PCI PAL DATA PRIVACY AND SECURITY ADDENDUM

BACKGROUND

This Data Privacy and Security Addendum ("DPSA") is entered into in addition to and incorporated by reference by the Master Agreement (or other written or electronic agreement between PCI Pal and Customer) for the Services and reflects the parties' agreement regarding the processing of Customer Data. This DPSA is intended to comply with various global data privacy laws and regulations.

Customer enters into this DPSA on its own behalf and in the name of and on behalf of its Affiliates, to the extent that PCI Pal processes Customer Data on behalf of such Affiliates.

APPLICATION

If Customer is a party to the Master Agreement, this DPSA is an addendum to and forms part of the Master Agreement. The PCI Pal entity that is a party to the Master Agreement is party to this DPSA.

If Customer has executed a Service Order Form and/or Statement of Work with PCI Pal pursuant to the Master Agreement, but is not itself a party to the Master Agreement, this DPSA is an addendum to that Service Order Form and/or Statement of Work (and any subsequent renewals), and the PCI Pal entity that is a party to that Service Order Form and/or Statement of Work is a party to this DPSA.

If Customer is not a party to a Service Order Form and/or Statement of Work, EULA or Master Agreement directly with PCI Pal, but is a customer indirectly through an authorized reseller of PCI Pal's services, then this DPSA is not valid or legally binding and such entity should contact its authorized reseller to discuss whether any amendment to its agreement with that reseller is required.

This DPSA is not intended to replace any comparable or additional rights related to the Processing of Customer Data contained in Customer's Master Agreement (including any existing data processing agreement or addendum to the Master Agreement).

AGREED TERMS

1.Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPSA. Capitalised terms used in this DPSA but not defined herein shall have the meaning given to them in the Master Agreement or the Data Protection Legislation.

1.1Definitions:

Affiliates: means a business entity that: (a) Controls the party; (b) is Controlled by the party; or (c) is under common Control with the party, but only during the time that such Control exists. Under this DPSA, "Control" means the ability to determine the management policies of an entity through ownership of a majority of shares or by control of the board of management.

Controller, Processor, Data Subject, Personal Data, Personal Data Breach and Processing: have the meanings given to them in the Data Protection Legislation.

Controller Instructions:: means the instructions from the entity acting as the Controller.

Customer: means the customer entity which has entered into the Master Agreement and/or the customer receiving the Services and any of its Affiliates.

Customer Data:means the Personal Data that is uploaded to the Services by Customer or an entity acting on behalf of Customer.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; the EU GDPR; the California Consumer Privacy Act; and all other

legislation and regulatory requirements in force from time to time which apply to a party relating to the Processing of Personal Data (including, without limitation, the privacy of electronic communications);

EU GDPR: means the General Data Protection Regulation ((EU) 2016/679).

EEA: means the European Economic Area.

Master Agreement: means the agreement executed by PCI Pal and Customer for the provision of Services, including any electronic agreement and/or terms of service.

Records: has the meaning given to it in Clause 8.

Services: means the software, cloud services, professional services and support services provided by PCI Pal to Customer as further described under the Master Agreement.

Subprocessor: means any subprocessor engaged by PCI Pal who agrees to process Customer Data on behalf of PCI Pal in accordance with Controller Instructions, this DPSA, or the Master Agreement.

Term: means this Agreement's term as defined in Clause 2.1.

UK GDPR: has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2The Annexes form part of this DPSA and will have effect as if set out in full in the body of this DPSA. Any reference to this DPSA includes the Annexes.

1.3A reference to writing or written includes email.

2.Term and Termination

2.1Term: This DPSA will remain in full force and effect so long as:

(a)the Master Agreement remains in effect; or

(b)PCI Pal retains any of Customer Data related to the Master Agreement in its possession or control (the “Term”).

2.2Any provision of this DPSA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement to protect Customer Data will remain in full force and effect.

2.3Termination: If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Master Agreement obligations, the parties may agree to suspend the Processing of Customer Data until that Processing complies with the new requirements. If the parties are unable to bring Customer Data Processing into compliance with the Data Protection Legislation within thirty (30) days, either party may terminate the Master Agreement on not less than thirty (30) days’ written notice and without liability to the other party.

3.Data Processing

3.1Scope: This DPSA governs the Processing of Customer Data (with Customer as the Controller) by PCI Pal as the Processer. Annex A describes the subject matter, duration, nature and purpose of the Processing and Customer Data categories and Data Subject types in respect of which PCI Pal may Process Customer Data to provide the Services.

3.2Compliance with Data Protection Legislation: Each party shall comply with the Data Protection Legislation applicable to it. If PCI Pal believes that the Data Protection Legislation applicable to it and any Subprocessor prevents them from fulfilling Controller Instructions and its respective obligations under this DPSA and the sub-processing agreement, PCI Pal shall promptly notify Customer and Customer shall be entitled to suspend transfer of Customer Data or terminate this DPSA.

3.3PCI Pal Personnel: PCI Pal will ensure that all of its personnel:

(a)are informed of the confidential nature of Customer Data and are bound by written confidentiality obligations and use restrictions in respect of Customer Data;

(b)have undertaken training on the Data Protection Legislation and how it relates to their handling of Customer Data and how it applies to their particular duties; and

(a)are aware both of PCI Pal's duties and their personal duties and obligations under the Data Protection Legislation and this DPSA. PCI Pal will take reasonable steps to ensure the reliability, integrity and trustworthiness of and conduct background checks consistent with applicable domestic law on all of PCI Pal's personnel with access to Customer Data.

3.4Complaints, Data Subject Requests and Third-party Rights: PCI Pal will:

(a)promptly notify Customer if it receives any complaint, notice or communication that relates directly or indirectly to the processing of Customer Data or to either party's compliance with the Data Protection Legislation;

(b)promptly notify Customer if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation;

(c)assist Customer, insofar as this is possible (considering the nature of the processing and the information available to PCI Pal), in responding to any complaint, notice, communication or Data Subject request; and

(b)not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with Customer's written instructions, or as required by the Data Protection Legislation.

3.5Cross-border Transfers: If directed by Controller Instructions, PCI Pal (and any Subprocessor) will not transfer or otherwise process Customer Data outside the UK or the EEA without obtaining Customer's prior written consent and subject to the parties ensuring lawful safeguards are in place prior to any transfer.

3.6Deletion and/or Return of Customer Data: On termination of this DPSA, PCI Pal and its Subprocessors shall, at Customer's election and on its request (unless otherwise restricted or directed by Data Protection Legislation):

(a)return all Customer Data Processed by PCI Pal or any Subprocessor and the copies thereof directly to Customer; or

(b)delete Customer Data and provide notice to Customer that it has done so.

4.PCI Pal's Responsibilities

4.1DPO: PCI Pal has appointed a Data Protection Officer in accordance with the applicable Data Protection Legislation. The privacy office may be contacted for urgent enquiries by emailing dataprotection@pcipal.com.

4.2Access or Use: PCI Pal will only process Customer Data to the extent, and in such a manner, as is necessary to perform the Services and in accordance with the Controller Instructions. PCI Pal will not process Customer Data for any other purpose or in a way that does not comply with this DPSA or the Data Protection Legislation. For the avoidance of doubt, PCI Pal will never sell Customer Data.

4.3Disclosure: PCI Pal will maintain the confidentiality of Customer Data and will not disclose Customer Data to third parties unless Customer or this DPSA specifically authorises the disclosure, or as required by the Data Protection Legislation, court or regulator. If the Data Protection Legislation, court or regulator requires PCI Pal to process or disclose the Personal Data to a third-party, PCI Pal will inform Customer of such legal or regulatory requirement and give Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

4.4Compliance: PCI Pal will reasonably assist Customer with meeting Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of PCI Pal's processing and the information available to PCI Pal, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the regulator under the Data Protection Legislation. For the avoidance of doubt, the Customer must remain responsible for conducting any data privacy impact assessments. PCI Pal will provide all information, documentation and assistance necessary for Customer to meet all the requirements of applicable Data Protection Legislation and to demonstrate compliance with such requirements.

4.5Security: PCI Pal will at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful Processing, access, copying, modification, reproduction, display or distribution of Customer Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Customer Data including, but not limited to, the security measures set out in Annex B. The technical and organisational measures are subject to technical progress in accordance with industry standards and further development. PCI Pal may implement alternative adequate measures provided that this does not reduce the security provided. Subprocessors provide sufficient guarantees in respect of the technical and organisational security measures specified in this DPSA and in accordance with Data Protection Legislation.

5.EU Digital Operational Resilience Act Addendum(DORA): if Customer is a financial entity within the meaning of Article 2 of DORA, PCI Pal will comply with its obligations under Annex C.

5.Security Breach Notification

5.1Notification: PCI Pal will without undue delay and in any event within seventy-two (72) hours notify Customer in writing if it becomes aware of:

(a)any accidental, unauthorised or unlawful processing of Customer Data; or

(b)any Personal Data Breach.

5.2Information: Where PCI Pal becomes aware of (a) or (b) above, it will, without undue delay, also provide Customer with the following written information:

(a)description of the nature of (a) or (b)), including the categories of in-scope Customer Data and approximate number of both Data Subjects and Customer Data records concerned;

(b)the likely consequences; and

(c)a description of the measures taken or proposed to be taken to address (a) or (b), including measures to mitigate its possible adverse effects.

5.3Co-operation and Investigation: Following any accidental, unauthorised or unlawful Customer Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, PCI Pal will reasonably co-operate with Customer in Customer's handling of the matter, including:

(a)assisting with any investigation;

(b)facilitating interviews with PCI Pal's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

(c)making available relevant records, logs, files, data reporting and other materials required to comply with Data Protection Legislation; and

(d)taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Customer Data processing.

6.Subprocessing

6.1Customer agrees that PCI Pal may use Subprocessors solely in connection with the provision of the Services. PCI Pal's current Subprocessors are listed in Annex A. Customer consents to PCI Pal's use of such Subprocessors.

6.2Other than those Subprocessors as set out in Annex A, PCI Pal may not authorise any other third-party or subcontractor to process Customer Data, unless:

(a)Customer is provided with an opportunity to object to the appointment of each Subprocessor within 10 working days after PCI Pal supplies Customer with full details regarding such Subprocessor;

(b)PCI Pal enters into a written contract with the Subprocessor that contains terms substantially the same as those set out in this DPSA, in particular, in relation to requiring appropriate technical and organisational data security measures; and

(c)PCI Pal maintains control over all of Customer Data it entrusts to the Subprocessor.

6.3Where the Subprocessor fails to fulfil its obligations under the written agreement with PCI Pal which contains terms substantially the same as those set out in this DPSA, PCI Pal remains fully liable to Customer for the Subprocessor's performance of its agreement obligations.

7.Financial Institutions

7.1Applicability: This Clause only applies where: (a) Customer is an institution as defined in Article 4(1)(3) of Regulation (EU) No 575/2013 or otherwise subject to the EBA.REC/2017/03; or (b) Customer uses the Services for purposes that are subject to regulatory oversight by EEA authorities (including BaFin) with authority to regulate Customer's financial service activities.

7.2Access and Audit: Subject to appropriate confidentiality obligations, PCI Pal agrees to provide Customer and Customer's statutory auditor with: (a) full access to its business premises, and (b) rights of inspection and auditing related to the Services. The following conditions apply:

(a)Customer will exercise such rights in a risk-based and proportional manner considering the nature of the Services.

(b)Customer may appoint a third party to perform such audits, provided that Customer can verify the third-party has the necessary skills and knowledge to perform the audit effectively.

(c)Customer must provide written notice in a reasonable time period prior to an on-site visit.

(d)If Customer's audit rights could risk another PCI Pal customer's data or services, PCI Pal and Customer will agree on an alternate means to provide necessary assurances.

(e)When possible, Customer will rely on certifications, reports, and attestations in place of an audit.

7.3PCI Pal Outsourcing. PCI Pal will enter into written agreements with any Subprocessors that contain obligations and restrictions substantially similar to those found herein.

8.Records

8.1PCI Pal will keep detailed, accurate and up-to-date written records regarding any processing of Customer Data, including the access, control and security of Customer Data, approved Subprocessors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 4.5 ("Records").

9.Audits

9.1Subject to appropriate confidentiality obligations, PCI Pal will permit Customer and/or its independent third-party auditors to audit PCI Pal's compliance with its obligations under this DPSA, once per annum and on at least 30 days' notice, during the Term. PCI Pal will give Customer and/or its third-party auditors reasonable and necessary assistance to conduct such audits. The assistance may include:

(a)physical access to, remote electronic access to, and copies of the Records and any other relevant information held at PCI Pal's premises or on systems storing Customer Data;

(b)access to and meetings with any of PCI Pal's personnel reasonably necessary to provide all explanations and perform the audit effectively; and

(c)inspection of all Records and the infrastructure, electronic data or systems, facilities, equipment, or application software used to process Customer Data.

9.2Any audit performed under this Clause 9 shall be conducted during PCI Pal's business hours and with minimal disruption to its business operations. Customer and/or its third-party auditors will comply with any reasonable health and safety, access and security policies notified to it by PCI Pal.

9.3The notice requirements in Clause 9.1 will not apply if a Personal Data Breach has occurred or PCI Pal is in material breach of any of its obligations under this DPSA or any of the Data Protection Legislation.

9.4On Customer's written request, PCI Pal will make all relevant certifications available to the Customer for review, including: (a) PCI Pal's latest PCI DSS certification, (b) PCI Pal's ISO/IEC 27001 certification; and any other relevant certifications. Customer will treat such certifications as the PCI Pal's confidential information under the Master Agreement.

10.Warranties

10.1PCI Pal warrants and represents that:

(a)it and anyone operating on its behalf will process Customer Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards, and other similar instruments;

(b)it has no reason to believe that the Data Protection Legislation prevents it from providing the Services; and

(c)considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised, or unlawful processing of Customer Data and the loss or damage to, Customer Data, and ensure a level of security appropriate to:

(i)the harm that might result from such accidental, unauthorised, or unlawful processing and loss or damage;

(ii)the nature of Customer Data protected; and

(iii)comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 4.5.

10.2The Customer warrants and represents that PCI Pal's expected use of Customer Data to provide the Services and as specifically instructed by Customer will comply with the Data Protection Legislation.

11.Notice

11.1Any notice or other communication given to a party under or in connection with this DPSA must be in writing and delivered in accordance with the applicable notice provisions under the Master Agreement.

12.Liability

UNLESS OTHERWISE AGREED UNDER THE MASTER AGREEMENT, PCI PAL'S TOTAL AGGREGATE LIABILITY IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND BREACH OF STATUTORY DUTY HOWSOEVER ARISING), MISREPRESENTATION (WHETHER INNOCENT OR NEGLIGENT), RESTITUTION OR OTHERWISE, ARISING IN CONNECTION WITH THE PERFORMANCE OR CONTEMPLATED PERFORMANCE OF THIS DPSA OR ANY COLLATERAL CONTRACT INSOFAR AS IT RELATES TO THE OBLIGATIONS SET OUT IN THIS DPSA, OR THE DATA PROTECTION LEGISLATION SHALL BE LIMITED TO $500,000.

ANNEX A

Data Processing Description

Nature and Purpose of Processing: PCI Pal will Process Customer Data pursuant to the Master Agreement and as further instructed by Controller Instructions.

Duration of Processing: Subject to the DPSA, PCI Pal will Process Customer Data for the duration of the Master Agreement, unless otherwise agreed in writing.

Personal Data Categories:

Customer Data is Processed to the extent of which is determined and controlled by Controller Instructions, and may include:

- First and last name
- Contact information (email, phone number, physical business address)
- Cardholder data (full Primary Account Number (PAN), cardholder name, expiration date, and/or service code)

Data Subject Types: Customer Data is Processed to the extent determined and controlled by Controller Instructions, and may include the following categories of Data Subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors or freelancers of Customer (who are natural persons)
- Customer's users authorized by Customer to use the Services
- Customer's customers (who are natural persons)

Approved Subprocessors:

Subprocessor	Location	Purpose/Services	Further Information
Amazon Web Services (AWS)	United States Ireland AWS region selected by Customer	Cloud services, website hosting, and data center services	https://aws.amazon.com/
Dropbox	United States	Document hosting	https://www.dropbox.com/
Microsoft Corporation	United States	Cloud services (Speech Recognition services only), Business administration, delivery, support and related services	https://www.microsoft.com
Salesforce.com Inc	United States	Data integration, as applicable	https://www.salesforce.com/
Docusign	United States	Contract signature tool	https://www.docusign.com

Customer Data will reside in the AWS region selected by Customer throughout the term of the relevant Service Order Form. PCI Pal will not change the AWS region without Customer's prior written consent.

ANNEX B

Security Measures

PCI Pal provides secure payment processing software delivered as a service (the “Platform”). All content in the Platform is stored in the cloud on AWS. Beyond the Platform, PCI Pal’s own employees also store emails and documents in Dropbox, Microsoft and Salesforce. This Annex B (Security Measures) sets out the minimum security measures PCI Pal shall implement in respect of the Services. PCI Pal may amend these measures from time to time in accordance with best industry practices and never in a way so as to degrade the level of security set forth herein.

Key Points:

- PCI Pal does not store or retain any payment card data.
- PCI Pal uses third-party service providers for operational aspects of PCI Pal’s business that involve Customer Data. PCI Pal only uses reputable vendors and verifies their security and privacy standards to ensure they are in compliance with industry standards.
- PCI Pal is PCI DSS compliant and ISO 270001, ISO 23201, ISO 14001, and ISO 9001 certified.
- All data, including Customer Data is encrypted, in transit and at rest, in accordance with industry best practices.
- PCI Pal operations are fully hosted in secure remote cloud environments. There are no on-premise servers or equipment at our corporate facilities except network routers and switches that provide internet connectivity for in-office workers. These networks are operated on enterprise grade equipment and configurations.

1.Security Measures

1.1Data Hosting: PCI Pal’s processing environment is hosted on Amazon Web Services (AWS) secure and resilient physical infrastructure, running Virtual Machines based on the latest patched operating systems and automatically hardened to CIS standards, operating from inside network segments designed to monitor, log and restrict traffic to necessary minimums. AWS are certified to a wide array of international standards for physical security, data privacy and business continuity, which can be reviewed here - https://aws.amazon.com/compliance/programs/. PCI Pal does not operate any on-premise servers, nor any business- or service-critical assets from our offices or other owned physical spaces, and we utilise reputable third-party service providers for all operational aspects of our business that involve Customer Data.

1.2Data Storage

(a)Data, including cardholder data, sent to PCI Pal or captured within the Platform application in the process of performing the Services (“Session Data”) are held solely in volatile memory of secured processing servers within AWS for the duration of a session and are promptly destroyed at the end of a session by automatic memory de-indexing and reallocation mechanisms without being written to disk or recorded. These secured processing servers are automatically created by Infrastructure-as-Code deployment scripts running the latest application version branch, and are designed to process, scale-up and -down, create audit trails, and be destroyed and replaced without need of manual human access.

(b)PCI Pal operates a logging cluster hosted within AWS which holds telephony/network routing data (SIP messages, IP addresses/phone numbers) and payment transaction metadata (payment amount, result) as well as internal security/audit logs (admin actions, authentications, changes to certain critical configuration), which are held to comply with its legal obligations, to provide support and troubleshooting to customers, and to allow PCI Pal to improve the Services. There is no other storage of any service-related data in any other system or with any other Subprocessor.

(c)Customer Data will reside in the AWS region selected by Customer throughout the term of the relevant Service Order Form. PCI Pal will not change the AWS region without Customer’s prior written consent.

1.3Encryption: Data transmitted to or from the Platform is always encrypted. PCI Pal supports strong modern ciphers for HTTPS with TLS 1.2 for web traffic, and can support SRTP, encrypted VPN, or SD-WAN solutions for Customer telephony designs as selected by Customer. Data stored at rest is also encrypted with AES-256, block level encryption (more information can be found here: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html). All ciphers and solutions may be subject to further

change and development as industry best practices relating to encryption evolve, but will never be degraded to a lesser standard of security as described herein.

1.4Authentication: Each customer owns and operates within a provided tenant in the Platform application, and can only view that tenant and any subtenant (e.g. a reseller may view and provide administrative services for their resold customers but cannot see that any other reseller operates a tenant nor view those tenants). Customer access and use of the Services is conditional upon customers' compliance with the Acceptable Use Policy - https://www.pcipal.com/acceptable-use-policy/. PCI Pal enforces password complexity standards upon all direct frontend application access, which each Customer tenant may vary within acceptable boundaries to match their own guidelines. PCI Pal does not directly support multi-factor authentication (MFA) for direct frontend application authentication; however this can be achieved via standard integrations or SSO with systems utilising MFA.

1.5Incident Management and Vulnerability Scanning: PCI Pal operates a 24/7 Incident Response team, with First Line responders directly accessible by customers to report any service-impacting events, disruptions, or concerns for security in accordance with the service levels for response set out in the relevant customer contract. PCI Pal operates a wide array of monitoring and alerting systems and components that feed into the 24/7 Incident Response process to ensure that any identified or disclosed event of concern can be assessed and remediated, with regular communications to impacted customers. PCI Pal uses WAF and IDS systems to prevent and detect security incidents. PCI Pal conducts penetration testing and vulnerability scanning at least every six months or quarter (respectively) as well as SAST scanning of all prospective code releases to ensure potential vulnerabilities and concerns are identified and remediated swiftly. PCI Pal tracks the severity of reported issues within the internal issue tracking system and security issues are immediately triaged to be remediated.

1.6Asset Management: There are no on-site physical computing assets. All of PCI Pal's production and internal corporate services are hosted in secure remote cloud environments. Employee end-user devices are encrypted with disk-level encryption, centrally managed from cloud MDM solution (including password standards and firewall configurations), and are monitored with alerting from a 24/7 SOC solution. Removable storage media are generally forbidden with specific exemptions permitted with approval by the Information Security & Compliance team, and decommissioned assets are securely disposed with certified destruction to ensure any locally-held data is destroyed.

1.7Physical Security: PCI Pal production data is processed and stored in world-renowned data centres which use state-of-the-art access controls, including:

(a)Fencing;

(b)Vehicle assess barriers;

(c)Electronic access cards;

(d)Biometric checks;

(e)Intrusion detection;

(f)Security camera surveillance; and

(g)24/7 trained security personnel.

PCI Pal's corporate offices are located in access-controlled facilities.

2.Risk Assessment

2.1Security is at the core of what we do and we continuously perform risk assessments, including:

(a)The enforcement of code reviews. All code is reviewed prior to merge and Secure Coding Guidelines are considered during manual code reviews. Automatic code scanning for security vulnerabilities is carried out on any new code, covering OWASP Top 10 and SANS 25 amongst others;

(b)Vendor assessments, each time new vendors are onboarded or changed. Vendor relationships are not accepted if the security standards are lower than our own and best practices;

(c)Vulnerability assessments; and

(d)Annual third-party audits, including against certified standards. Copies of certifications can be provided on request.

Annex C

EU Digital Operational Resilience Act Addendum

1. Application

1.1 This EU Digital Operational Resilience Act Addendum (Addendum) shall be incorporated into and form part of the Agreement if:

(a) Customer is a financial entity within the meaning of Article 2 of DORA; and

(b) the Services provided by PCI Pal under the Agreement are ICT services which do not support a critical or important function of Customer within the meaning of Article 3 of DORA.

1.2 If Customer has determined that the ICT services do support a critical or important function of Customer, the Parties will work in good faith to amend this Addendum to accommodate such determination.

1.3 If and to the extent that any term of this Addendum conflicts with a term the Agreement, the term of this Addendum shall prevail, unless expressly stated otherwise.

2. Definitions

2.1 All capitalised terms not defined in this Addendum shall have the meaning given to them in the Agreement.

2.2 In this Addendum, the following capitalised terms shall have the following meanings, unless the context requires otherwise:

Agreement: means the Master Services Agreement, Services Agreement, Order Form, End User License Agreement or any other similar or analogous terms and conditions governing the supply of the ICT services to Customer agreed between Customer and PCI Pal.

DORA means Regulation (EU) No 2022/2554 on digital operational resilience for the financial sector.

ICT means information and communications technology.

ICT Incident means a single event or a series of linked events unplanned by Customer that compromises the security of network and information systems and that has an adverse impact on of the availability, authenticity, integrity or confidentiality of Customer Data, or on Customer's services.

Regulator means a government, regulatory body or competent authority in any European Union jurisdiction with binding authority to regulate Customer in respect of DORA.

3. Services

3.1 Customer acknowledges that:

(a) the Agreement (including any order form) contains a clear and complete description of the Services provided by PCI Pal; and

(b) for the purpose of Article 30(2)(e) of DORA, the Service Level Agreement referred to in the General Terms and Conditions applies to the Services.

4. Protection of Data

4.1 Customer acknowledges that the data protection and confidentiality provisions of the Agreement, together with the provisions of this Data Privacy and Security Addendum, provide for the protection of the availability, authenticity, integrity and confidentiality of Customer Data, including Personal Data.

5. Permitted Locations

5.1 PCI Pal may:

(a) provide the Services from the United Kingdom and the Amazon Web Services (AWS) location selected by Customer; and

(b) process and/or store Customer Data in the United Kingdom and the AWS location selected by Customer,

(together the Permitted Locations).

5.2 PCI Pal shall notify Customer in advance if there are any changes to the Permitted Locations.

6. Retrieval of Customer Data

6.1 In the event of insolvency, resolution or discontinuation of PCI Pal's business operations, or if the Agreement terminates for any reason, PCI Pal will make reasonable arrangements to enable Customer to access and retrieve (in an easily accessible format) Customer Data in its possession or control [for a period of up to 10 business days.

6.2 Customer acknowledges that this clause 6 applies solely to Customer Data and expressly excludes Aggregated Data and De-identified Data.

7. ICT Incident Assistance

7.1 On Customer's written request, PCI Pal shall provide reasonable assistance to Customer in support of Customer's response and management of an ICT Incident.

8. Cooperation with Regulators

8.1 Upon a Regulator's request, PCI Pal will cooperate, in consultation with PCI Pal's legal counsel and subject to any applicable obligations of confidentiality and its own legal and regulatory responsibilities, with the Regulator, including responding as soon a reasonably practicable to information requests or queries from the Regulator in respect of the Services.

9. Training

9.1 If Customer can reasonably demonstrate that it is necessary to support Customer's compliance with DORA, then PCI Pal shall, following Customer's written request, reasonably participate in Customer's ICT security awareness programme and digital operational resilience training ("Customer Training"), provided that:

(a) Customer shall give PCI Pal no less than thirty (30) days' prior written notice of a request to participate in the Customer Training;

(b) Customer shall only request PCI Pal's participation in Customer Training once in any twelve (12) month period;

(c) the Customer Training shall not to exceed a total of 4 hours in duration;

(d) the Customer Training shall be virtual unless otherwise agreed between the parties;

9.2 PCI Pal shall be entitled to charge Customer, and Customer shall reimburse PCI Pal, for all costs reasonably incurred by PCI Pal in connection with the Customer Training (including PCI Pal's personnel time in participating the Customer Training; and

9.3 Customer shall ensure that any Customer Training is:

(a) reasonable, relevant and subject to the principle of proportionality, having due regard to the nature of the Services; and

(b) requested and conducted in a manner which does not unreasonably disrupt or impede PCI Pal (or its personnel) from providing the Services or otherwise conducting its business.

9.4 Customer agrees that PCI Pal may determine (acting reasonably) which personnel, or categories of personnel, are to participate in such Customer Training.

10. Termination

10.1 In addition to the termination rights in clause 10 of the General Terms and Conditions, Customer may terminate the Agreement with respect to the affected Services only, by giving written notice to PCI Pal in the event:

(a) there are identified circumstances through Customer's monitoring of ICT third-party risk that are deemed capable of altering the performance of the Services, including material changes that affect the arrangement or the situation of PCI Pal; or

(b) there are evidenced weaknesses regarding PCI Pal's ICT risk management, including the manner in which PCI Pal and/or its subcontractors ensure the availability, authenticity, integrity and confidentiality of Customer Data; or

(c) a Regulator notifies Customer that it is no longer in a position to supervise effectively Customer as a result of the conditions of or circumstances related to the Agreement,

(a "Termination Event") and, in each case, solely to the extent PCI Pal is unable to address the cause of such Termination Event within sixty (60) days of being notified in writing by Customer to do so. Customer shall ensure such notice includes all relevant details necessary to enable PCI Pal to understand the cause of the Termination Event.

10.2 For the avoidance of doubt, if Customer does not notify PCI Pal of a Termination Event within 14 days of the such Termination Event arising, Customer's right to terminate shall immediately lapse and Customer shall be deemed to have waived its right to terminate for such Termination Event.*

*Note – right to terminate for significant breach of law, regulation or contractual terms, as required under Art. 28(7)(a), is already covered in the General Terms and Conditions.