Processing of Customer Personal Information.**

1.1 **Processor designation**. The parties acknowledge and agree that with respect to the Personal Information that Cardinal Processes on behalf of Customer ("Customer Personal Information") to provide Cardinal Products and Services, that Cardinal is a "processor" or "service provider" or such equivalent term under Applicable Data Protection Law, if any. Such Cardinal Products and Services may include, by way of example and for illustrative purposes, the Processing detailed on the Details of Processing Customer Personal Information (Exhibit 3).

1.2 **Authorization to Process**. Cardinal will Process Customer Personal Information to provide Cardinal Products and Services, and Customer authorizes Cardinal to Process Customer Personal Information solely in connection with the following activities:

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

1.2.2 Based on the instructions of Customer, Cardinal will transfer Customer 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;

1.2.3 As reasonably necessary to enable Cardinal to comply with any other directions or instructions provided by Customer; and

1.2.4 To detect, reduce or eliminate fraud.

2 **Compliance with Law**. Cardinal, in its provision of services to Customer, and Customer, in its use of the services, shall Process Customer Personal Information in accordance with Applicable Data Protection Law. To the extent necessary 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 the GDPR Schedule and/or CCPA Schedule, each, to the extent applicable.

3 **Privacy Notice.** Customer shall provide its Data Subjects with all privacy notices, information and any necessary choices and shall obtain any necessary consents to enable Cardinal to comply with Applicable Data Protection Law.

4 **Data Subject Rights**. Processor will, to the extent legally permitted, provide reasonable assistance to Customer to respond to requests from Data Subjects 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 Cardinal Products and Services. Where Cardinal receives any such

request, it shall advise the Customer that the Customer is responsible for handling such requests by a Data Subject in accordance with Applicable Data Protection Law.

5 **Engaging with Sub-Processors**. Processor shall ensure that when engaging with another data processor (a "Sub-Processor") for the purposes of carrying out specific Processing activities on behalf of Customer, there is a written agreement between Processor and the relevant Sub-Processor that provides at least the same level of protection for Customer Personal Information as set forth in this DPA.

6 **Staff**. Cardinal shall ensure that persons authorized to Process Customer Personal Information are under an appropriate obligation of confidentiality in accordance with applicable laws or regulations governing the same.

7 **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 to the rights and freedoms of natural persons, Cardinal will implement technical and organizational measures to ensure a level of security appropriate to that risk. In assessing the appropriate level of security, Cardinal 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. Cardinal shall provide reasonable assistance to Customer in ensuring Customer meets its own compliance obligations with respect to these same security measures. The parties shall also comply with Payment Card Industry Data Security Standard (PCI-DSS) as set out in the Agreement.

8 **PCI Compliance**. Cardinal's storage, processing, and transmission of any payment instrument data shall comply with the PCI-DSS, and Cardinal shall regularly validate its compliance as determined by its status as a Service Provider (as Service Provider is defined in the PCI Security Standard). Upon Customer's request, Cardinal shall provide Customer with written confirmation of its PCI-DSS compliance status.

9 **Security Breach**

9.1 In the event of an actual Security Breach (defined below) affecting Customer Personal Information contained in Cardinal's systems, Cardinal shall (i) investigate the circumstances, extent and causes of the Security Breach and report the results to Customer and continue to keep Customer informed on a regular basis of the progress of Cardinal's investigation until the issue has been effectively resolved; and (ii) cooperate with Customer in any legally required notification by Customer to affected Data Subjects.

9.2 Cardinal shall notify Customer without undue delay upon Cardinal or any Sub-Processor becoming aware of an actual Security Breach affecting Customer Personal Information, providing the Customer with sufficient information and reasonable assistance to allow Customer to meet its obligations under Applicable Data Protection Law to (i) notify a Supervisory Authority (as defined under Applicable Data Protection Law) of the Security Breach; and (ii) communicate the Security Breach to the relevant Data Subjects.

9.3 Except as required by applicable law or regulation, Cardinal will not make (nor permit any third party to make) any statement concerning the Security Breach that directly or indirectly references Customer, unless Customer provides its explicit written authorization.

9.4 To the extent that a Security Breach was caused by Customer or Customer's Data Subjects, end users or clients, Customer shall be responsible for the costs arising from the Cardinal's provision of assistance under this section 9.

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

11 **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 this DPA, this DPA does not apply to any data or information that does not relate to one or more identifiable individuals, that has been aggregated or de-identified in accordance with Applicable Data Protection Law, or to the extent that Cardinal and you have entered separate data processing terms that address the subject matter hereof.

12 Cardinal shall pay reasonable costs related to a Security Breach, but only to the extent (i) that Customer is a direct licensee of Cardinal (as opposed to a customer of a reseller of, or other third party offering Cardinal's products and services) and (ii) such Security Breach is caused by or attributable to Cardinal's negligence or breach of this DPA, including reasonable costs of breach notifications and any credit monitoring for Data Subjects required by Customer, up to an amount not to exceed one (1) million US dollars ($1,000,000.00), or such amount otherwise expressly mandated by Applicable Data Protection Law, solely to the extent such mandated amount exceeds one million US dollars.

13 **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"), UK Data Protection Laws, 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"), 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.
"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 a Data Subjects 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, unauthorised 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", 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.
"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 Cardinal Products and Services or to the extent 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 Cardinal 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 required or 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 consistently with Applicable Data Protection Law;

II. Stop and remediate unauthorized use of Customer Personal Information; and

III. To conduct reasonable assessments of Cardinal's policies and technical and organizational measures. Cardinal 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

4 Each of Cardinal 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 Cardinal, 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 your use of Cardinal Products and Services or to the extent 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 **Additional Processor Obligations**

1.1 **Processing of Customer Personal Information**. Processor shall Process Customer Personal Information pursuant only to documented reasonable instructions from Customer (including instructions with respect to Transfers of Customer Personal Information to a third country, if applicable) unless Processor is required to otherwise Process Customer Personal Information by Applicable Data Protection Law. In such circumstances, Processor shall inform Customer of that legal requirement before Processing, unless prohibited from doing so by applicable law, on important grounds of public interest.

1.2 **Use of Sub-Processor**

1.2.1 Processor will not engage any Sub-Processor without the specific or general written authorization from Customer. In accordance with this section 1.2 of this GDPR Schedule, Customer provides authorization for Processor to engage with the Sub-Processors listed on Exhibit 1.

1.2.2 Processor shall inform Customer of any intended changes concerning the addition or replacement of other Sub-Processors to give Customer the reasonable opportunity to object to such changes. In the event Customer objects to Processor's change or addition of Sub-Processor, Customer shall promptly notify Processor of its objections in writing within ten (10) business days after receipt of Processor's notice of such change or addition.

1.2.3 Processor may, at its option, undertake reasonable efforts to make available to Customer a change in Cardinal Products and Services or recommend a commercially reasonable change to Customer's configuration or use of Cardinal Products and Services to avoid Processing of Customer Personal Information by the objected-to new Sub-Processor. If Processor is unable to make available such change within a commercially reasonable period of time, Customer may terminate the Agreement with respect to only those aspects of Cardinal Products and Services, which cannot be provided by Processor without the use of the objected-to new Sub-Processor by providing written notice to Processor. If the Cardinal Products and Services as a whole cannot be performed without the objected-to new Sub-Processor, Customer may terminate the entire Agreement, provided that Customer's objections to the new Sub-Processor are (i) commercially reasonable and (ii) based solely on reasonable concerns related to information security.

1.2.4 Processor reserves the right to maintain its Sub-Processor list through means such as publication of its Sub-Processor list online.

2 **Data Protection Impact Assessments and Prior Consultation with Regulator**

2.1 Processor shall immediately inform Customer if, in Processor's opinion, Customer's instructions would be in breach of Applicable Data Protection Law. Customer agrees that Processor shall be under no obligation to take actions designed to form any such opinion.

2.2 Processor shall provide reasonable assistance to Customer with any legally required (a) data protection impact assessments; and (b) prior consultations initiated by the Customer 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 Processor on behalf of Customer under the Agreement taking into account the nature of the Processing and information available to Processor.

3 **Demonstrating Compliance with this DPA**

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

3.2 Customer's right under section 3.1 of this GDPR Schedule is subject to the following:

3.2.1 If requested by Customer, on no more often than an annual basis during the term of the Agreement, Processor shall (i) provide Customer with a copy of the result of its annual SOC 2, Type II audit within a reasonable period after receiving the report from its auditor; and (ii) provide Customer with a copy of the Attestation of Compliance resulting from its annual PCI audit within a reasonable period after receiving the report from its Qualified Security Assessor.

3.2.2 To the extent that 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 Customer with an audit report issued by an independent third party auditor (provided that Customer will comply with appropriate confidentiality obligations as set out in the Agreement and shall not use such audit report for any other purpose), Customer agrees that it will not conduct an audit or inspection under section 3.1 above.

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

4.1 **Transfers subject to the GDPR, UK GDPR or Swiss DP Laws:** Module 2 (Transfer controller 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 Cardinal and any of its affiliated entities in the United States or other third countries ("Cardinal Entities"). The parties acknowledge and agree that Module 2 (Transfer controller to processor) of the EEA Standard Contractual Clauses is hereby incorporated by reference and;

4.1.1 Customer and any of its commonly owned or controlled affiliates that have signed an Agreement for Cardinal Product and Services ("Customer Entities") shall be deemed to be "data exporters" and the Cardinal Entities shall be the "data importer";

4.1.2 Clause 7 – *Docking clause* shall apply;

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

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

4.1.5 Clause 13(a) – *Supervision*.

4.1.6 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."

4.1.7 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."

4.1.8 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."

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

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

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

4.1.12 Transfers subject to the UK GDPR: where the Transfer is subject to the UK GDPR, the EEA Standard Contractual Clauses 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 2.

4.1.13 If there is any conflict or inconsistency between a term in the body of this DPA, an Agreement and a term in Module 2 (Transfer controller to processor) of the EEA Standard Contractual Clauses as incorporated into this DPA, the term in Module 2 (Transfer controller to processor) of the EEA Standard Contractual Clauses shall take precedence.

SCHEDULE C
RESELLER ADDENDUM

This Reseller Schedule applies in addition to any terms set forth in the body of the DPA (and is incorporated therein) when Customer is authorized to resell the Cardinal Products and Services. Capitalized terms not defined herein have the meaning assigned to them under the DPA. To the extent there are any conflicts between this Reseller Schedule and the DPA, this Reseller Schedule shall prevail.

1 **Customer Personal Information**. The term Customer Personal Information is amended to mean the Personal Information that Cardinal Processes on behalf of Customer's clients.

2 **Sub-Processor designation**. Section 1.1 of the body of the Agreement is amended in its entirety to state:

> **Sub-Processor designation**. The parties acknowledge and agree that with respect to the Customer Personal Information that Cardinal Processes to provide Cardinal Products and Services, that Customer's clients shall be considered as "controllers" (or equivalent term pursuant to Applicable Data Protection Laws), Customer shall be considered a "data processor", and Cardinal shall be considered a "sub-processor" engaged by Customer to carry out specific processing activities for Customer's clients. Such Cardinal Products and Services may include, by way of example and for illustrative purposes, the Processing detailed on the Details of Processing Customer Personal Information (Exhibit 3).

3 **Privacy Notice**. Section 3 of the body of the Agreement is amended in its entirety to state:

> **Privacy Notice**. Customer shall ensure that its clients provide their Data Subjects with all privacy notices, information and any necessary choices and shall obtain any necessary consents to enable Cardinal to comply with Applicable Data Protection Law.

4 **Data Subject Rights**. The last sentence of section 4 of the body of the Agreement is amended in its entirety to state:

> Where Cardinal receives any such request, it shall advise the Customer that its applicable client is responsible for handling such requests by a Data Subject in accordance with Applicable Data Protection Law.

5 **Cross-Border Transfers**. In lieu of section 4 of the GDPR schedule, the following provision shall apply. Cardinal shall comply with Customer's documented instructions concerning the Transfer of Customer Personal Information to a third country. Cardinal shall only Transfer any Customer Personal Information outside the Customer's applicable jurisdiction or the End-User's resident jurisdiction, including, without limitation, outside the European Economic Area ("EEA"), the UK or Switzerland, only in compliance with the Applicable Data Protection Law. Customer agrees and acknowledges that Cardinal 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 Cardinal 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 Customer and any of their commonly owned or controlled affiliates that have signed an Agreement for Cardinal Product and Services ("Customer Entities"), shall be deemed to be the "data exporter" and the Cardinal 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*

5.1.6 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."*

5.1.7 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."*

5.1.8 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."*

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

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

5.1.11 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.

5.2 **Transfers subject to the UK GDPR.** where the Transfer is subject to the UK GDPR, the EEA Standard Contractual Clauses 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 2.

5.2.1 If there is any conflict or inconsistency between a term in the body of this DPA, an Agreement and a term in Module 2 (Transfer controller to processor) of the EEA Standard Contractual Clauses, incorporated into this DPA, the term in Module 2 (Transfer controller to processor) of the EEA Standard Contractual Clauses shall take precedence.

EXHIBIT 1
SUB-PROCESSORS

The following Sub-Processors may be used in the provision of Cardinal Products and Services.

Company	Address	Description
Visa USA, Inc.	44901 Russell Branch Pkwy, Ashburn, VA	Security and fraud
	8910 S Ridgeline Blvd Highlands Ranch, CO	

EXHIBIT 2
INFORMATION REQUIRED FOR THE EEA STANDARD CONTRACTUAL CLAUSES

Table 1: Information to be incorporated into the EEA Standard Contractual Clauses

Information to be incorporated into the EEA Standard Contractual Clauses	
ANNEX I A. List of Parties	
Data EXPORTER identity and contact details	
Name	Customer Entities
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 3 under "Nature and Purpose of the Processing".
Role (controller/processor):	Module 2: Controller Module 3: Processor
Data IMPORTER identity and contact details	
Name	Cardinal 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 3 under "Nature and Purpose of the Processing".
Role (controller/processor):	Processor
ANNEX I B. Description of Transfer	
Categories of data subjects whose personal data is transferred	As set out in the table in Exhibit 3 under "Categories of Data Subjects".
Categories of personal data transferred	As set out in the table in Exhibit 3 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 3 under "Nature and Purpose of the Processing".
Purpose(s) of the data transfer and further processing	As set out in the table in Exhibit 3 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 Cardinal's retention policies, for only as long as is required to meet Cardinal'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 3 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.	CardinalCommerce 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 Cardinal Corporation and its affiliates (such standards, the "PCI Standards"). As evidence of compliance, Cardinal will provide its current Attestation of Compliance signed by a Payment Card Industry Qualified Security Assessor upon Customer's written request.

	CardinalCommerce 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. CardinalCommerce engages its independent certified public accountants to conduct a review of Cardinal Corporation's operations and procedures at Cardinal 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 Cardinal Corporation. Upon request, and subject to standard confidentiality obligations, Cardinal will provide its most recent SSAE 18 and, in Cardinal's 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 Transaction Services: initiatives, products, processes and supporting technology are assessed from a data privacy perspective, allowing Cardinal to embed privacy controls to mitigate risks at early stages (privacy by design). Cardinal 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 through their account manager.

ANNEX III List of Sub-Processors *The controller has authorised the use of the following sub-processors:*
As set out in Exhibit 1

EXHIBIT 3
DETAILS OF PROCESSING CUSTOMER PERSONAL INFORMATION

Service	Nature and purpose of processing	Types of personal information	Categories of data subjects related to the personal information
Cardinal Consumer Authentication ("CCA")	CCA provides Customer authentication services, to include an authentication outcome that may be used by the Customer in their own risk decision in an effort to reduce fraud. Customer Personal Information is collected by Cardinal as required by EMVCo authentication protocols for 3D Secure in the operation and delivery of the service.	When presented, Cardinal will use transaction information, including, without limitation, account number, IP address, IP geolocation of the consumer device, device characteristics, cardholder name, billing address, shipping address, email and phone number. Further detail on these fields is included in the applicable Technical Documentation provided at the time of implementation of the Service.	Data Subjects as defined under this Agreement, include: credit card holders, debit card holders and all end users whose cardholder or bank account data submitted to Processor for processing.