DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**Addendum**” or “**DPA**”) is made effective by and between Abnormal Security Corporation (“**Company**”) and the “**Customer**” that is identified in the applicable Company Trial Agreement and/or Master Service Agreement (either, the “**Agreement**”), or alternatively in the applicable Company Order Form, as of the Effective Date of the Agreement and is incorporated by reference therein. All capitalized terms used but not otherwise defined herein have the respective meanings ascribed to them in the Agreement.

Customer has purchased a subscription to the Service pursuant to the Agreement that involves the Processing of Personal Data subject to Data Protection Laws.

This Addendum, together with the Agreement, serves as the binding contract referred to in Article 28 (3) of the GDPR that sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and categories of data subjects as well as the obligations and rights of the Controller.

In the provision of the Service by Company to Customer pursuant to the Agreement, Customer acts as Controller and Company acts as Processor with respect to the Personal Data or as the case maybe, Customer acts as a Processor for its end user customers (as ultimate Controllers), and Company will act as a Sub-Processor acting on the instruction of the Customer on behalf of its end user customers.

The parties agree as follows:

1. **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them herein.

   “**Controller**” has the meaning given to it in the Data Protection Laws and for the purposes of this Addendum means Customer, including when acting on behalf of its own end user customer.

   "**Data Protection Laws**” means: (i) the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the “**Privacy Directive**”) and the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“**GDPR**”); and (ii) to the extent applicable to the Service, any other EU or EU Member State data protection laws with respect to the processing of Personal Data under the Agreement.

   “Data Subject” has the meaning given to it in the Data Protection Laws.

   “**EEA**” means the European Economic Area.

   “**Personal Data**” has the meaning given to it in the Data Protection Laws and for the purpose of this Addendum relates to the personal data Processed by Company on behalf of Customer as described in Section 4.

   “**Personal Data Breach**” has the meaning given to it in the Data Protection Laws and for the purpose of this Addendum relates to the personal data Processed by Company on behalf of

Customer.

"**Processing**" has the meaning given to it in the Data Protection Laws and "process", "processes" and "processed" will be construed accordingly.

"**Processor**" has the meaning given to it in the Data Protection Laws and for the purposes of this Addendum means Company.

"**Standard Contractual Clauses"** means the terms attached to this Addendum as Exhibit 1 and promulgated pursuant to the European Commission's decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to Processors established in third countries which do not ensure an adequate level of data protection.

2. **Compliance with Laws**. Each party will comply with the Data Protection Laws as applicable to it. In particular, Customer will comply with its obligations as Controller (or on behalf of Controller) and Company will comply with its obligations as Processor.

3. **Customer Obligations**. Customer as Controller (or on behalf of the ultimate Controller) undertakes that all instructions for the Processing of Personal Data under the Agreement or this Addendum or as otherwise agreed will comply with the Data Protection Laws, and such instructions will not in any way cause Company to be in breach of any Data Protection Laws. Customer is solely responsible for ensuring the accuracy, quality, and legality of Personal Data Processed by Company including the means by which Customer acquired Personal Data.

4. Data Processing. Company will Process the Personal Data for the sole purpose of providing the Service to Customer. Company will Process the Personal Data in accordance with Customer's instructions as documented in the Agreement and this Addendum for the term of the Agreement. Company will not access, use or otherwise Process such Personal Data, except as necessary to provide the Service.

   Unless prohibited by applicable law, Company will notify Customer if in its opinion, an instruction infringes any EU Member State law to which it is subject, in which case Company will be entitled to suspend performance of such instruction, until Customer confirms in writing that such instruction is valid under EU Member State law. Any additional instructions regarding the manner in which Company Processes the Personal Data will require prior written agreement between Company and Customer.

   Company will not disclose Personal Data to any government, except as necessary to comply with applicable law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If Company receives a binding order from a law enforcement agency for Personal Data, Company will notify Customer of the request it has received so long as Company is not legally prohibited from doing so.

   Company will ensure that individuals with access to or involved in the Processing of Personal Data are subject to appropriate confidentiality obligations and/or are bound by related obligations under Data Protection Laws or other applicable laws.

5. **Transfers of Personal Data Outside of EEA**. Company may process Personal Data in connection with its provision of the Service in countries that have different data protection regulations than the Data Protection Laws (**"Third Countries"**). In such event, subject to the terms of this Addendum, the Standard Contractual Clauses in the form provided in Exhibit 1 will govern the transfer of Personal Data to such Third Countries,

including to Subprocessors in such Third Countries, unless the transfer of Personal Data occurs via an alternative means permitted by the Data Protection Laws, such as the EU-US and Swiss-US Privacy Shield Frameworks.

6. **Technical and organizational measures**. 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, Company will in relation to the Personal Data implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk as further described on Exhibit 2 of the Addendum.

   In assessing the appropriate level of security, Company will take into account in particular the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7. **Data Subjects rights**. Company will assist Customer in responding to Data Subjects' requests exercising their rights under the Data Protection Laws. To that effect, Company will (i) to the extent permitted by applicable law, promptly notify Customer of any request received directly from Data Subjects to access, correct or delete its Personal Data without responding to that request, and (ii) upon written request from Customer, provide Customer with information that Company has available to reasonably assist Customer in fulfilling its obligations to respond to Data Subjects exercising their rights under the Data Protection Laws.

8. **Data Protection Impact Assessments**. If Customer is required under the Data Protection Laws to conduct a Data Protection Impact Assessment, then upon written request from Customer, Company will assist where reasonably possible in the fulfilment of the Customer's obligation as related to its use of the Service, to the extent Customer does not otherwise have access to the relevant information. If required under Data Protection Laws Company will provide reasonable assistance to Customer in the cooperation or prior consultation with the Data Protection Authorities in relation to any applicable Data Protection Impact Assessment.

9. **Audit of Technical and Organizational Measures.** Company will make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Service. To this end, upon written request (not more than once annually) Customer may, at its sole cost and expense, verify Company's compliance with its data protection obligations as specified in this Addendum by: (i) submitting a security assessment questionnaire to Company; and (ii) if Customer is not satisfied with Company's responses to the questionnaire, then Customer may conduct an audit in the form of meetings with Company's information security experts on a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Company's normal business operations and subject to Company's agreement on scope and timing. The Customer may perform the verification described above either itself or by a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon Non-Disclosure Agreement ("**NDA**"). Customer will be responsible for any actions taken by its authorized auditor. All information disclosed by Company under this Section 9 will be deemed Company Confidential Information, and Customer will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Company will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 9 within a mutually agreeable

timeframe.

10. **Breach notification**. If Company becomes aware of a Personal Data Breach that results in unlawful or unauthorized access to, or loss, disclosure, or alteration of the Personal Data, which is likely to cause a risk to the fundamental rights and freedoms of the Data Subjects', then Company will notify the Customer without undue delay after becoming aware of such Personal Data Breach and will cooperate with the Customer and take such reasonable commercial steps as agreed with the Customer to assist in the investigation, mitigation and remediation of such Personal Data Breach. Company will provide all reasonably required support and cooperation necessary to enable Customer to comply with its legal obligations in case of a Personal Data Breach pursuant to Articles 33 and 34 of the GDPR.

11. **Subprocessing**. Customer agrees that Company may engage either Company affiliated companies or third parties providers as sub-Processors under the Agreement and this Addendum ("**Subprocessors**") and hereby authorizes Company to engage such Subprocessors in the provision of the Service. Company will restrict the Processing activities performed by Subprocessors to only what is strictly necessary to provide the Service to Customer pursuant to the Agreement and this Addendum. Company will impose appropriate contractual obligations in writing upon the Subprocessors that are no less protective than this Addendum, and Company will remain responsible for the Subprocessors' compliance with the obligations under this Addendum.

    Company maintains a list of all Subprocessors used by Company in the provision of Service which is set forth on Exhibit 3 to this Addendum. Company may amend the list of Subprocessors by adding or replacing Subprocessors at any time. Customer will be entitled to object to a new Subprocessor by notifying Company in writing the reasons of its objection. Company will work in good faith to address Customer's objections. If Company is unable or unwilling to adequately address Customer's objections to its reasonable satisfaction, then Customer may terminate this Addendum and the Agreement in accordance with Section 4.2 of the Agreement (Termination for Cause).

12. **Return or Deletion of Personal Data**. Company will delete or return, in Customer's discretion and upon Customer's written request, Personal Data within a reasonable period of time following the termination or expiration of the Agreement.

13. **Entire Agreement; Conflict**. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

EXHIBIT 1

Standard Contractual Clauses
(processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: .....

Address:.....

Tel.: ..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: Abnormal Security Corporation

Address: 797 Bryant Street, San Francisco, CA 94107

Tel.:.....;
fax: .....;
e-mail: legal@abnormalsecurity.com

Other information needed to identify the organisation:

.....
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* will have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor will be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial

information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which will be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which will be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a

copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor will be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data

exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer will promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter will be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses will be governed by the law of the Member State in which the data exporter is established

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer will not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it will do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer will remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor will also

provide for a third- party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor will be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 will be governed by the law of the Member State in which the data exporter is established.

4. The data exporter will keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which will be updated at least once a year. The list will be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor will, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or will destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Vito Brandle

Position: Head of Operations and Finance

Address: 797 Bryant Street, San Francisco, CA 94107

Other information necessary in order for the contract to be binding (if any):

Signature…….

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer): As specified in the Addendum.

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
Abnormal Security Corporation provides a cloud-based email fraud detection solution.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Individual users of Data Controller's email system, as well as individuals sending messages to or receiving messages from such user accounts.

Categories of data
The personal data transferred concern the following categories of data (please specify):
First and Last Name
Email address
IP address
Personal Data contained in email message body or attachments

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
N/A

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
Scanning of email contents and metadata for malicious signatures

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

As specified on Exhibit 2 of the Addendum to which these Standard Contractual Clauses are attached.

Exhibit 2
Technical and Organizational Measures

Company has taken and will maintain the appropriate administrative, technical, physical and procedural security measures, for the protection of the Personal Data, including the measures set forth below or otherwise made reasonably available by Company.

Policy Controls:

- Company has established an information security policy.
- A framework of security standards has been developed, which supports the objectives of the security policy.
- Procedures and systems exist for requesting, establishing, issuing, suspending, deleting, and closing user accounts and associated access privileges, e.g. system access is granted based upon position, job function, and manager approval.
- Company prevents unauthorized internal access to customer data by limiting access to only employees who need access to offer and improve the Service
- Multi-Factor Authentication, including biometric fingerprint verification, is required to access Company systems and Customer Data.
- Access to Company offices is controlled via card key access, and is under 24/7 CCTV monitoring.
- No Customer Data is stored on premise.

Collection of Data:

- All email processed through the Service is stored for 180 days and then automatically deleted at the end of the 180-day period.
- All Customer Data is encrypted at rest using multi-factor encryption with a per-file key and AES-256 block cipher, with keys managed by AWS Key Management Service

Backup Copies

- Procedures for backup and retention of data and programs have been documented and implemented.
- Data and programs are backed up regularly and replicated between geographically diverse data centers.

Computers and Access Terminals

- New employees are required to sign a non-disclosure agreement relating to proprietary software and confidentiality of information relating to customers.
- New employees are required to acknowledge receipt of Company's Information Security Policy.
- Access to the production environment is authorized by the Chief Technology Officer and is based on business need. A two-factor authenticated VPN is utilized for any access outside Company offices
- Customer Data is processed in memory and is not available for printing. All print services are disabled by default on all production servers

Access Controls

- All Data Importer employees and contractors are provided with unique userIDs
- Access is only granted to employees whose role requires it
- Access is disabled upon role reassignment or termination.
- Access is revoked on termination.

Security while transferring and processing

- Isolated network environment using Amazon VPC
- Default blocked firewall policies
- Limited number of integration-related endpoints are accessible via public internet. Majority of services protected by firewalls as private endpoints.
- Public endpoints utilize Application Load Balancers, and are resilient to dynamic changes in query load/throughput
- Data in transit encrypted using TLS 1.2 sessions with a 2048-bit RSA asymmetric key
- HTTPS required for all web traffic
- Encrypted connectors for databases using SSL

EXHIBIT 3

Subprocessors

As stated in the Agreement