DATA PROTECTION AND INFORMATION SECURITY

ADDENDUM

WHEREAS, Company and Service Provider (collectively, the "**Parties**") have an existing commercial relationship in the context of which Service Provider provides services to Company; and

WHEREAS, Company is subject to a number of data protection and information security requirements, in particular in the context of being a Financial Institution, and is required by law to impose substantially similar standards on its service providers.

Service Provider covenants and agrees that it will comply as follows:

1. DEFINITIONS. Any capitalized term used in this Data Protection and Information Security Addendum (this "***Addendum***") shall have the respective meanings set forth in this Section 1:

"***Affiliate***" means as to any natural or legal person, any other person that is in Control of, or is Controlled by, or is under common Control with said person;

"***Applicable Laws***" means all applicable laws, legislation, guidelines, directives, rules, regulations or other similar instruments enacted by any Regulatory Authority or by common law to the extent applicable to a Party, to the business of that Party or to the obligations of that Party in relation to the performance of the Services, including the Data Protection Legislation;

"***Company***" means the entity that is receiving services from Service Provider and that has signed this Addendum;

"***Company Data***" means any data (including, without limitation, Personal Information and meta data) contributed or made available by or on behalf of Company or any of its Affiliates to Service Provider or Service Provider's Affiliates, including any modification, adaption, enhancement or derivation of any such Company Data;

"***Control***" means the power, directly or indirectly, either to: (a) vote twenty-five percent (25%) or more of the securities having ordinary voting power for the election of directors (or persons performing similar functions); or (b) direct or cause the direction of the management and policies of such person, whether by contract or otherwise;

"***Data Protection Legislation***" means all Applicable Laws which relate to the Processing of Personal Information, including but not limited to California Consumer Privacy Act (CCPA), applicable State Attorney Generals' data breach reporting requirements, Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation of the European Union (GDPR), etc.;

"***Data Subject***" means any individual (including employees, consumers and household within the meaning of CCPA) who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity;

"Financial Institution" shall have the meaning of Financial Institution as defined within the Gramm-Leach-Bliley Act (GLBA);

"***Malware***" means any "backdoor", "logic bomb", "Trojan horse", "worm", "ransomware", "virus", "rootkit", or other computer software or hardware intended or designed to:

(i) disable, damage, erase, disrupt or impair the normal operation of; or

(ii) provide unauthorized access to or modification of computer systems or any software or information stored on those computer systems;

"***Process***" *or* "***Processing***" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, including but not limited to collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"***Personal Information***" means any information relating to an identified or identifiable natural person, or a household: an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"***Personnel***" means Service Providers' employees, contractors, and all other individual Processing or having access to Company Data;

"*Regulatory Authority*" means any national, regional, state, or local government or governmental agency or subdivision thereof, any agency, authority, instrumentality, regulatory body, court, central bank or other entity exercising executive, legislative, judicial, taxing, regulatory or administrative functions, including State Attorney Generals and the Federal Trade Commission;

"***Services***" mean the service(s) provided by the Service Provider to the Company;

Service Provider" means the entity or person providing Services to Company that has signed this Addendum;

"***Security Event***" means any occurrence related to assets or the environment indicating a possible compromise of policies or failure of controls, or an unmapped situation that can impact security; and

"***Sub-processor(s)***" means a third-party subcontractor, other than a Service Provider Affiliate, engaged by Service Provider and which may process Company Data as set forth in Sections 2.8 and 2.9.

2. SAFEGUARDING DATA

2.1. All Company Data provided directly or indirectly to Service Provider shall be and shall remain the sole property of Company.

2.2. Unless required by Applicable Law to retain a copy of Company Data, Service Provider shall, as soon as reasonably practicable, return to Company or, if Company so elects, securely destroy (and, upon written notice from Company, certify in writing that Service Provider has fully complied with this Section 2.2), all Company Data upon any of the following:

(a) Company's written request;

(b) termination or cessation of the Services; or

(c) when Company Data is no longer required by Service Provider for the provision of the Services.

2.3. If no explicit instruction has been provided by Company within 6 months following the termination or cessation of the Services, Service Provider shall securely destroy all Company Data.

2.4. Service Provider shall ensure that where Company Data, including Company Data stored on electronic devices, is destroyed under Sections 2.2 and 2.3 hereof, such destruction takes place in a secure manner such that Company Data is not recoverable.

2.5. Service Provider and its Personnel shall comply at all times with all applicable Data Protection Legislation when Processing Company Data.

2.6. Except as permitted under any agreement between the Parties and this Addendum, Service Provider agrees and certifies that it shall not retain or use any Company Data for any purpose other than provision of the Services and shall not disclose Company Data to any third party. Service Provider shall not exploit, use, or disclose any Company Data for a commercial purpose outside of the direct business relationship with Company, including, without limitation, by selling Company Data, generating or deriving other information from Company Data, other than in connection with provision of the Services.

2.7. When Processing Company Data, Service Provider shall:

(a) Process the Company Data strictly in accordance with the documented instructions from Company (which shall include the terms of any agreement between the Parties) unless specifically required to Process the Company Data for other necessary purposes by Applicable Law. Where such a requirement is placed on Service Provider, it shall provide prior notice to Company unless Applicable Law prohibits the giving of such notice;

(b) promptly carry out any request from Company requiring Service Provider to amend, transfer, or otherwise Process Company Data or any part of the Company Data;

(c) ensure that Company Data is accessed only by those Service Provider Personnel that require access for the purpose of provision of the Services and that all such Personnel have committed themselves to appropriate confidentiality obligations when Processing Company Data;

(d) conduct mandatory data protection (including confidentiality and the handling and protection of Personal Information) training for all Personnel, on a regular basis and at least annually;

(e) not Process Company Data in a public place or any location where such Company Data may be viewed by others, including, without limitation, in waiting areas, on public transport, or across unencrypted public networks;

(f) promptly notify Company of any request from a Data Subject to exercise his or her rights under Data Protection Legislation and of any other complaint, allegation, or request (including, without limitation, by a Data Subject or any regulatory or other competent authority) relating to Company's obligations under Data Protection Legislation;

(g) promptly provide assistance and information to Company as Company may reasonably request in relation to any request, complaint or allegation envisaged under Section 2.7(f) (each an "**Event**") and take whatever action is reasonably necessary to minimize the impact of the Event and/or prevent the Event from recurring, as the case may be, at no additional cost to Company;

(h) provide reasonable assistance to Company to conduct privacy impact assessments (and any related consultations with Regulatory Authorities) to comply with Company's obligations under applicable Data Protection Legislation;

(i) implement appropriate technical and organizational measures to safeguard Company Data against unauthorized or unlawful Processing (including, without limitation, theft, unauthorized access, use or disclosure), and against accidental loss or destruction of, or damage to Company Data; and

(j) provide any information as may be reasonably requested by Company regarding what steps Service Provider takes to comply with its obligations under this Addendum and allow Company to audit that compliance (either itself or by using an auditor nominated by Company). Service Provider shall allow for and contribute to audits at no cost for Company, insofar as such audits are performed no more than once a year, or unless such audits are required by a Regulatory Authority or a legal obligation Company or Service Provider is subject to, or arise following non-compliance with the terms of this Addendum. Service Provider shall bear all costs in connection with remediating any non-compliance identified during such audits.

2.8. Service Provider shall ensure that all Service Provider Affiliates and Sub-processors Processing Company Data are subject to prior and continuous due diligence, as well as required by written agreement to abide by the same or higher level of data protection and security, and subject to the purpose limitations as Service Provider under this Addendum.

2.9. Service Provider shall provide a prior written notice to Company no later than 2 (two) weeks before appointing a new Sub-processor or a Service Provider Affiliate to Process Company Data, thereby giving Company the opportunity to object to such changes. In relation to Sub-processors:

(a) An up-to-date list as at the effective date of this Addendum including all Sub-processors and Service Provider Affiliates who are (or will be) Processing Company Data is provided in Annex B; and

(b) Company shall have the right to require at any point an up-to-date list of all Sub-processors and Service Provider Affiliates who are Processing Company Data for as long as Service Provider is Processing any Company Data.

2.10. Company may request that Service Provider audit a Sub-processor or provide confirmation that such an audit has occurred (or, where available, obtain or assist Company in obtaining a third-party audit report concerning the Sub-processor's operations) to verify compliance with such obligations. Company will also be entitled, upon written request, to receive copies of the relevant data protection and security terms of Service Provider's agreement with any Sub-processors and Service Provider Affiliates that may process Company Data.

2.11. Where Service Provider Affiliates or Sub-processors fail to fulfil their data protection and security obligations in compliance with the terms of this Addendum and applicable Data Protection Legislation, Service Provider shall remain fully liable to Company for the performance of those Service Provider Affiliates' or Sub-processors' obligations.

2.12. Service Provider shall defend, indemnify and hold harmless Company and its Affiliates from and against all costs, expenses (including legal expenses), damages, loss, liabilities, demands, claims, actions or proceedings, which Company may incur arising out of any breach by Service Provider of any of its obligations under this Addendum.

3. INFORMATION SECURITY

3.1. Service Provider shall establish, implement, and maintain documented security processes and plans which shall ensure the confidentiality and security of the Company Data (and allow Company to meet its own respective relevant obligations under Data Protection Legislation) in accordance with the requirements set out in this Addendum (the "**Security Plan**").

3.2. Without prejudice to any other obligations of Service Provider under this Addendum, Service Provider shall ensure that at all times it is operating in accordance with the terms of the Security Plan.

3.3. Service Provider will provide upon request by Company copies of the Security Plan or equivalent Company-facing security documents and any other documentation evidencing Service Provider's compliance with its obligations under this Addendum (the "**Compliance Documentation**"). Where Company reasonably believes that the Compliance Documentation does not demonstrate how Service Provider meets these requirements on data protection and security

policies and procedures, Company will detail this in writing and the Parties will work together in good faith to update the Compliance Documentation to address the issues identified by Company.

3.4. In the provision of the Services, Service Provider will adopt and use good development and coding practices and adhere to any other industry standards specified in this Addendum and any addenda. Service Provider will ensure that any application code or other materials developed for Company are sufficiently tested and assured so as to ensure that no Malware is introduced into Company's systems, products, services, software, websites, information or otherwise.

3.5. Service Provider shall perform security tests of its networks and systems ("**Security Tests**") at least annually in a manner to ensure Service Provider is operating in accordance with the Security Plan. Upon request, Service Provider will promptly share the results of Security Tests with Company.

3.6. If Company reasonably considers that controls identified or tested by the Security Tests:

(a) are insufficient to ensure the integrity and security of the Company Data; or

(b) fail to meet the requirements of any regulatory authority or other competent authority applicable to Company;

then Company may request Service Provider to remedy such insufficiency or failure and Service Provider, at its own cost, shall, as soon as is reasonably practicable, take steps to do so. Where such steps affect Service Provider's Affiliates, suppliers or sub-contractors, Service Provider shall ensure that the same steps are also implemented by those parties.

3.7. Service Provider shall also allow for and contribute to audits and other types of assessments, as might be required by Company to periodically evaluate Service Provider's security controls and their continued adequacy.

3.8. Service Provider shall notify Company in writing immediately (and in any event within 24 hours) if:

(a) it becomes aware that any Company Data has been corrupted or rendered unusable using the template notice at Annex C of this Addendum;

(b) it becomes aware of a Security Event, or any suspected or actual security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to or non-availability of access to Company Data using the template notice at Annex C of this Addendum;

(c) it becomes aware of a breach of any of its obligations under this Addendum or of any event requiring disclosure by Company (or itself) of a Security Event to a Regulatory Authority or the Company's customers;

3.9. Service Provider shall at its own cost promptly implement whatever actions or remedial measures are necessary to minimize the impact of any event envisaged under clause 3.8 and to prevent such events recurring (including, without limitation, any action reasonably requested by Company). Service Provider shall also promptly provide Company with evidence of the implementation of such remedial measures, and shall provide assistance to Company in relation to communication with Regulatory Authorities and Data Subjects concerned, as might be required by Data Protection Legislation.

4. INFORMATION SECURITY AND TECHNICAL REQUIREMENTS

4.1. Service Provider will ensure that the Security Plan requires, and Service Provider will implement and maintain:

(a) up to date anti-virus software;

(b) a patch management process, which ensures patches are appropriately tested and promptly deployed to rectify security vulnerabilities in a reasonable timeframe;

(c) vulnerability management processes that includes mechanisms to accurately and expeditiously identify vulnerabilities, implement appropriate fixes to remediate identified vulnerabilities and verify that those have been fixed;

(d) access management processes and procedures to ensure that access to the Company Data under its control is restricted to those with a business need. Access shall be assigned using unique login credentials to ensure accountability is maintained; access shall be monitored and logged. Login credentials must be stored securely;

(e) two-factor authentication for those of its Personnel who work remotely and for those with administrative privileges upon systems used to provide the Services;

(f) conduct mandatory information security training for all Personnel, on regular basis or at least annually;

(g) mechanisms (including but not limited to data loss prevention) to prevent the unauthorized removal or disclosure of Company Data from Service Provider's networks via technologies such as removable media, the internet, email or instant messaging services;

(h) encryption technologies to protect the Company Data during transmission and storage and where appropriate, the pseudonymization of Company Data;

(i) encryption technologies upon portable devices such as laptops, PDAs and smartphones;

(j) physical and logical controls to mitigate the risk of unauthorized intrusion into Service Provider's premises, networks and systems;

(k) systems and software development processes to ensure that no Malware is introduced into systems, software, websites or other media used to supply any of the Services;

(l) separate environments between test and production systems and will ensure that no production data of Company is used in test systems;

(m) processes to ensure that changes to the premises, networks, systems, software, information, websites and other media used to supply the Services are appropriately tested and implemented to limit the potential for any adverse impact on the supply of the Services (including, without limitation, any breach of this Addendum by Service Provider);

(n) processes to continually monitor its networks and systems for potential or actual Security Events;

(o) measures to restore the availability and access to Company Data in a timely manner in the event of a physical or technical incident (including, without limitation, measures relating to business continuity and disaster recovery);

(p) and measures to ensure the ongoing confidentiality, integrity, availability and resilience of Service Provider's systems and services; and

(q) if Service Provider processes cardholder data, Service Provider shall ensure that all systems used by Service Provider to store or otherwise process cardholder data are Payment Card Industry Data Security Standard (PCI DSS) certified and audited on an annual basis.

4.2. Service Provider shall ensure that the processes it employs in the provision of the Services are designed to prevent conflicts of interest, fraud or error (including, without limitation, by invoking appropriate segregation of duties between Service Provider's Personnel).

5. GENERAL TERMS

5.1. The terms of this Addendum (including Annexes A, B, and C that are incorporated by reference and form an integral part of this Addendum) shall supersede all prior agreements, oral or written, by the Parties with respect to the subject matter covered herein.

5.2. This Addendum shall be effective on the last signature date set forth below.

[REMAINDER OF PAGE LEFT BLANK INTENTIONALLY]

ANNEX A

DETAILS OF PERSONAL INFORMATION PROCESSING

Subject Matter, Nature, and Purpose of the Processing

……

……

Duration of the Processing

……

Retention Period of Personal Information

……

Categories of Personal Information

……

……

……

……

……

Data Subjects to whom Personal Information Relates

……

……

……

……

ANNEX B

LIST OF SUB-PROCESSORS AND SERVICE PROVIDER AFFILIATES PROCESSING COMPANY DATA

#	Legal Name	Country of establishment	Description of Processing purposes
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

ANNEX C

BREACH NOTIFICATION TEMPLATE

Security Event and security breach notification must be made electronically and shall contain at least the following minimum details:

Reporting made by	
Date of incident	
Date of identification	
Explanation of any delay	(Please provide details of any delays in identifying the breach and/or reporting)
Description of the breach	(Please describe what has happened)
Categories of Personal Information impacted	(What Personal Information has been compromised)
Number of affected data subjects	(Please provide the exact or estimated number of individuals that will be affected by the breach)
Number of affected records	(Please provide the exact or estimated number of the records affected)
Likely consequences	(Please describe the likely consequences e.g. risk of media coverage, identity theft, financial loss, etc.)
Mitigating Measures	(Please describe what action has taken place to address the breach and mitigate its effects)
Notification	(Specify if the incident has been disclosed to media, regulator, directly to data controller or any other party)

COMPANY:	**SERVICE PROVIDER:**
_____	_____
SIGNATURE	SIGNATURE
_____	_____
NAME	NAME
_____	_____
TITLE	TITLE
_____	_____
COMPANY	COMPANY
_____	_____
DATE	DATE