PRIVACY AND SECURITY ADDENDUM

TO THE MASTER SERVICES AGREEMENT

This Privacy and Security Addendum (the **"Addendum"**) to the Master Services Agreement (the **"Agreement"**) by and between **MX TECHNOLOGIES, INC.** a Delaware corporation, having its principal place of business at 3401 N Thanksgiving Way, Suite 500, Lehi, Utah 84043 (**"MX"**), and (**"Client"**) is entered into and effective as of the last date signed below (the **"Effective Date"**). MX and Client being individually a **"Party"** and collectively the **"Parties"**.

In order for MX to provide Client with modern data connectivity, to protect the privacy and security of Client's Users and their User Data, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties agree to the addition of the following terms to the Agreement, solely and expressly as stated herein, all terms of the Agreement remaining in full force and effect and this Addendum governing in the case of any inconsistencies between the Agreement and the Addendum but in all cases adding to and not replacing any similar terms in the Agreement:

1. DEFINITIONS

1.1 "**Third Party Data Provider**" means any third party entity, including financial institutions, which provides User Data or other data to MX for use in the Services.

2. SERVICE

2.1 Provision of Service. Client shall provide to MX such information regarding Client's data requirements and services as MX may reasonably require to facilitate its provision of the Service. MX may disclose any such information to its Third Party Data Providers where reasonably necessary for the provision of the Service. MX has the right to monitor any and all use of the Service without notice to Client or its personnel and may provide any information obtained through such monitoring to its Third Party Data Providers. Additionally, MX may, from any location in which it does business, store or process business contact information of Client and its personnel.

3. MUTUAL RIGHTS AND RESPONSIBILITIES

3.1 Client Responsibilities. Client shall not charge User any fees that identify, or are identifiable to, MX, any Third Party Data Provider, or to User's use of the Service. If Client both accesses User Data and initiates payments, it must obtain separate and distinct consents from User for these separate activities. With respect to consents required to be obtained from Users hereunder, Client must have and maintain such systems and procedures as may be reasonably necessary or otherwise required by MX to actively track, monitor and document such User consent and any revocation thereof.

3.2 User Access. The EULA, as amended and supplemented by MX from time to time, shall: (i) be prominent, written, accurate, and easy-to-understand by a reasonable consumer; (ii) accurately set forth what data, including all compilations, aggregations, and combinations of the same, is collected, how collected data will be used, and how collected data will be accessed, shared, exchanged, or sold; (iii) provide clear and conspicuous disclosures to all Users and prospective Users sufficient to comply with applicable law regarding the collection, use, and sharing described; (iv) identify or disclose to each User any and all categories of third parties to whom User Data may be provided or who may use, receive, store, or process the same; (v) inform Users of their rights with respect to User Data including, without limitation, the right to terminate access and require deletion; (vi) inform Users that the User Data does not represent an official record of the User's account with any relevant financial institution; (vii) state that Client is acting independently, and not on behalf of any third party, in providing its application or services; (viii) describe how the User Data will be protected in the event that Client ceases operating as a going concern or otherwise ceases to make available the Client application to Users, describing how User Data in Client's possession or control will be safeguarded, deleted, and purged in such circumstances; (ix) provide MX and its' Third Party Service Providers the same liability restrictions and limitations and warranty disclaimers to which Client is entitled under its agreement with Users, to include but not be limited to (a) exclusion of all implied warranties, including without limitation for merchantability and fitness for a particular purpose, (b) exclusion of consequential, special, indirect, incidental, punitive, exemplary and tort damages in connection with the Service and User Data made available through the Services, and (c) inclusion of a quantifiable limitation of liability for direct and indirect damages in connection with the Services as further set forth herein and in the Agreement; (x) release MX and its Third Party Service Providers of all liability and obligation related to any delays, inaccuracies or incomplete Service caused by the failure of Client or its Third-Party Service Providers to properly or timely meet their obligations or requirements; and (xi) be agreed to by Users prior to access to the Service or restrict such access until after User consent to the EULA has expressly occurred.

3.3 Access and Use Rights.

3.3.1 Client shall only request User Data through the Service that is expressly consented to by the User. Client may only host and/or store User Data from locations within the United States unless otherwise approved in advance and in writing by MX, and where applicable, by an applicable Third Party Data Provider. With respect to User Data made available through the Service, Client will not, nor shall it attempt to: (i) use, disclose or process the User Data to target market products or services to Users that are directly competitive to those offered by any Third Party Data Provider, by using such Users' status as a customer of a Third Party Data Provider as criteria; (ii) use any APR, APY, credit limit or similar data included within the User Data to ascertain confidential or proprietary information of any Third Party Data Provider, including, without limitation, credit models, credit algorithms, and other business processes and calculations not available to the public; or (iii) where the User Data is provided in a deidentified form, re-identify or attempt to re-identify such User Data.

3.3.2 Client shall not use or disclose any User Data accessed through the Service, except for the purposes of: (i) providing the User Data directly to the applicable User; and (ii) complying with applicable law or mandatory requests of a government or regulatory body. Client must provide Users the ability to unlink such User Data from any Client application or service. In the event that any User unlinks (or requests the unlinking of) its User Data from any Client application or service, Client will promptly notify MX of the same. Upon request by User, Client shall promptly and permanently delete all User Data in Client's possession or control, and promptly notify MX of the same.

3.3.3 Client acknowledges and agrees that MX is neither a "consumer reporting agency" nor a "furnisher" of information to consumer reporting agencies under the Fair Credit Reporting Act 15 U.S.C. §1681 ("FCRA") and Client shall not request or demand of MX any required compliance with the FCRA. Client further acknowledges that the User Data is not a "consumer report" under the FCRA and cannot be used as or in such. Client represents and warrants that it will not, and will not permit or enable any third-party to, use the Service or the User Data as, or as part of, or in preparation of a "consumer report" as that term is defined in the FCRA or otherwise use the Services or the User Data such that they would be deemed "consumer reports" under the FCRA.

3.3.4 MX shall provide Client a list of Internet Protocol addresses ("IP Addresses") from which MX may access User Data from Client on behalf of Users. MX may update the provided list from time to time. Client shall not block or otherwise obstruct MX from accessing User Data from Client using the IP Addresses in the provided list.

3.4 Suspension Rights. MX shall have the right to suspend Client's access, in whole or in part, to the Service and any User Data for the following reason(s): (i) MX's good-faith belief that Client is acting in an unauthorized manner with respect to its access to the Service or any User Data; (ii) a User requests that MX or any Third Party Data Provider no longer permit Client to access its User Data (such suspension will only be applied to the requesting User); (iii) MX's good-faith belief that there is a material risk to the security or integrity of the Service, the User Data, or any systems of MX or Client; or (iv) that suspending access is reasonably necessary to prevent harm to the business or reputation of MX, any Third Party Data Provider, and/or their respective customers. Upon any notice of suspension, Client shall immediately cease any attempt to access the Service or any User Data, including by screen scraping. Unless prohibited by applicable law, MX will provide Client with prompt (and, where reasonably practicable, advance) notice of the suspension, including, if permitted, a description of the scope of the suspension and the reasons for the suspension. The Parties will work together to remediate the reason for any suspension, with MX having the final authority as to the duration and extent of any suspension. At any point during such suspension, upon notice to Client, MX will have the right to terminate this Agreement and Client's access to the Service and User Data by providing Client notice (which will be at least thirty (30) days' notice, where reasonably practicable). Additionally, if Client's account is thirty (30) days or more overdue, except for charges then under reasonable and good faith dispute, then, following five (5) business days' written notice and opportunity to cure, which notice may be provided via email, in addition to any of its other rights or remedies, MX reserves the right to suspend Client's access to the Service until such amounts are paid in full.

3.5 Security.

3.5.1 Security Awareness. Each Party shall ensure that all of its employees and other personnel are familiar with and have received adequate training with respect to its written information security program and their obligations thereunder.

3.5.2 Assurance Reports. At least annually during the Term, Client shall have a certified independent public accounting firm or another independent, certified, industry-recognized third party: (i) conduct a review or assessment and provide a full attestation, review, or report under SOC 2 Type II of all Client systems and operational controls used by Client to access the Service or access, store, or process any User Data; and (ii) conduct and provide a full report of an independent network and application penetration test. Client shall provide copies of all such reports and the results of any testing to MX, together with such other independent third party audit reports as MX may request, which may include, without limitation: SOC 1, Type II reports; SOC 2, Type II reports; ISAE 3402 reports; or any similar audit reports. All reports and results provided to MX hereunder shall be treated as confidential by MX, except that MX may provide the same to any Third Party Data Provider, provided such Third Party Data Provider is bound by obligations of confidentiality.

3.5.3 Information Security. In connection with all Nonpublic Personal Information, the Parties shall establish and maintain a written information security program that is consistent with generally accepted industry standards, including "Generally Accepted Principles and Practices for Securing Information and Technology Systems" (GAPPs) issued by the National Institute of Standards & Technology and the ISO 27000, including safeguards against the disclosure, destruction, loss, or alteration of User Data. At a minimum, each Party's written information security program will be designed to: (i) ensure the security, integrity, and confidentiality of all User Data; (ii) detect patterns, practices, or specific activity that indicates the possible existence of identity theft or other threats or hazards to the security or integrity of User Data; (iii) protect against unauthorized access, interception, use, or disclosure of User Data; (iv) ensure that all transfers of User Data are accomplished in a secure and confidential manner and in compliance with best practices in the financial services industry and latest industry encryption standards; and (v) ensure the proper disposal of User Data, where applicable. Each Party shall maintain on all of its systems on which User Data is accessed, stored, used or otherwise processed (i) real-time intrusion detection systems, and (ii) up-to-date and reputable antivirus software and/or other commensurate anti-malware tools and applications. Without limiting a Party's obligations under Section 3.5.4 (Security Incident), each Party shall promptly report to the other Party any patterns, practices, or specific activity detected with respect to Client's systems that may indicate the possible existence of identity theft and shall take appropriate steps to prevent or mitigate the same.

3.5.4 Security Incident. Each Party will promptly (and in any event, within 48 hours of discovery) notify the other Party of a Security Incident, as defined below. Such notice shall include a detailed description of the Security Incident, and any other information the other Party may reasonably request concerning the Security Incident, including, without limitation, the number of records, types of information, and number of Users impacted by the Security Incident, the known or suspected causes of the Security Incident, any actual or anticipated impact on the other Party or its customers, and remediation plans. Each Party will maintain records of all actual or suspected Security Incidents consistent with security best practices in the financial services industry and will make such reports available to the other Party upon request. Each Party agrees to promptly and at its own cost and expense investigate and take all reasonable measures necessary or advisable to mitigate the effects of and remedy any Security Incident, including, where appropriate and without limitation, providing credit monitoring services and related call center or similar support activities to impacted parties. Each Party further agrees to fully cooperate with and provide all reasonable assistance to the other Party in regard to its investigation of any Security Incident. Without limiting the generality of the foregoing, each Party shall cooperate with the other Party in determining its legal obligations with respect to notification of Users, regulators, and/or law enforcement, if any, and each Party agrees to provide to the other any documentation in such Party's possession which is necessary for the other to issue required or advisable notifications or communications. Unless otherwise required by applicable law, neither Party will (and will ensure that each of its representatives and agents do not) inform any unrelated third party of any Security Incident without first obtaining the other Party's prior written consent. Where any disclosure of a Security Incident by a Party is required by applicable law, such Party will use its commercially reasonable efforts to obtain the other Party's approval regarding such disclosure. For purposes of this Agreement, "Security Incident" shall mean any breach, incident or other event that compromises (or would be reasonably likely to result in a compromise of) the security, integrity or confidentiality of the User Data or other Party's Confidential Information, or that otherwise results in (or that would be reasonably likely to result in) the unauthorized access, use, disclosure or loss of User Data or the other Party's Confidential Information. Each Party shall notify the other Party within 48 hours of receiving any complaint alleging the improper or unauthorized access or use of User Data. Client shall be responsible for managing all disputes or issues raised by a User with respect to any Client application; provided, however, that MX may, at its option, engage directly with any User with respect to issues or complaints relating to the access or use of User Data, and may take all steps deemed necessary by MX to resolve such issues or complaints, including, without limitation, terminating access to the Service and/or to any User Data. Notwithstanding the foregoing, Client acknowledges and agrees that Client shall remain responsible for any unauthorized access or use of User Data once it has been accessed through the Service, is in the possession or control of Client, or thereafter. Each Party shall reasonably cooperate with any investigation undertaken by the other Party with respect to any act of dishonesty, breach of trust, or violation of law by any of its employees or personnel with respect to the Service or the User Data.

4. PROPRIETARY RIGHTS

4.1 Client Intellectual Property. Client hereby grants to MX a worldwide, non-exclusive, revocable, limited license during the Term of this Agreement, to use the trademarks, marks, logos and trade names ("Marks") of Client, and to sublicense the same to Third Party Data Providers, for the sole purpose of providing the Service and identifying Client to Users as a recipient of User Data and obtaining consent from such Users. MX shall use the Marks and shall require that any Third Party Data Provider use the Marks in compliance with any reasonable trademark use policies Client may promulgate from time to time and provide to MX in writing.

5. WARRANTIES AND DISCLAIMERS

5.1 Additional Disclaimer. MX, ON BEHALF OF ITSELF AND ALL THIRD PARTY DATA PROVIDERS, EXPRESSLY DISCLAIMS ANY TYPE OF REPRESENTATION OR WARRANTY REGARDING THE AVAILABILITY OR RESPONSE TIME OF THE SERVICE OR USER DATA OR THAT ACCESS TO THE SERVICE OR USER DATA WILL BE UNINTERRUPTED OR ERROR-FREE AND, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, EXPRESSLY DISCLAIMS THE ACCURACY, COMPLETENESS AND CURRENCY OF ALL USER DATA.

6. ATTESTATIONS

6.1 Attestation Rights. During the Term of the Agreement and for one year thereafter, Client will, upon reasonable advance written notice from MX, provide to MX or any Third Party Data Provider a written attestation of Client's compliance with the terms and conditions of this Agreement governing the processing of User Data, the prompt reporting of all Security Incidents, and obligation to refrain from re-identifying or attempting to re-identify any aggregated or de-identified User Data (an "Attestation"). Client agrees to reasonably cooperate with and shall promptly take all actions necessary to remediate any material deficiencies and non-compliance discovered as a result of any Attestation. All Attestations shall be considered Client's Confidential Information; provided, however, that MX may disclose copies of the same to any Third Party Data Provider at MX's sole discretion. Nothing in this Section 6 is or shall be construed as limiting the rights of any governmental or regulatory authority to conduct audits or investigations. Client acknowledges that MX intends to fully comply with all governmental and regulatory authorities, including with respect to any law enforcement or judicial investigations, and that in connection with the foregoing, MX may disclose the identity of, and any information transmitted or received by, persons accessing the Service. Client agrees to fully cooperate with any audits or investigations conducted by a governmental or regulatory authority pursuant to applicable law.

7. GENERAL PROVISIONS

7.1 Insurance. Each Party shall obtain and maintain at its own expense, throughout the Term and for a period of two years thereafter, (a) sufficient insurance coverage for its business, its activities hereunder, and any reasonably anticipated risks; and (b) without limiting the foregoing, (1) Commercial General Liability Insurance, (2) Crime Insurance (Employee Dishonesty), and (3) Cyber Risk/Data Security and Privacy Liability Insurance covering claims (and any associated costs and damages, including data breach investigation, data breach notification and credit monitoring costs) arising from: (i) breaches of computer systems and data security, (ii) violations of any privacy right, (iii) breaches of data privacy and data security laws and regulations, (iv) breach of PCI-DSS or any similar rules promulgated by the PCI Council, and (v) data theft, damage, destruction, or corruption, including unauthorized access, unauthorized use, identity theft, theft of personally identifiable information, and transmission of a computer virus or other type of malicious code.

7.2 Advertising and Publicity. Client may not issue any media release or make any public announcement or public disclosure relating to or referencing any Third Party Data Provider or the provision of User Data by or through such Third Party Data Provider in connection with this Agreement, without the prior written consent of such Third Party Data Provider.

7.3 Third Party Beneficiaries. Third Party Data Providers are intended third party beneficiaries of those provisions specifically protective of those parties. Otherwise, no person or entity not a party to this Agreement will be deemed to be a third party beneficiary of this Agreement or any provision hereof.

IN WITNESS WHEREOF, the Parties hereto have caused their respective authorized representatives to execute this Agreement on the dates set forth below to be effective as of the Effective Date.

MX TECHNOLOGIES, INC.

By:	______________________________	By:	______________________________
Name:	______________________________	Name:	______________________________
Title:	______________________________	Title:	______________________________
Date:	______________________________	Date:	______________________________