

**PAYMENTECH, LLC  
AMENDMENT TO  
SELECT GOVERNMENT MERCHANT PAYMENT INSTRUMENT PROCESSING AGREEMENT**

**MERCHANT NAME: Fort Bend County**

This Amendment to the Select Government Merchant Payment Instrument Processing Agreement (the "Amendment") is dated as of the date last signed below (the "Effective Date") and is attached to and forms a part of that certain Select Government Merchant Payment Instrument Processing Agreement dated as of the Effective Date of the Agreement, as may have been amended, between Paymentech, LLC, (or its predecessor in interest) for itself and on behalf of JPMorgan Chase Bank, N.A. a national banking association ("Member"), and the Merchant(s) whose signature(s) appear below (collectively referred to as "Merchants") (the "Agreement"). Terms not otherwise defined herein have the meanings set forth in the Agreement. To the extent that any conflict or inconsistency exists between the terms of this Amendment and the Agreement, the terms of this Amendment will control.

**1. NEW PRICING.**

Your pricing shall be modified in accordance with the selection below:

- The fees for one or more of the services specified on your pricing schedule shall be modified in accordance with the following table. Only the fees described in "Description of Service" below are hereby added to reflect the fees. All other fees in the existing Schedule A shall continue in full force and effect and are unchanged by this Amendment.

| Description of Service              | Fee:    |
|-------------------------------------|---------|
| Safetech Encryption Item (Verifone) | \$0.025 |

If Merchant obtains point of sale device(s) from Paymentech or a third party for use with Safetech Encryption and Paymentech or the third party provides the encryption services, additional fees shall be assessed: (a) a one-time device fee of \$10.90 per device; and (b) an encryption injection fee of \$34.95 per device per occurrence. These assessments are in addition to the above Safetech Encryption Fee(s).

If Merchant obtains point of sale device(s) from Verifone directly and Verifone provides the Safetech Verifone Point Enterprise Solution encryption injection to the devices, then the above one time device fee(s) and injection fee(s) will not apply. Merchant acknowledges and understands that its use of any fraud mitigation or security enhancement solution (e.g. an encryption product or service), whether provided to merchant by Paymentech, Verifone or a third party, in no way limits Merchant's obligation to comply with the Security Standards or Merchant's liabilities set forth in the Agreement.

**2. 12. NO DISCLOSURE OF CUSTOMER INFORMATION:**

Section 12 of the Agreement is hereby amended to read in its entirety as follows:

**12. TRANSACTION DATA AND PAYMENT INSTRUMENT INFORMATION; PAYMENT CARD INDUSTRY COMPLIANCE.**

**12.1** Merchant financial information, information related to Merchant's Transactions, and other information that Merchant provides to Paymentech may be shared by Paymentech with its affiliates and the Payment Brands. Paymentech will not otherwise disclose or use such information other than (a) as necessary to process Merchant's Transactions or otherwise provide services and maintain Merchant's account pursuant to this Agreement; (b) to detect, prevent, reduce, or otherwise address fraud, security, or technical issues; (c) to enhance or improve Paymentech's products and services generally; or (d) as required or permitted by the Payment Brands or applicable law. Paymentech may prepare, use, and/or share with third parties, aggregated, non-personally identifiable information derived from Transaction Data of all of Paymentech's customers or specific segments of Paymentech's customers.

**12.2 Payment Card Industry Compliance.** Merchant acknowledges and understands the importance of compliance with the Security Standards, such as those relating to the storage and disclosure of Transaction Data and Payment Instrument Information. Therefore, Merchant shall not disclose or use Payment Instrument Information, other than (a) to Merchant's agents and contractors for the purpose of assisting Merchant in completing a Transaction; (b) to the applicable Payment Brand; or (c) as specifically required by law or pursuant to a government or regulatory demand. Furthermore, Merchant acknowledges and understands that its use of any fraud mitigation or security enhancement solution (e.g. an encryption product or service), whether provided to Merchant by Paymentech or a third party, in no way limits Merchant's obligation to comply with the Security Standards or Merchant's liabilities set forth in this Agreement.

Merchant is allowed by the Payment Brand Rules to store only certain Payment Instrument Information (currently limited to the Customer's name, Payment Instrument account number, and expiration date) and is prohibited from storing additional Payment Instrument Information, including, without limitation, any security code data, such as CVV2, CVC2, and PIN data, and any magnetic stripe track data. Merchant shall store all media containing Payment Instrument Information in an unreadable format wherever it is stored and in an area limited to selected personnel on a "need to know" basis only. Prior to either party discarding any material containing Payment Instrument Information, the party will render the account numbers unreadable in accordance with the requirements of the Security Standards. If at any time Merchant determines or suspects that Payment Instrument Information has been compromised Merchant must notify Paymentech immediately and assist in providing notification to such parties as may be required by law or Payment Brand Rules, or as Paymentech otherwise reasonably deems necessary.

Merchant agrees to comply with all Security Standards, as defined herein. Merchant further agrees to provide Paymentech, upon its request, with such tests, scans, and assessments of Merchant's compliance with Security Standards as may from time to time be required by the Payment Brands.

Merchant must immediately notify Paymentech of its use of any Service Provider. Merchant shall ensure that, to the extent required by each Payment Brand, its Service Providers are (d) compliant with all applicable Security Standards; and (e) appropriately registered with, or otherwise recognized as being compliant with the Security Standards, by all applicable Payment Brands. To the extent required by each Payment Brand, all Payment Applications, or software involved in processing, storing, receiving, or transmitting of Payment Instrument Information, shall be (f) compliant with all Security Standards applicable to such Payment Applications or software; and (g) registered with and/or recognized by such Payment Brand(s) as being so compliant. Furthermore, to the extent Merchant is required under the Payment Brand Rules, or Merchant otherwise elects, to utilize EMV chip-capable terminals, all EMV chip-capable terminals used by Merchant must appear on the EMV co-approved terminal list maintained by the Payment Brands.

Merchant understands that its failure, or the failure of any of its Service Providers, to comply with the Payment Brand Rules, including the Security Standards, or the compromise of any of Payment Instrument Information (whether such Payment Instrument Information is under the control of Merchant or its Service Provider), may result in assessments, fines, and/or penalties by the Payment Brands, and Merchant agrees to indemnify and reimburse Paymentech immediately for any such assessment, fine, or penalty imposed on Paymentech or the Member and any related loss, cost, or expense incurred by Paymentech or the Member. If any Payment Brand requires a forensic examination of Merchant or any of Merchant's Service Providers due to a Data Compromise Event, Merchant agrees to cooperate with, and cause all applicable Service Providers to cooperate with, such forensic examination until it is completed, including, without limitation, the engagement of an examiner acceptable to the relevant Payment Brand. Notwithstanding the foregoing, the Payment Brands may (h) directly engage, or demand that Paymentech engage, an examiner on behalf of the Merchant in order to expedite the investigation of the Data Compromise Event; or (i) pursuant to the Payment Brand Rules, permit Paymentech to investigate the Data Compromise Event. In either scenario, Merchant agrees to pay for all costs and expenses related to such forensic examination, including all of Paymentech's reasonable attorneys' fees and other costs relating to such forensic examination.

By executing this Agreement, Merchant represents that, in the event of its failure, including bankruptcy, insolvency, or other suspension of business operations, Merchant shall not sell, transfer, or disclose to third parties any materials that contain Transaction Data or Payment Instrument Information. Upon request, Merchant must return such information to Paymentech or provide Paymentech with acceptable proof of its destruction.

*As they are used in Section 12 of the Agreement, the following terms are hereby defined.*

**"Customer"** means the person or entity to whom a Payment Instrument is issued or who is otherwise authorized to use a Payment Instrument.

**"Data Compromise Event"** means an occurrence that results, or could result, directly or indirectly, in the unauthorized access to or disclosure of Transaction Data and/or Payment Instrument Information.

**"EMV"** means Europay, MasterCard and Visa.

**"Merchant"** means the legal entity identified in the Application and on the first and signature pages of this Agreement.

**"Member"** means The Bank of Nova Scotia and JPMorgan Chase Bank, N.A. or other entity providing sponsorship to Paymentech as required by all applicable Payment Brands. Member is a principal party to this Agreement and Merchant's acceptance of Payment Brand products is extended by the Member.

**"Payment Application"** means a third party application used by merchant that is involved in the authorization or settlement of Transaction Data.

**"Payment Brand"** means any payment method provider whose payment method is accepted by Paymentech for processing, including, without limitation, Visa Inc., MasterCard International, Inc., Discover Financial Services, LLC, Interac, Acxsys Corporation, and other credit and debit card providers, debit network providers, gift card, and other stored value and loyalty program providers. Payment Brand also includes the Payment Card Industry Security Standards Council.

**"Payment Brand Rules"** means all bylaws, rules, programs, regulations, specifications, and manuals, as they exist from time to time, of the Payment Brands.

**"Payment Instrument"** or **"Payment Card"** means an account, or evidence of an account, authorized and established between a Customer and a Payment Brand, or representatives or members of a Payment Brand that Merchant accepts from Customers as payment for a good or service. Payment Instruments include, but are not limited to, credit and debit cards, stored value cards, loyalty cards, electronic gift cards, authorized account or access numbers, paper certificates, and credit accounts. Use of the term Payment Instrument or Payment Card throughout this Agreement includes any Payment Instrument with an embedded microcomputer EMV chip.

**PAYMENTECH, LLC  
AMENDMENT TO  
SELECT GOVERNMENT MERCHANT PAYMENT INSTRUMENT PROCESSING AGREEMENT**

**MERCHANT NAME: Fort Bend County**

“**Payment Instrument Information**” means information related to a Customer or the Customer’s Payment Instrument, that is obtained by Merchant from the Customer’s Payment Instrument, or from the Customer in connection with his or her use of a Payment Instrument (e.g., a security code, a PIN number, credit limits, account balances, or the customer’s zip code when provided as part of an address verification system). Without limiting the foregoing, such information may include a the Payment Instrument account number and expiration date, the Customer’s name or date of birth, PIN data, security code data (such as CVV2 and CVC2), and any data read, scanned, imprinted, or otherwise obtained from the Payment Instrument, whether printed thereon, or magnetically, electronically, or otherwise stored thereon. For the avoidance of doubt, the data elements that constitute Payment Instrument Information shall be treated according to their corresponding meanings as “cardholder data” and “sensitive authentication data” as such terms are used in the then current PCI DSS.

“**Paymentech**” or “**Chase Paymentech**” means Paymentech, LLC, a Delaware limited liability company, having its principal office at 8181 Communications Parkway, Plano, Texas 75024.

“**Security Standards**” means all rules, regulations, standards, or guidelines adopted or required by the Payment Brands or the Payment Card Industry Security Standards Council relating to privacy, data security, and the safeguarding, disclosure, and handling of Payment Instrument Information, including, without limitation, the Payment Card Industry Data Security Standards (“PCI DSS”), Visa’s Cardholder Information Security Program (“CISP”), Discover’s Information Security & Compliance Program (“DISC”), American Express’s Data Security Operating Policy, MasterCard’s Site Data Protection Program (“SDP”), Visa’s Payment Application Best Practices (“PABP”), the Payment Card Industry’s Payment Application Data Security Standard (“PA DSS”), MasterCard’s POS Terminal Security program, and the Payment Card Industry PIN Transmission Security program (“PCI PTS”), in each case as they may be amended from time to time.

“**Service Provider**” means any party that processes, stores, receives, transmits, or has access to Payment Instrument Information on Merchant’s behalf, including, without limitation, its agents, business partners, contractors, and subcontractors.

“**Transaction**” means a transaction conducted between a Customer and Merchant utilizing a Payment Instrument in which consideration is exchanged between the Customer and Merchant.

“**Transaction Data**” means the written or electronic record of a Transaction, including, without limitation, an authorization code or settlement record, which is submitted to Paymentech.

**3. MISCELLANEOUS:**

The following language shall be added to Section 15 of the Agreement as sub-section 15.14 and 15.15:

**15.14 Merchant Taxpayer Certification and Paymentech Reporting Obligations.** Pursuant to 26 USC 6050W, Paymentech is a “payment settlement entity”, obligated to collect and report certain taxpayer information to the United States Internal Revenue Service. Therefore, in conjunction with the execution of this Agreement, Merchant shall provide Paymentech with the appropriate taxpayer certification documentation, via Internal Revenue Service (IRS) Form W-9 (or the appropriate versions of Form W-8, if applicable). Merchant shall promptly notify Paymentech if there are any changes in this information. Paymentech may deduct withholding taxes, if any, from proceeds payable to Merchant or any entity that is a party to this agreement where required under Applicable Law. Paymentech may, in accordance with Applicable Law and from time to time during the term of this Agreement, request Merchant to recertify its taxpayer certification hereunder. Furthermore, Merchant shall be responsible for any penalties related to the reporting obligations of Paymentech hereunder.

**15.15 Required Clauses for Texas Governmental Entity Contracts.** As required by Chapter 2270, Government Code, Paymentech hereby verifies that it does not boycott Israel and will not boycott Israel through the term of this Agreement. For purposes of this verification, “boycott Israel” means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes. By signature below, Paymentech represents pursuant to Section 2252.152 of the Texas Government Code, that Paymentech is not listed on the website of the Comptroller of the State of Texas concerning the listing of companies that are identified under Section 806.051, Section 807.051 or Section 2253.153.

**4. CONTINUED EFFECT:** Except to the extent amended hereby, all terms, provisions and conditions of the Agreement are hereby ratified and shall continue in full force and effect and the Agreement shall remain enforceable and binding in accordance with its terms.

*[Signature Page Follows]*

**PAYMENTECH, LLC  
AMENDMENT TO  
SELECT GOVERNMENT MERCHANT PAYMENT INSTRUMENT PROCESSING AGREEMENT**

**MERCHANT NAME: Fort Bend County**

**This Amendment shall be effective on the Effective Date.**

**Agreed and Accepted by:**

Fort Bend County

MERCHANT LEGAL NAME (Print or Type)

301 Jackson, Richmond, TX 77469

Address (Print or Type)

By (authorized signature)

By, Name, Title (Print or Type)

Date

**Agreed and Accepted by:**

PAYMENTECH, LLC for itself and on behalf of  
JPMORGAN CHASE BANK, N.A.

By: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Address: 8181 Communications Pkwy, Plano, TX 75024

**AUDITOR'S CERTIFICATE**

I hereby certify that funds in the amount of \$\_\_\_\_\_ are available to pay the obligation of Fort Bend County within the foregoing Agreement.

\_\_\_\_\_  
Robert Ed Sturdivant, County Auditor