TransArmor® Solution Services Addendum

This TransArmor® Solution Services Addendum ("Addendum") is made and entered into by and between First Data Merchant Services Corporation ("Processor") and _____ ("Client or "you") as of _____, to amend and supplement that certain Merchant Processing Application and Agreement between the parties dated _____ (the "Agreement").

The terms and conditions set forth in this Addendum govern the provision of the TransArmor Solution Services ("TransArmor Services" or "Services"). The TransArmor Services are provided to you by Processor and not Bank, and Bank is not liable to you in any way with respect to such services. For the purposes of this section, the words "we," "our" and "us" refer only to the Processor and not the Bank.

The TransArmor Services provided, transactions processed and other matters contemplated under this Addendum are subject to the rest of your Agreement, as applicable, except to the extent the terms of this Addendum directly conflict with another provision of the Agreement, in which case the terms of this Addendum will control.

In consideration of the mutual covenants herein contained, and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged**,** Processor and Client hereby agree as follows:

1. TransArmor Service. The following is a description of the TransArmor Services available to you, subject to the terms of this Addendum. The TransArmor Services are available during a calendar year only if you have less than one (1) million Visa Card transactions and less than one (1) million MasterCard Card transactions in such year.

(a) Data Protection that provides encryption of card holder data at your payment environment and replaces the data with a token or randomly generated number;

(b) POS software monitor ("POS Software Monitor") that provides a suite of monitoring, scanning and anti-virus software services to help protect point of sale computer systems;

(c) PCI Rapid Comply ("PCI Rapid Comply Service") which provides access to on-line PCI DSS Self-Assessment Questionnaires (SAQ) to validate PCI data standards. If an internet scan is required to complete the SAQ, you will have access to such scanning services;

(d) POS hardware monitor ("POS Hardware Monitor") which is a tool to assist in detecting physical terminal tampering and substitution, in accordance with additional terms and conditions provided to you upon downloading the POS Hardware Monitor; and

(e) Liability warranty under which Processor will provide a waiver of your liability for card association expenses in the event of a security breach up to $100,000 per MID, and up to $500,000 aggregate for all MID's, subject to terms and conditions set forth herein.

2. Fees.

(a) **TransArmor Solution Fee**. The fee for access to the TransArmor Services will be $5.00 per month ("TransArmor Solution Fee"). The TransArmor Solution Fee will also replace any transaction fees for current TransArmor functionality. You understand and agree that the payment of your fees does not affect your compliance responsibilities and obligations associated with your Merchant Account. We may increase your fees for the Services as provided in your Agreement.

(b) **Non-Compliance Fee**. The fee for your failure to provide us receipt of your validation of compliance with your PCI DSS standards as required under your Processing Agreement ("Non-Validation Fee") will be changed to $19.95 per month.

3. Data Protection.

3.1. Definitions.

(a) "Multi-Pay Token" means the option to support businesses that need to submit a financial transaction in a card-not-present situation. These tokens are unique to each merchant that uses them and are stored in place of the primary account number (PAN). With these tokens, merchants can initiate new or recurring payments within their own environment instead of using the original card number. Multi-Pay Token allows a Token Registration process—a non-financial transaction to request a token to be placed in their payment page or "e-wallet" for future or recurring payments. It is common for eCommerce merchants to ask their customers to register by providing profile information such as name, address, and phone number to the merchant website before or upon checkout;

(b) "Registered PAN" means the processing of creating a Client specific Token for a PAN;

(c) "Token/Tokenization" means a form of data substitution replacing sensitive payment card values with non-sensitive token, or random-number, values. Post-authorization transactions are handled via Processors SafeProxy tokenization technology, which returns a token with the transaction's authorization to the merchant;

(d) "Token Request" means your ability to obtain a Multi-Pay Token for credit card information only without an immediate authorization required which permits you to store a Multi-Pay Token for future transactions involving its customer; and

(e) "Data Protection Service" means those services described in Section 3.4. below and may be either Data Protection VeriFone Edition Service or Data Protection Base Service as described below.

3.2. Eligible Point of Sale Device. The Data Protection Service can only be used with a point of sale device, gateway and/or VAR that are certified by us as Data Protection eligible. It is your responsibility to ensure that you have eligible equipment in order to use the services. If you are uncertain whether you have eligible equipment, contact a client service representative at 866-359-0978.

3.3. Grant of License. Subject to the terms of this Addendum, we grant to you a non-transferable, non-assignable, non-exclusive, revocable sub-license during the term of this Addendum to use the Data Protection Service and the Data Protection Service Marks (as identified in the Data

Protection Rules and Procedures) in the United States in accordance with this Addendum, including without limitation the Data Protection Rules and Procedures. Upon expiration or termination of the Agreement or this Addendum for any reason, your license shall automatically be revoked. Furthermore, your right to use or access the Data Protection Service shall cease.

3.4. Services. The Data Protection Service only applies to Card transactions sent from you to us for authorization and settlement pursuant to the Agreement, and specifically excludes electronic check transactions. We will provide an encryption key to you to be used to encrypt (make unreadable) Card data during transport of the authorization request from your point of sale to our systems. During the period when the transaction is being transmitted to us for authorization processing, all historical transaction data, including Card number and full magnetic stripe data (track data and expiration date), will be encrypted. We will then generate or retrieve a unique, randomly generated token assigned to the Card number that will be returned to you in the authorization response (the "Token"). You have the options below for the Data Protection Service depending on your point of sale device:

(a) Data Protection VeriFone ("VF") Edition. This service option is limited to those merchants who have an eligible VeriFone point of sale ("POS") device and desire the software or hardware based Data Protection to be activated through the VeriFone device.

(b) Data Protection Base Service. This service option provides software based Data Protection that is available to merchants to integrate into their POS or the point of sale device.

3.5. Responsibilities of Client. You are responsible to comply with the following regarding your use of the Data Protection Service:

(a) You are required to comply with the Card Organization Rules, including taking all steps required to comply with the Payment Card Industry Data Security Standards (PCI DSS). You must ensure that all third parties and software use by you in connection with your payment processing are compliant with PCI DSS. Use of the Data Protection Service will not, on its own, cause you to be compliant or eliminate your obligations to comply with PCI DSS or any other Card Organization Rule. You must demonstrate and maintain your current PCI DSS compliance certification. Compliance must be validated either by a Qualified Security Assessor (QSA) with corresponding Report on Compliance (ROC) or by successful completion of the applicable PCI DSS Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC), as applicable, and if applicable to your business, passing quarterly network scans performed by an Approved Scan Vendor, all in accordance with Card Organization Rules and PCI DSS.

(b) Use of the Data Protection Service is not a guarantee against an unauthorized breach of your point of sale systems or any facility where you process and/or store transaction data (collectively, "Merchant Systems").

(c) You must deploy the Data Protection Service (including implementing any upgrades to such service within a commercially reasonable period of time after receipt of such upgrades) throughout your Merchant Systems including replacing existing Card numbers on your Merchant Systems with Tokens. Full Card numbers must never be retained, whether in electronic form or hard copy.

(d) You must use the Token in lieu of the Card number for ALL activities subsequent to receipt of the authorization response associated with the transaction, including without limitation, settlement processing, retrieval processing, chargeback and adjustment processing and transaction reviews.

(e) If you send or receive batch files containing completed Card transaction information to/from us, you must use the service provided by us to enable such files to contain only Tokens or truncated information.

(f) You must use truncated report viewing and data extract creation within reporting tools provided by us.

(g) You are required to follow rules or procedures we may provide to you from time to time related to your use of the Data Protection Service ("Data Protection Rules and Procedures"). We will provide you with advance written notice of any such rules or procedures or changes to such rules or procedures.

(h) You will use only unaltered version(s) of the Data Protection Service and will not use, operate or combine the Data Protection Service or any related software, materials or documentation, or any derivative works thereof with other products, materials or services in a manner inconsistent with the uses contemplated in this Addendum.

(i) You will promptly notify us of a breach of any these terms.

3.6. Tokenization Limited Warranty. We warrant that the Token returned to you, as a result of using the Data Protection Service, cannot be used to initiate a financial sale transaction by an unauthorized entity/person outside the Merchant Systems. This warranty by Processor is referred to herein as the "Limited Warranty" and is subject to the terms and conditions set forth in this Addendum. To be eligible for the Limited Warranty, you must maintain a processing relationship with us and be in compliance with all the terms of the Agreement, including this Addendum, and any other agreement relating to Cards eligible for the Data Protection Service. Subject to the terms, conditions and limitations set forth in the Agreement including this Addendum, including the limitation of liability provisions, we agree to indemnify and hold you harmless from direct damages, including third party claims, resulting from our breach of the Limited Warranty. The express remedy for our breach of the Limited Warranty set forth in this paragraph constitutes our entire liability and your sole and exclusive remedy for our breach of the Limited Warranty. The Limited Warranty is void if (i) you use the Data Protection Service in a manner not contemplated by, or in violation of, the Agreement, including this Addendum, or any other agreement relating to Cards eligible for the Data Protection Service or (ii) you are grossly negligent or engage in intentional misconduct.

4. POS Software Monitor.

4.1. Software as a Service. Subject to the terms and conditions of this Addendum, we agree to provide you with the POS Software Monitor software application, including all updates, upgrades, new versions, and other enhancements or improvements thereto (the "Software"), to the extent the applicable fees are paid. You hereby authorize us or our vendors to begin scanning immediately upon your installation and/or deployment of the Software. The Software can only be used with certain computer operating systems. It is your responsibility to ensure that your computer has the software in order to use the POS Software Monitor.

4.2. License Grant. Subject to the terms of this Addendum, we hereby grant to you a non-exclusive, non-transferable, non-assignable, revocable sub-license during the term of this Addendum to (i) access and use the Software solely for the benefit of you and only for systems owned or licensed by you; (ii) access and use the Software solely for its intended use; and (iii) use all applicable end user documentation.

4.3. Revocation of License. Upon expiration or termination of the Agreement or this Addendum for any reason, your license shall automatically be revoked. Furthermore, your right to use or access the Software shall cease.

4.4. IP & Other Data Retrieval, Transmission and Scanning.

(a) IP/Data Retrieval and Transmission. You hereby grant us or our vendors, the right to retrieve, transmit and monitor, for the intended purpose of the POS Software Monitor, any dynamic or static IP address and other data, including without limitation policy and system settings, point of sale system type, version, security event logs, or other related information, from any system with the POS Software Monitor loaded, deployed, or otherwise installed. You shall not, in any event or in any manner, impede the retrieval or transmission of such IP addresses or data. You hereby assume full responsibility for all damages and losses, of any nature, for all adverse results caused by your impeding the such retrieval and transmission of the IP addresses and data. You further agree to defend, indemnify and hold us harmless from any third party claim resulting from your impeding this process.

(b) IP Scanning & Log Monitoring. You acknowledge and understand that provisioning of the Software will enable static or dynamic IP addresses associated with the POS Software Monitor to be scanned. You further acknowledge that such IP addresses may be for external network devices which protect the POS Software Monitor host system. You hereby grant us and our vendors (i) the right to access and scan the IP addresses associated with the POS Software Monitor whether they are dynamic or static IP addresses (the "Authorized IP Addresses"), (ii) the right and authority to gather and transmit system data, including point of sale system information, to us or our vendors, and (iii) the right and authority to collect, transmit and review security event logs from the systems on which the Software is deployed. You further agree to provide us or our vendors reasonable assistance to enable such access and scanning. You understand that your failure to cooperate with the provision of services may significantly impair the services.

(c) Updates. You acknowledge and understand that the POS Software Monitor, in our sole discretion, can automatically install, download, and/or deploy updated and/or new components ("update process"), which may include a new version of the POS Software Monitor itself. You shall not, in any event or in any manner, impede the update process. You hereby assume full responsibility for all damages and losses, of any nature, for all adverse results caused by your impeding the update process. You agree to defend, indemnify and hold us harmless from any third party claim resulting from your impeding the update process.

(d) Authorized Disclosure. You acknowledge that, in conjunction with providing the Software, we may make certain "pass" or "fail" determinations regarding your online security and the electronic vulnerability of your IP addresses. You hereby authorize us or our vendors to share these "pass/fail" results, point of sale data, and other information collected during the scans to Card Organizations, Payment Card Industry Security Standards Council or any Card Organization sponsor bank.

5. PCI Rapid Comply Service

5.1. License Grant. Subject to the terms of this Addendum, we hereby grant to you a non-exclusive, non-transferable, non-assignable revocable sub-license to (i) access and use the PCI Rapid Comply Service solely for the benefit of you and only on a single computer or computer network owned or licensed by you, (ii) access and use the PCI Rapid Comply Service solely for its intended use and (iii) use all applicable end user documentation. Upon expiration or termination of the Agreement or this Addendum for any reason, your license shall automatically be revoked. Furthermore, your right to use or access the PCI Rapid Comply Service shall cease.

5.2. Access. You acknowledge and agree that, although you will generally have access to the PCI Rapid Comply Service twenty-four hours per day, seven days per week (except in the event of a force majeure event), access to customer accounts and certain other services may not be available on a continuous basis and the PCI Rapid Comply Service will be subject to periodic downtime to permit, among other things, hardware and/or software maintenance to take place.

5.3. Data Disposal. From time to time, your account data or information, which is over 180 days old, may be deleted, purged or otherwise disposed. In addition, only a limited amount of your account data or information may be available online. Therefore, you are advised to print and download your account data and information, for record keeping purposes, on a periodic basis. You specifically agree that we are authorized to delete or dispose of your data or information and shall not be responsible for the deletion or disposal of your data or information from the PCI Rapid Comply Service. You assume full responsibility to backup and/or otherwise protect your data against loss, damage or destruction prior to and during all phases of the PCI Rapid Comply Service, and to take appropriate measures to respond to any potential adverse impact of the systems or disruption of service.

5.4. Copyrighted Material. The PCI Rapid Comply Service (including the website), contains copyrighted material, trademarks and other proprietary information, including, but not limited to, text, software, photos, video, and graphics. You may not modify, publish, transmit, participate in the transfer or sale, create derivative works, or in any way exploit any of the content, in whole or in part, whether copyrighted, trademarked or proprietary, or otherwise. You may download copyrighted material solely for your own internal use as contemplated under this Addendum. Except as expressly provided by copyright law, any copying, redistribution, or publication must be with the express permission of the owner. In any copying, the redistribution or publication of copyrighted material and any changes to or deletion of author attribution or copyright notice is expressly prohibited.

6. Liability Waiver

6.1. Data Security Event Expenses. Subject to the limitations, terms and conditions of this **Section 6**, we agree to waive liability **(**the **"Liability Waiver")** that you have to us under the Agreement for Security Event Expenses and Post Event Services Expenses resulting from a Data Security Event first discovered by you or us while this Addendum is in effect. Except for the Liability Waiver for expenses as specifically set forth in this Addendum, (i) you remain responsible to perform all agreements and obligations under the Agreement and this Addendum including, without limitation your obligation to comply with data security requirements and (ii) we waive no rights or remedies under your Agreement including, without limitation, our right to terminate the Agreement in the event of a Data Security Event.

6.2. Maximum Waiver Amount.

(a) The maximum amount of liability that we shall waive under the Agreement for all Security Event Expenses and Post Event Services Expenses arising out of or relating to the your Data Security Events first discovered during any Program Year regardless of the number of such Data Security Events is as follows:

(1) $100,000.00 maximum per each MID (merchant identification number) you have; and

(2) $500,000 aggregate maximum for all of your MID's**.**

(b) The maximum amount of liability during any Program Year that we will waive under the Agreement for EMV Upgrade Costs is as follows:

(1) $10,000 maximum per each MID you have; and

(2) $25,000.00 aggregate maximum for all of your MID's.

For avoidance of doubt, the limit set forth in this **Section 6.2(b)** is part of and not in addition to the maximums set forth in **Section 6.2(a)**.

6.3. Definitions:

(a) "Cardholder Information" means the data contained on a Card, or otherwise provided to Customer, that is required by the Card Organization or us in order to process, approve and/or settle a Card transaction;

(b) "Card Organization Assessment" means a monetary assessment, fee, fine or penalty levied against you or us by a Card Organization as the result of (i) a Data Security Event or (ii) a security assessment conducted as the result of a Data Security Event; the Card Organizational Assessment shall not exceed the maximum monetary assessment, fee, fine or penalty permitted upon the occurrence of a Data Security Event by the applicable rules or agreement in effect as of the inception date of this Addendum for such Card Organization;

(c) "Card Replacement Expenses" means the costs that the we or you are required to be paid by the Card Organization to replace compromised Cards as the result of (i) a Data Security Event or (ii) a security assessment conducted as the result of a Data Security Event;

(d) "Data Security Event" means the actual or suspected unauthorized access to or use of Cardholder Information, arising out of your possession of or access to such Cardholder Information, which has been reported (i) to a Card Organization by you or us or (ii) to you or us by a Card Organization. All Security Event Expenses and Post Event Services Expenses resulting from the same, continuous, related or repeated event or which arise from the same, related or common nexus of facts, will be deemed to arise out of one Data Security Event;

(e) "EMV Upgrade Costs" means cost to upgrade payment acceptance and processing hardware and software to enable you to accept and process EMV-enabled Card in a manner compliant with PCI Data Security Standards;

(f) "Forensic Audit Expenses" means the costs of a security assessment conducted by a qualified security assessor approved by a Card Organization or PCI Security Standards Council to determine the cause and extent of a Data Security event;

(g) "Liability Waiver" has the meaning as set forth in Section 6.1 above;

(h) "Pollutants" means, but are not limited to, any solid, liquid, gaseous, biological, radiological or thermal irritant or contaminant, including smoke, vapor, dust, fibers, mold, spores, fungi, germs, soot, fumes, asbestos, acids, alkalis, chemicals and waste. "Waste" includes, but is not limited to, materials to be recycled, reconditioned or reclaimed and nuclear materials; and

(i) "Post Event Services Expenses" means reasonable fees and expenses incurred by us or you with our prior written consent, for any service specifically approved by us in writing, including without limitation, identity theft education and assistance and credit file monitoring. Such services must be provided by or on behalf of us or you within one (1) year following discovery of a Data Security Event to a Cardholder whose Cardholder Information is the subject of that Data Security Event for the primary purpose of mitigating the effects of such Data Security Event;

(j) "Program Year" means the period from June 1st through May 31st of each year; and

(k) "Security Event Expenses" means Card Organization Assessments, Forensic Audit Expenses and Card Replacement Expenses. Security Event Expenses also includes EMV Upgrade Costs you agree to incur in lieu of a Card Organization Assessment.

6.4. Duties in the Event of a Data Security Breach

(a) You shall contact us immediately and, as directed by us, investigate, perform all remedial events and cooperate fully with us, in the event of a Data Security Event. In all events, you shall not take any action, or fail to take any action, without our prior written consent, which prejudices our rights hereunder.

(b) Under all circumstances, you shall not admit any liability, assume any financial obligation, pay any money, or incur any expense in connection with any Data Security Event without our prior written consent. If you do so, it will be at your own expense.

6.5. Exclusions

The Liability Waiver hereunder shall not apply to:

(a) Any Security Event Expenses and Post Event Services Expenses arising out of or resulting, directly or indirectly, from any dishonest, fraudulent, criminal or malicious act, error or omission, or any intentional or knowing violation of the law, if committed by you or your employees, officers, agents or director;

(b) Any Security Event Expenses and Post Event Services Expenses arising out of or resulting from a claim, suit, action or proceeding against you that is brought by or on behalf of any federal, state or local government agency;

(c) Any Data Security Event relating to you which has experienced a prior Data Security Event unless you were later certified as PCI compliant by a qualified security assessor;

(d) Any Data Security Event arising out of your allowing any party (other than its employees or us) to hold or access Cardholder Information;

(e) Any Data Security Event if Client: (i) is categorized by any Card Organization as "Level 1" or (ii) processes more than six million (6,000,000) Card transactions during the twelve month period prior to the date this Addendum became effective;

(f) Any expenses, other than Security Event Expenses and Post Event Services Expenses, incurred by you arising out of or resulting, directly or indirectly, from a Data Security Event, including without limitation, expenses incurred to bring you into compliance with the PCI Data Security Standard or any similar security standard;

(g) Any Security Event Expenses, and Post Event Services Expenses arising out of or resulting, directly or indirectly, from physical injury, sickness, disease, disability, shock or mental anguish sustained by any person, including without limitation, required care, loss of services or death at any time resulting therefrom;

(h) Any Security Event Expenses, and Post Event Services Expenses arising out of or resulting, directly or indirectly, from any of the following:

1. fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, an act of God or any other physical event, however caused; or

2. strikes or similar labor action, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not), civil war, mutiny, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions;

(i) Any Security Event Expenses, and Post Event Services Expenses arising out of or resulting, directly or indirectly, from the presence of or the actual, alleged or threatened discharge, dispersal, release or escape of Pollutants, or any direction or request to test for, monitor, clean up, remove, contain, treat, detoxify or neutralize pollutants, or in any way respond to or assess the effects of pollutants;

(j) Your failure to comply with this Addendum or the Agreement in connection with a Data Security Event;

(k) Any Data Security Event occurring before the effective date of this Addendum;

(l) Any expenses incurred for, or as a result of, regularly scheduled, recurring or routine security assessments, regulatory examinations, inquiries or compliance activities;

(m) Any fines or assessment levied against you that are not the direct result of a Data Security Event;

(n) Any Data Security Event arising out of any software not within your control; provided, however, this exclusion shall not apply to a Data Security Event arising out of a virus, Trojan horse or other software used by a third party to obtain fraudulent access to data to your computer system or to collect data in transit to or from your computer system; or

(o) Any Data Security Event arising out of a breach in a computer system in which you and other merchants, with no legal relationship to one another, have hosted accounts or share a common database, operating system or software applications.

7. Processor Technology and IP. All technology used by us or our licensors in connection with performing the TransArmor Services including, software, portals, data processing systems (each of the foregoing, in object code and source code form), report templates, documentation and materials (collectively, "Processor Technology"), and any of our or our licensor's patents, trademarks, copyrights, trade secrets and other intellectual property ("Processor IP"), and any derivative works of or modifications to the Processor Technology or Processor IP, is the sole and exclusive property of, and is valuable, confidential and proprietary to, Processor or its licensors. Except as otherwise expressly provided herein, you shall not acquire any rights in any Processor Technology or IP as a result of receiving the TransArmor Services. You will not file any action, in any forum that challenges the ownership any of the TransArmor Services, Processor Technology or Processor IP. Failure to comply with this provision will constitute a material breach of this Addendum. We have the right to immediately terminate your access to and use of the TransArmor Services in the event of a challenge by you. No additional rights are granted by implication, estoppel or otherwise.

8. Data Collection. In the course of providing the TransArmor Services, we may collect information relating to activities on your network (the "Data") including, but not limited to, network configuration, TCP/IP packet headers and contents, log files, malicious codes, and Trojan horses. We retain the right to use the Data or aggregations thereof for any reasonable purpose.

9. Service Does Not Guarantee Compliance or Security. You acknowledge and agree that your use of the TransArmor Services does not guarantee your compliance with any of the rules or security standards established by the Card Organizations. You further acknowledge and agree that your use of the TransArmor Services does not guarantee the security of your IP addresses or that your systems are secure from unauthorized access. You are responsible for establishing and maintaining your own security policies and procedures, and for compliance with the Card Organization Rules and security standards, including any obligation to notify a Card Organization and/or us of any suspected breach of your systems or any suspicious transactions or fraudulent activity. You are responsible for any fines or penalties imposed by any Card Organization any other expenses and liabilities pursuant to the Agreement less only the benefits to which you may be entitled under the Liability Waiver provisions of this **Addendum**. In the event of a suspected breach of your systems or any suspicious transactions or fraudulent activity, you authorize us to share the details of any questionnaire or compliance report with the Card Organizations, and grant us and our vendors the right to access and perform a scan of the IP addresses identified within your profile. You agree and authorize payment for the additional scan. You further agree to cooperate with an investigation into such matter to include complying with the Card Organization and us pursuant to the terms of the Agreement.

In addition to your obligations under the Agreement to comply with all laws, you are solely responsible for monitoring legal developments applicable to the operation of your business, interpreting applicable laws and regulations, determining the requirements for compliance with all applicable laws and regulations, and maintaining an on-going compliance program.

10. Scanning Authority; Scanning Obligations. You represent and warrant that you have full right, power, and authority to consent for the TransArmor Services to scan for vulnerabilities the IP address and/or URL and/or domain names identified to us by you for scanning, whether electronically or by any other means, whether during initial enrollment or thereafter. If applicable, you shall obtain all consents and authorizations from any third parties necessary for us or our vendors to perform the TransArmor Services, including, without limitation, third party datacenters, co-locations and hosts. We will not be required to execute agreements with any such third parties. You agree to defend, indemnify and hold us and our vendors harmless from any third party claim that such access was not authorized. You may use the TransArmor Services and portals only to scan IP addresses, URLs and domain names owned by and registered to you. You understand that your failure to provide a complete list of and complete access to your IP addresses will significantly impair the scanning services and may result in incomplete or inaccurate results. You agree that all TransArmor Services hereunder, including without limitation their functionality and contents, is confidential information, and Client's use and/or access to the TransArmor Services is subject to the terms of Confidentiality in the Agreement.

11. Scanning Risks. You acknowledge and understand that accessing, retrieving, transmitting, and scanning IP addresses and other data involves inherent risks, including, without limitation, risks related to system or network performance and availability, and data corruption. You assume full responsibility to backup and/or otherwise protect your data against loss, damage or destruction, and to take appropriate measures to respond to any potential adverse impact of the systems or disruption of service.

12. Use of TransArmor Services and Portals. Your use of our or our vendors' services, portals, reports, and scanning solution is subject to the following restrictions: (i) TransArmor Services, portals, and reports may only be used for the stated purposes in this Addendum for your internal business purposes in accordance with all applicable laws (including any export control laws); (ii) TransArmor Services and portals utilized for scanning may only scan IP addresses, URLs and domain names owned by and registered to you; and (iii) you shall limit access to the portals to only those employees and/or contractors who have an obligation of confidentiality with you and only to those who have a requirement for such access on a "need to know" basis and you shall be solely responsible for disabling portals accounts for those employees and/or contractors who no longer require access. You shall promptly notify us of any unauthorized use of the TransArmor Services. You shall not (i) decompile, reverse engineer, disassemble, or otherwise derive the source code from any component of the TransArmor Services or portals including the software embedded therein; (ii) modify, enhance, translate, alter, tamper with, upgrade or create derivatives works of the portals, software or documentation; (iii) distribute, lease, license, sell, assign, sublicense or otherwise disseminate or transfer its rights to use any portion of the TransArmor Services to any third party or (iv) strip out or alter any trademark, service mark, copyright, patent, trade secret, ownership or any other proprietary or Intellectual Property notices, legends, warnings, markings or indications on or within any component of the portals, software or documentation, or attempt (i), (ii), (iii) and/or (iv) above. You shall notify us immediately if you know, suspect or have reason to know that you or anyone you have granted access to the TransArmor Services violated any provision of this Addendum. Further you agree not to share your personal information (DDA, tax ID, MID, etc.) with a third party so they may gain access to the TransArmor Services.

13. Disclaimers. We do not make and hereby expressly disclaim all representations or warranties including, without limitation (i) that access to the TransArmor Services will be uninterrupted or error free; (ii) that security breaches will not occur with respect to any information communicated through the TransArmor Services, the Internet, or any common carrier communications facility; and (iii) as to the results that may or may not be obtained by you in connection with your use of the TransArmor Services. **WE DO NOT MAKE ANY WARRANTY, GUARANTEE OR REPRESENTATION (EITHER EXPRESS OR IMPLIED) OF ANY KIND INCLUDING, WITHOUT LIMIATION, THE**

MERCHANTABILITY, TITLE, NONINFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE OF ANY SERVICES PROVIDED UNDER THIS ADDENDUM, AND ALL SUCH WARRANTIES, GUARANTEES AND REPRESENTATIONS ARE HEREBY EXPRESSLY DISCLAIMED. ALL SERVICES PROVIDED UNDER THIS ADDENDUM ARE PROVIDED ON AN "AS-IS, WITH ALL FAULTS".

USE OF THE SERVICES DOES NOT GUARANTY SECURITY OR PREVENT A SECURITY BREACH OR COMPROMISE. WE MAKE NO WARRANTIES, EITHER EXPRESSED OR IMPLIED THAT PARTICIPATION AND/OR USE OF OUR SERVICES WILL DETECT EVERY VULNERABILITY ON YOUR SYSTEM, IFANY, OR THAT OUR VULNERABILITY ASSESSMENTS, SUGGESTED SOLUTIONS OR ADVICE WILL BE ERROR-FREE OR COMPLETE. CUSTOMER AGREES THAT WE SHALL NOT BE RESPONSIBLE OR LIABLE FOR THE ACCURACY OR USEFULNESS OF ANY INFORMATION PROVIDED BY US, OR FOR ANY USE OF SUCH INFORMATION.

You acknowledge and agree that we shall not be liable to you for any claims, damages, losses, obligations, costs or expenses or other liability arising directly or indirectly from or otherwise concerning (i) any termination, suspension, delay or disruption of service (including billing for a service) by the Internet, any common carrier or any third party service provider; (ii) any failure, disruption or malfunction of any of the TransArmor Services, the Internet, or any communications network, facility or equipment beyond our or a third party's reasonable control, whether or not attributable to one or more common carriers; (iii) your failed attempts to access the TransArmor Services or to complete transactions via any of the TransArmor Services; (iv) any failure to transmit, obtain or collect data or for human, machine or software errors or faulty or erroneous input by you; (v) any damages resulting from any delays and/or losses arising in connection with the TransArmor Services provided hereunder; or (vi) any loss of or inability to access data or information stored or generated by TransArmor Services.

14. Limitation of Liability. Notwithstanding anything to the contrary in this Addendum or elsewhere, our cumulative liability to you for any claim related to this Addendum, and your use of the Services (whether arising from tort, statute, contract or otherwise) shall in all cases be limited to the actual, direct and proven out-of-pocket losses, damages or expenses suffered or incurred by you. Furthermore, our cumulative liability to you shall not, in any case, exceed the TransArmor Solution Fees paid to us by you during the 12 month period immediately preceding the date the event giving rise to the claim occurred. Notwithstanding anything to the contrary in this Addendum or elsewhere, in no event shall we be liable to you or to any third party for any indirect, special, incidental, consequential, punitive or unproven losses, damages or expenses of any kind, including, without limitation, lost profits or loss of goodwill arising from the use or inability to use the Services including, without limitation, the inability to access your data or information generated or stored on the Services, and regardless of whether such claim arises in tort, in contract or by statute or regulation, each of which is hereby excluded, regardless of whether such damages were foreseeable or whether you have been advised of the possibility of such damages.

The parties acknowledge and agree that the provisions and limitations of this Section 15 are of the essence of this Addendum and that absent them, the parties would not have agreed to this Addendum.

15. Miscellaneous; Termination. Except as may be provided in the Agreement, a person who is not a party to this Addendum, shall have no rights or remedies under this Addendum. Our obligations hereunder are subject to our ability to obtain and maintain any and all required governmental licenses, permits or other authorizations, and our ability to comply with any and all laws, regulations, orders and other governmental directives which may be imposed related to the TransArmor Services. We may terminate any or all of the TransArmor Services at any time for any reason.

Except as set forth herein, the Agreement is hereby ratified in all respects and shall remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have caused this Addendum to be duly executed by their authorized officers, all as of the day and year first written above.

Client:	**First Data Merchant Services Corporation**
_____	
By: _____	By: _____
Printed: _____	Printed: _____
Title: _____	Title: _____
Date: _____	Date: _____