

January 29, 2024

Tokenization Terms

Batch Tokenization Terms

Customer will provide input file(s) for tokenization via SFTP upload.

TokenEx will provide SFTP credentials and connection information to Customer

Only the standard SFTP port is authorized (tcp/22)

The file must be in one of the following supported standards-based file formats: XML, Delimited (pipe, comma, etc), Fixed Width.

The input file(s) must be encrypted with either a public PGP key Customer provides to TokenEx, or with TokenEx's public PGP key.

TokenEx will decrypt the input file(s), either tokenize or detokenize the appropriate data, and generate response file(s) containing the updated data.

Customer will provide a public PGP key for encrypting the response file(s).

TokenEx will place the response file(s) on its SFTP server, available for download by Customer. Customer is responsible for thoroughly testing the flow once configured by TokenEx.

If the file format or transmission flow is changed by Customer and TokenEx determines the new format or flow is not supported, TokenEx may cease its efforts to provide the batch file configuration described herein, upon written notice of incompatibility to Customer.

Customer agrees to pay the batch configuration fee described above. Customer will be invoiced upon signature and payment is due thirty (30) days from receipt of the invoice.

Network Tokenization Terms

Customer must have a merchant Token Requestor ID ("**TRID**") for each card network which it wants to issue network tokens. If Customer does not have the required TRIDs already, TokenEx can facilitate acquiring TRIDs from supported card networks. Use of the network tokenization service will not be available until the appropriate TRIDs are in place.

Network Tokenization Operations are counted separately from and do not affect the base subscription Operation counts.

Network Tokenization API calls are Operations which result in a charge. A list of the applicable calls can be found at <https://docs.tokenex.com> under "Network Tokenization API."

Multiple Operations may be involved to request a network token:

"Tokenize" is required for every card PAN at least once;

"Get Payment Bundle" is required on an initial merchant-initiated transaction;

"Get Payment Bundle" is required on every customer-initiated transaction

Additional Product and Services Terms

3D Secure Terms

3D Secure ("3DS") is a service provided by TokenEx to assist Customer with fraud prevention and detection efforts in card not present transactions. Use, licensing and provision of 3D Secure functionality is provided via the TokenEx Platform and is subject to the following terms specifically applicable to the 3DS Services

Prior to use of the 3DS Services, Customer is required to obtain a Requestor ID from Visa, Mastercard and Discover. Customer will incur a charge for each 3DS-specific API call but a 3DS-specific API call will not be additionally included in Customer's general monthly operations count. Customer remains responsible for separately paying any networks' fees charged in connection with each authentication request submission. Additionally, upgrades of the 3DS Services, e.g., a new version or enhancement offering that incorporates significant additional or improved features, may be subject to additional fees.

Customer may only use the 3DS Services as set forth in the Agreement and under no circumstances is Customer authorized to use the 3DS Services for any purpose other than as permitted under the Agreement. 3DS Services are provided and made available for Customer's non-transferable, non-exclusive use, without right to sub-license. Customer must not remove any copyright or other proprietary notices on or in the 3DS Services. No right, title, or interest in the 3DS Services or any intellectual property rights in the 3DS Services is transferred to Customer.

Customer represents and warrants that the use, analysis and/or processing of Customer Data to perform and/or provide the 3DS Services are collectively permitted under applicable laws, regulations and regulatory guidance and the terms of Customer's contracts with, notices to or other consents from its customers, contractors, suppliers or other third parties.

Customer agrees to indemnify, defend, and hold harmless TokenEx, its Affiliates, and respective officers, directors, employees, agents and representatives from and against any third-party claim and agrees to pay any losses, costs, liabilities, demands, damages, and expenses including reasonable attorneys' fees incurred as a result of any such third party claim (except to the extent caused by TokenEx's breach of any of its obligations relating to 3DS Services) arising from or attributable to Customer's material breach of any of its obligations, representations, and warranties hereunder; or gross negligence or willful misconduct in the performance of its obligations in connection with the 3DS Services. Customer's indemnification obligations will survive expiration or termination of the Agreement.

Account Updater Terms

These are additional terms that govern Customer's use of the TokenEx Account Updater Service ("**Account Updater Product Service**").

The Account Updater Product Service enables card issuers to supply the most current account information through acquirers to registered merchants that require electronic maintenance of customer account data. Participating merchants use updated cardholder account information to support subscription services, recurring payments, and other account-on-file functions. The Account Updater Product Service provides an automated, dedicated, secure clearinghouse to make changes to limited cardholder account information (such as account numbers, expiration data, account closures or other changes) available in a timely, efficient, and cost-effective manner.

The parties agree to the following terms regarding the Account Updater Product Service:

1) CUSTOMER QUALIFICATIONS

- a) a) Customers who are designated by Visa as high-risk (High-Risk Acquirer Program with a condition of RED or higher) or on the Mastercard Alert to Control High-risk Merchants (MATCH) system may **not** participate in Account Updater.
- b) Customer is not and shall not be engaged in business categorized by the following merchant codes: 5962, 5966, 5967, or 7995.
- c) Customer must have been in business for at least six (6) months and must process an average of 1,000-5,000 card transactions per month.
- d) Customer shall not be under any special conditions imposed by Visa Corporate Risk Management.

1) Customer Participation Requirements.

Customer must continue to meet Visa Merchant Participation Requirements as established by Visa from time to time, and MasterCard Participation Requirements as established by MasterCard from time to time, including:

- a) a) Customer shall be a registered merchant. If Customer is not registered as a merchant with Visa and MasterCard on the date of execution of this agreement, Customer agrees to allow TokenEx to facilitate its registration. Customer further agrees it will not be able to use the Account Updater Service until this registration is complete.
- b) Customer shall not have been disqualified from participating in either Visa or MasterCard systems.
- c) Customer shall comply with Visa Operating Regulations and MasterCard Operating Regulations.
- d) Customer shall comply with all applicable laws and regulations.
- e) Pursuant to the Visa Account Updater Terms of Use, Customer shall request a Visa Account Updater update for every participating Visa account in Customer's database of customers at least once every 180 calendar days if Customer bills daily, weekly, monthly, quarterly or bi-annually, or at least once every 365 calendar days if Customer bills annually.

2) SECURITY REQUIREMENTS FOR CUSTOMER

- a) a)Customer shall comply with all applicable laws, such as data protection laws (including gathering specific consent of cardholders for processing and transfer of personal data via third parties, if applicable).
- b) Customer shall ensure that cardholder information is securely stored, and that such information is available only to those employees of Customer who have a legitimate business need and authorization to access cardholder information.
- c) Customer shall ensure that employees who have access to cardholder information are aware of and familiar with Customer's policies as they relate to the use of such cardholder information (and related personal data).
- d) Customer shall delete all Account Updater files with cardholder information after use to minimize the likelihood of improper access to or use of the data.
- e) Customer shall remain compliant with the Payment Card Industry Data Security Standard at all times.
- f) Customer shall use the same standard of care for confidential information returned in connection with the Account Updater Service as it uses for its own Confidential Information but no less than industry standard for protection of confidential information.

3) CUSTOMER RESPONSE RECORDS

- a) a)Customer shall update its customer account database within two (2) business days of receipt of updated cardholder information from TokenEx.
- b) Customer shall ensure that information received in connection with the Account Updater Service is properly, completely, and accurately incorporated into the Customer's customer database for utilization in future transactions.
- c) Customer shall not re-submit cardholder data that has returned a response of "Closed Account" or "Contact Cardholder."

4) ACCOUNT UPDATER PRICING

- a) TokenEx will invoice Customer as described in an Order in which Customer purchases the Account Updater Service.
- b) Pricing for the Account Updater Service is based on the number of Match Operations, with a "**Match Operation**" defined as any of the following responses: (i) Account Number Changes (ii) Account Expiration Date changes (iii) Closed Account (iv) Contact Cardholder.
- c) Customer shall only submit cardholder information for updating for which Customer has a valid business need, such as a recurring billing, subscriptions, or advanced payment.
- d) Customer shall have cardholder permission to submit the account information to third-party for account updating purposes.

5) CUSTOMER'S REPRESENTATIONS AND WARRANTIES

- a) Customer represents and warrants the following:
 - a)Customer is and shall at all times remain compliant with all Card Brand rules.
- b) Customer shall restrict access to Account Updater updates and cardholder Information to those persons having a legitimate business-related need to know.
- c) Customer is solely responsible for providing notice to and obtaining any necessary consent from cardholders in connection with the processing of personal data in connection with Account Updater.

- d) Customer is not a High-Risk Merchant as designated by Visa.
- e) Merchant has not been listed on Mastercard's MATCH system.
- f) Customer has never been disqualified from any Card Brand participation.
- g) Customer has been in business for more than 6 months.
- h) Customer is not a merchant under merchant codes 5962, 5966, 5967, or 7995.
- i) Customer's business is not predominantly quasi-cash, account funding or any combination of the sorts.
- j) Customer shall submit update requests solely for itself and for not for any other business entity.
- k) Customer is solely responsible for handling requests from cardholders to access, correct, block, or delete their personal data in connection with Account Updater.

6) INDEMNIFICATION

Customer agrees to indemnify and hold TokenEx and its respective directors, officers, agents, and employees harmless against any and all liability, costs, damages, and actions arising in connection with (i) Customer's use of the Account Updater Service, confidential information, and/or any associated written materials, and/or (ii) any breach of its obligations stated in this Account Updater Addendum.

7) CONFIDENTIALITY

Customer acknowledges and agrees to the following:

- a) The Account Updater Service contains confidential information of TokenEx and others that has been disclosed to the Customer or to which the Customer has been provided access.
- b) Customer shall not misappropriate such confidential information.
- c) The Account Updater Service contains personal data disclosed by Customer.
- d) Any and all Confidential Transaction Data (as defined in the Card Network rules) or other personal data provided to the Card Networks in connection with Customer's use of the Account Updater Service may be used by the Card Networks for the purposes described in their respective rules and for purposes of providing the Account Updater Service and other services requested by Customer.

For purposes of clarity, Customer represents and warrants that Customer will be solely responsible for providing notice to and obtaining any necessary consent from cardholders in connection with the processing of personal data by the Card Networks.

8) WARRANTY DISCLAIMER AND LIMITATION OF LIABILITY

TOKENEX DOES NOT REPRESENT OR WARRANT THAT THE ACCOUNT UPDATER SERVICE IS FREE OF DEFECT AND/OR MISTAKE; THE ACCOUNT UPDATER SERVICE IS PROVIDED ON AN "AS IS" BASIS, "WITH ALL FAULTS". TOKENEX AND ITS ACCOUNT UPDATER COMPONENT SUPPLIERS DISCLAIM ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO: THE ACCOUNT UPDATER SERVICE, CONFIDENTIAL INFORMATION AND/OR ANY ASSOCIATED WRITTEN MATERIALS; THEIR USABILITY, CONDITION, OR OPERATION; THEIR MERCHANTABILITY; THEIR FITNESS FOR ANY PARTICULAR PURPOSE; OR NON-INFRINGEMENT OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS. TOKENEX DOES NOT WARRANT THAT THE ACCOUNT UPDATER SERVICE WILL ALWAYS BE AVAILABLE, ACCESSIBLE, UNINTERRUPTED, TIMELY, SECURE, FREE OF BUGS OR VIRUSES OR OTHER DEFECTS, OPERATE WITHOUT ERROR, OR WILL CONTAIN ANY PARTICULAR FEATURES OR FUNCTIONALITY.

IN NO EVENT WILL TOKENEX BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF INCOME, USE, OR INFORMATION, NOR ANY OTHER COST OR EXPENSE INCURRED BY CUSTOMER OR ANY THIRD PARTY ARISING FROM OR RELATED TO USE OR RECEIPT OF THE ACCOUNT UPDATER SERVICE, WHETHER IN AN ACTION IN CONTRACT OR IN TORT, AND EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. CUSTOMER ASSUMES THE ENTIRE RISK OF USE OR RECEIPT OF THE ACCOUNT UPDATER SERVICE AND CONFIDENTIAL INFORMATION.

If the limitation of liability set forth in the immediately preceding paragraph is deemed by a court of competent jurisdiction to be contrary to applicable law, the total liability, in the aggregate, of TokenEx to Customer and anyone claiming by or through the Customer, for any claims, losses, costs, or damages, including attorneys' fees and costs, fees and expenses of any nature whatsoever resulting from or in any way related to the Account Updater Service shall not exceed the total compensation received by TokenEx from the Customer for the use of the Account Updater Product Service during the six months ending on the date that TokenEx was advised by the Customer of the concern. It is intended that this limitation apply to any and all liability or cause of action however alleged or arising, to the fullest extent permitted by law.

9) MISCELLANEOUS

- a) All other terms of the Agreement not expressly modified in This Account Updater Terms remain unaltered and in full effect. The parties agree that the Service Level Agreement referenced in the Master Services Agreement is applicable to the portion of the Account Updater Service within the control of TokenEx and does not apply to service availability of third parties including but not limited to an acquirer or Visa.
- b) In the event of a conflict between the Master Services Agreement, the terms of any previous addendums, amendments, proposals, or change orders, and the terms of this Account Updater Terms shall prevail.

Bin Look Up Product Terms

Bin Look Up is powered by Pagos. If Customer is purchasing this service, Customer agrees and acknowledges that TokenEx shall provide Customer name, Order Tier and dates of proposed subscription to Pagos who will, in turn, share this information with their credit card networks.

Fraud Services Product Terms

Fraud Product Services are powered by Kount, Inc. ("Kount"). Fraud Product Services are provided by TokenEx to assist Customer with electronic commerce services including, but not limited to, risk control management and fraud screening. Use, licensing and provision of Fraud Product Services functionality is provided via the TokenEx Platform and is subject to the following terms:

1. Definitions. In addition to the defined terms otherwise set forth in the Agreement, the following terms as used in these Terms have the meanings set forth below:

- a) "**Cardholder Data**" shall have the same meaning as defined by the Payment Card Industry (PCI) Data Security Standards Glossary, Abbreviations and Acronyms, found at https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary_v1-1.pdf, as updated from time to time.

- b) **“Customer Communications”** means the data exchanged between Customer and Kount, or TokenEx and Kount, associated with provision of the Fraud Services, which may include Personal Data.
- c) **“Digest Form”** means any hashed or encoded representations of Personal Data that have been aggregated and/or anonymized so that the individual to which it relates can no longer be identified and that cannot be reversed or otherwise manipulated to become Personal Data.
- d) **“Indications”** means output returned from use of the Fraud Services, including the scores, flags, reason codes, reports, risk control opinions, authorization codes, report information and similar results.
- e) **“Laws”** means all applicable international, federal, state, and local statutes, rules, directives, regulations, and ordinances.
- f) **“Operation”** means each tokenization, detokenization, encryption, batch action, API call, or any other action performed by the Platform.
- g) **“Personal Data”** means: (a) any personally identifiable information (including, without limitation, Cardholder Data) disclosed or otherwise provided to Kount or TokenEx that, if compromised, could result in identity theft, or (b) any more restrictive definition required by any Laws.
- h) **“RIS Update”** means updated transaction information transmitted to Kount through the Risk Inquiry System, which includes all data elements specified in the Kount Technical Specifications Guide.
- i) **“Risk Inquiry”** means any transaction initiated by TokenEx or Customer in which the Risk Inquiry System is queried, including, but not limited to, for the purposes of obtaining an authorization code or risk control opinion.
- j) **“Risk Inquiry System”** means the primary Kount technical interface through which Risk Inquiries and RIS Updates are initiated, and through which Kount delivers an authorization code or risk control opinion as part of the Fraud Services.
- k) **“Security Incident”** means any unauthorized access to or use, alteration or disclosure of Cardholder Data or other Personal Data or a similar event under Laws that require notification to authorities or individuals.

1. Use of Fraud Product Services.

- a) A merchant identifier issued by Kount (“MID”) is required for use of Fraud Product Services and the parties agree that the TokenEx MID will be provided as part of Fraud Product Services. Customer will incur a charge for each Fraud Product Services-specific API call but such Fraud Product Services-specific API call will not be additionally included in Customer's general monthly operations count. Customer remains responsible for separately paying any networks' fees charged in connection with each Risk Inquiry submission. Additionally, upgrades of the Fraud Product Services, e.g., a new version or enhancement offering that incorporates significant additional or improved features, may be subject to additional fees.
- b) Customer represents it will use the Fraud Product Services only for the purpose permitted under and as set forth in these terms and otherwise in the Agreement. Fraud Product Services are provided and made available for Customer's non-transferable, non-exclusive use, without right to sub-license. Customer agrees not to remove any copyright or other proprietary notices on or in the Fraud Services. No right, title, or interest in the Fraud Services or any intellectual property rights in the Fraud Product Services is transferred to Customer.

2. Customer Consent.

- a) Customer agrees that provision of the Fraud Product Services requires that Customer provide the required Customer Communications and requires access by the Kount Risk Inquiry System to the contents of Customer Communications.

Customer expressly consents and grants permission to access any Customer Communication to the extent necessary to provide the Fraud Services.

- b) Customer represents and warrants that the use, analysis and/or processing of Customer Communications to perform and/or provide the Fraud Product Services are collectively permitted under Laws and the terms of Customer's contracts with, notices to or other consents from its customers, contractors, suppliers or other third parties. Customer represents it is in compliance with Laws regarding Customer Communications and shall be solely liable for the legal adequacy of the permissibility under Laws and the legal adequacy of and means used to obtain consents required for use of the Fraud Services.

- 4. **Cardholder Data.** Each party is solely responsible for the privacy and security of any and all Cardholder Data or Personal Data any time that the party accesses, stores, processes, transmits, or otherwise possesses such Cardholder Data or Personal Data. Any Cardholder Data submitted by Customer may be converted by Kount to Digest Form and may be retained and used for internal statistical purposes. Kount shall retain all ownership, interest, and title in and to all data converted to Digest Form so long as said information remains in Digest Form but shall only use such data for the purpose of providing fraud detection and mitigation services and for such other purposes as are expressly permitted by applicable payment card brand rules and regulations, and as permitted by Laws.

5.No Guarantee Regarding Transactions.

- a) Customer acknowledges and agrees that the Fraud Product Services do not constitute a guarantee, warranty or representation from Kount or TokenEx (a) of the identity of any individual or customer; (b) that the particular transaction is entered into by the actual authorized account holder; or (c) that the particular transaction is enforceable against the actual authorized account holder. Neither Kount nor TokenEx are liable to Customer for any reversals, refunds, fraud losses or chargebacks related to the Fraud Services.
- b) Indications provided to Customer as part of Fraud Product Services represent a combination of factors that refer to a customer's possible identity that is derived, in part, from the input information submitted to the Fraud Product Services. Indications do not constitute consumer reports as defined within the Fair Credit Reporting Act or credit references. Further, Indications are only to be used in relation to determining the likelihood of a customer's identity and not in any determination of a customer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living. Customer agrees that Indications are only one factor the Customer may consider and that the Indications are intended to enhance, not replace, Customer's risk control procedures. Customer agrees that it will not rely solely on the Indications to control fraud and that it will validate Indications as required by Laws.
- c) Neither Kount nor TokenEx shall have an obligation under this Agreement to provide duplicate copies or maintain any archive of the Indications. Further, Customer acknowledges that certain Fraud Product Services are dependent on the facilities, networks and connectivity of mobile number operators, governmental entities and other third parties. It is possible that the Fraud Product Services may be suspended or terminated if access to mobile number operator

services or other third-party data are interrupted or become unavailable for any reason. Endeavors will be made to provide advance notice, but Customer acknowledges that advance notice is not always possible.

4. Security Incident.

- a)** If a party discovers or otherwise becomes aware of Security Incident, that party shall (a) promptly notify the other party in writing of the Security Incident, subject to any reasonable restrictions placed on such party by any law enforcement agency in the process of conducting an investigation relating thereto; and (b) take reasonable steps to repair and/or remedy the causes of such Security Incident.
- b)** As may be required by PCI-DSS obligations or other card brand requirements, in the event that a party discovers a Security Incident that has resulted in unauthorized access to or use, alteration or disclosure of Cardholder Data, that party agrees to allow card associations (Visa, MasterCard, American Express, or Discover), or designated representatives of a card association, reasonable access during that party's normal business hours to that party's facilities where the Cardholder Data is stored to ensure that such party is complying with its obligations with respect to Cardholder Data. Furthermore, in the event of a known or suspected Security Incident of either party's systems, such party is responsible to determine if a Security Incident has occurred and to the extent any forensics investigation or audit is required by PCI-DSS or other card brand requirements, such party shall be responsible for any costs or expenses associated with such investigation or audit, and any fees, fines, or penalties that may be imposed with respect to such party's actions. In addition, to the extent that any required forensics investigation or audit determines that a Security Incident occurred, such that data was accessed, altered, taken, disclosed or lost by or from a party, its networks, systems, employees, agents, or third party service providers, such party shall be responsible for any actual direct costs, damages, expenses, or losses of third parties or incurred by either party to third parties that may result from such Security Incident (including, without limitation, actual fraud losses, account monitoring expenses, or card reissuance expenses). Neither party will have any liability for any indirect or consequential damages or any lost profits, lost business opportunities or damage to the business reputation of the other party arising from any unauthorized access to Cardholder Data by, or disclosure of Cardholder Data to, any third party.

5. Suspension or Termination of Fraud Services.

- a)** Notwithstanding anything to the contrary in the Master Service Agreement, Fraud Product Services may be terminated by Customer if a Force Majeure Event preventing delivery of the Fraud Services continues for a period of sixty (60) days or longer.
- b)** Fraud Product Services may be suspended immediately: (i) in the event of a Security Incident originating in Customer's systems, until such time as Customer is able to certify to Kount, in Kount's reasonable discretion, that the causes of such Security Incident have been remedied in full; or (ii) if Customer fails to timely pay any invoice for Fraud Product Services. If Fraud Product Services are suspended pursuant to (i) above and the remedy of causes of the Security Incident is not certified within a reasonable time, provision of Fraud Product Services to Customer may be terminated upon written notice. To the extent a Security Incident originates in a Customer system and Fraud Product Services are suspended or

terminated for all TokenEx customers as a result, Customer agrees to defend, indemnify and hold harmless TokenEx from and against any third-party Claim based on such Security Incident.

6. Survival. The obligations of the parties required by Laws hereunder survive termination of this Agreement

7. Limitation of Liability.

- a) EXCEPT FOR AN INDEMNIFICATION OBLIGATION RELATING TO FRAUD SERVICES, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY OR ANY OTHER PERSON FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING LOSS OF PROFIT OR GOODWILL, FOR ANY MATTER ARISING OUT OF OR RELATING TO THIS FRAUD PRODUCT SERVICES TERMS , WHETHER SUCH LIABILITY IS ASSERTED ON THE BASIS OF CONTRACT, TORT OR OTHERWISE EVEN IF EITHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR A PARTY'S INDEMNIFICATION OBLIGATIONS RELATING TO FRAUD SERVICES, IN NO EVENT WILL A PARTY'S TOTAL LIABILITY FOR ANY AND ALL DAMAGES ARISING UNDER THIS AGREEMENT FOR THE FRAUD PRODUCT SERVICES FROM ALL CAUSES OF ACTION AND UNDER ALL THEORIES OF LIABILITY EXCEED U.S. \$250,000. NOTWITHSTANDING THE FOREGOING, THE PARTIES' LIABILITY FOR INDEMNIFICATION OBLIGATIONS WILL NOT EXCEED FIVE MILLION U.S DOLLARS (\$5,000,000.00). THE PARTIES AGREE THAT THESE LIMITATIONS SURVIVE TERMINATION OF THE AGREEMENT AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THE AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.
- b) SUBJECT TO AND EXCLUSIVE OF ANY TOKENEX OBLIGATION FOR INDEMNITY RELATING TO FRAUD PRODUCT SERVICES, CUSTOMER ASSUMES TOTAL RESPONSIBILITY FOR USE OF THE FRAUD SERVICES, INDICATIONS, AND USES THE SAME AT ITS OWN RISK. NEITHER KOUNT NOR TOKENEX EXERCISE CONTROL OVER AND HAVE ANY RESPONSIBILITY WHATSOEVER FOR ANY REFUNDS, REVERSALS, FRAUD LOSSES, CHARGEBACKS, OR FRAUDULENT ACCESS TO A USER ACCOUNT IN CONNECTION WITH THE TRANSACTIONS UNDER THESE TERMS OR FOR CUSTOMER ACTIONS OR INACTIONS IN CONNECTION WITH USE OF THE FRAUD SERVICES OR WHEN THE FRAUD SERVICES MAY BE UNAVAILABLE. FRAUD PRODUCT SERVICES DO NOT GUARANTEE THAT A PARTICULAR TRANSACTION IS ENTERED INTO BY THE AUTHORIZED ACCOUNT HOLDER OR IS ENFORCEABLE AGAINST THE AUTHORIZED ACCOUNT HOLDER. NEITHER KOUNT NOR TOKENEX MAKE ANY REPRESENTATIONS OR WARRANTIES—EXPRESS OR IMPLIED—REGARDING THE RISK INQUIRY SYSTEM OR THE FRAUD SERVICES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, DATA ACCURACY, OR THAT THE FRAUD SERVICES WILL BE UNINTERRUPTED OR ERROR FREE, OR ANY WARRANTY BASED ON USAGE OF TRADE, COURSE OF PERFORMANCE OR COURSE OF DEALING AND ALL SUCH WARRANTIES ARE HEREBY DISCLAIMED BY KOUNT AND TOKENEX AND ARE WAIVED BY CUSTOMER TO THE EXTENT NOT PROHIBITED BY LAWS.