

PINACLE® Merchant Gateway

PINACLE® Merchant Gateway (“PINACLE Merchant Gateway”) is an online web-based application within PINACLE with various merchant tools and features that Customer can utilize in connection with various compatible payment processing and related services Customer receives from Bank and/or Bank’s affiliates.

Definitions. Capitalized terms used but not otherwise defined throughout this Service Schedule shall have the meanings prescribed below or otherwise in the Agreement.

- “Card” means a credit, debit, charge, purchase, or virtual card or any other card-based or Payment Network-based payment instrument.
- “Network Rules” means the applicable rules, regulations, policies, releases, procedures, interpretations and other requirements (whether contractual or otherwise) imposed, promulgated, or adopted by any Payment Network, the PCI Security Standards Council, LLC, the National Automated Clearing House Association, the Special Interest Group for IIAS Standards, Inc., and/or related authorities.
- “Payment Network” means any entity formed to administer and promote Cards, including without limitation Visa U.S.A., Inc. (“Visa”), Mastercard Worldwide (“Mastercard”), DFS Services LLC (“Discover”), PayPal, Inc. (“PayPal”), American Express Company, Inc. (“American Express”), and any applicable debit networks.

PNC Rights & Obligations

- PNC will make PINACLE Merchant Gateway available to Customer
- PINACLE administrators may authorize and de-authorize Customer’s use of the PINACLE Merchant Gateway or any of its features and may require PINACLE operator credentials to be used for access to the PINACLE Merchant Gateway and/or certain features thereof.
- PNC will update the Service and documentation from time to time and may add, modify, or remove any tools, features, or functionality. PNC will provide notice to the customer in the event of material changes, additions, or removal of functionality from the Service.

Customer Obligations

- Services provided by PNC to Customer under the Agreement include PINACLE Online and Mobile Platform Service, which is considered a Dependent Solution (defined below) for the PINACLE Merchant Gateway.
- Customer must use its PINACLE access credentials to access the PINACLE Merchant Gateway.
- Customer must follow the procedures provided by PNC in connection with implementing, accessing, operating, or otherwise using the PINACLE Merchant Gateway.
- The PINACLE Merchant Gateway must only be used for Customer’s bona fide commercial purpose and in a manner consistent with this Service Schedule and the Agreement
- Customer is exclusively responsible for compliance with all laws and Network Rules applicable to Customer and Customer’s use of PINACLE Merchant Gateway.
- Customer is exclusively responsible to obtain consents necessary or required under any applicable laws or Network Rules from its cardholder customers with respect to any information which may be shared with PNC, including specifically the consent to share, store, and/or maintain cardholder data, Customer Information, and/or other personally identifying information. In addition, Customer is responsible for the accuracy, quality, and legality of and the means by which Customer acquired such data, information, and consents.
- Customer is exclusively responsible for Customer’s collection, storage, and/or transmission of any cardholder data, personally identifying information, or other sensitive data in connection with Customer’s use of PINACLE Merchant Gateway.
- Customer agrees not to enter Personally Identifiable Information (PII) or Protected Health Information (PHI) into open text fields.

Dependent Solutions. Certain products or services may be required for certain tools, features, or functionality of the PINACLE Merchant Gateway to be successfully implemented and/or provided to Customer (“Dependent Solution”). Should a Dependent Solution not be obtained by Customer or if later terminated, expired, or otherwise be inactivated for any reason, Customer’s ability to use certain tools, features, or functionality or otherwise receive the PINACLE Merchant Gateway may be impacted without notice and PNC shall no longer be obligated to provide the PINACLE Merchant Gateway to Customer. Further, should a Dependent Solution be unavailable for any reason, Customer’s ability to use and/or access the PINACLE Merchant Gateway, or certain tools, features, or functionality thereof, may be impacted until availability of the Dependent Solution is restored.

Impermissible Use. PNC shall have no responsibility or liability arising out of any of the following, (each an “Impermissible Use”): (i) Customer’s use of PINACLE Merchant Gateway (or any feature or portion thereof) in any manner not expressly permitted under this Service Schedule or the Agreement, including Customer’s failure to use PINACLE Merchant Gateway in compliance with all applicable laws and Network Rules; (ii) for any activity other than Customer’s legitimate business purpose, including for any fraudulent or illegal purpose; (iii) Customer’s independent assembly, configuration, or modification of PINACLE Merchant Gateway (or any element, step, component, process, system, or portion thereof) or using PINACLE Merchant Gateway in combination with other products, services, methods or systems (including software or equipment) in a manner or method not previously disclosed and approved by PNC in writing, and (iv) any changes of PINACLE Merchant Gateway done by Customer, any third party used by Customer or otherwise. For clarity, changes, updates, or other modifications done by or otherwise required by PNC is not considered an Impermissible Use under this paragraph.

PINACLE Merchant Gateway Tools: Currently, the tools and their associated features available through PINACLE Merchant Gateway include the following:

- A. PINACLE Virtual Terminal. PINACLE Virtual Terminal (“Virtual Terminal”) is a web-based software application tool within PINACLE Merchant Gateway which enables Customer to accept Card payments from its cardholder-customers by Customer manually keying the Card data into the Virtual Terminal platform, together with related features.

Features and functionality of Virtual Terminal:

- Supports both sale transactions and refund/credit transactions.
- Customer can initiate pre-authorization(s), convert preauthorization(s) to sale transactions, and manage pending authorizations.
- Fields for Customer to include necessary information for inclusion on its transaction receipts together with receipt generation for Customer to provide transaction receipts to cardholders associated with each sale or refund transaction.
- Charge-again capacity for Customer to use stored tokens issued by Tempus to initiate sale or refund transactions or pre-authorizations.
- Customer can search Customer Profiles and select one of the Stored Credentials in the Customer Profile eWallet to initiate sale or refund transactions or pre-authorizations.
- Customer can designate a Card in a Customer Profile eWallet as the default Card to use for current and future Card transactions.
- Customer can retrieve transaction data to display and further search, filter and sort such data or generate reporting for download.
- Transaction data, including reversals, credits, void credits, authorizations, and forced authorizations for the most recent 24 months is available to be displayed.

B. Virtual Terminal Dependent Solutions. The following are each a Dependent Solution for Virtual Terminal:

- Payment gateway and tokenization services being provided to Customer by Tempus Technologies, Inc. (“Tempus”) a wholly owned subsidiary of PNC, pursuant to a separate agreement between Tempus and Customer;
- Card processing and related services being provided to Customer by PNC Merchant Services Company (“PNCMS”) pursuant to a separate agreement between Customer and PNCMS.;
- An electric or other power connection together with internet network or other telecommunication carrier connection and access with adequate bandwidth capacity;

PNC Obligations for Virtual Terminal. In addition to PNC's obligations for the PINACLE Merchant Gateway, PNC will initiate the transfer of transaction data and other necessary information associated with Customer's payment transactions initiated through Virtual Terminal to Tempus.

Customer Obligations for Virtual Terminal. In addition to Customer's obligations for the PINACLE Merchant Gateway, Customer has the following additional obligations when using Virtual Terminal:

- Customer is responsible for providing transaction receipts to its cardholder customers.
- Customer agrees it will not use the Virtual Terminal for purposes of accepting Card payment in exchange for any of the following goods or services: - healthcare, firearms, tobacco, pharmaceuticals.
- Customer is responsible for the accuracy of all data entered by Customer into Virtual Terminal, including calculating taxes, line-item descriptions, customer codes, invoice details, prices, Card data, postal codes, etc.
- Customer acknowledges that any pending authorizations or pre-authorizations conducted through Virtual Terminal which are not converted to a sale or otherwise reversed through Virtual Terminal in the time frames permitted under Network Rules may result in fees, fines, or other assessments against Customer.
- Customer acknowledges that Virtual Terminal does not process or manage chargeback or disputed transactions
- For Virtual Wallet transactions using a Stored Credential in a Customer Profile or eWallet, Customer must:
 - Before the first transaction occurs using a Stored Credential, Customer must either submit an authorization request for the transaction amount or if payment is not required, submit an account verification. If the initial authorization request or account verification is not approved, Customer must not store the Card as a Stored Credential, including as part of a Customer Profile or eWallet.
 - Before processing transaction initiated by the Card owner, Customer must validate the identity of the Card owner.
 - The authorization amount must not exceed the individual transaction amount.
 - If an authorization request for a transaction initiated by the Card owner using a Stored Credential is declined, the Customer must notify the Card owner in writing and allow at least 7 calendar days to pay by other means.

C. Customer Profiles and eWallet. Customer can create, configure, and manage information about their customers (each a “Customer Profile”) within PINACLE Merchant Gateway. Customer may elect to include Card data of its customers (each a “Stored Credential”), in the Customer Profile associated with such customer for use in connection with future payment transactions between Customer and its customer (“eWallet”).

Features and functionality of Customer Profiles and eWallet:

- Customer can add, modify, and/or remove a Customer Profile
 - Various personal and company demographic data fields are available for Customer to populate in each Customer Profile, including name, email address, mailing address, phone number, and unique customer identifier ("Reference ID") associated with the customers and individual Card owners.
 - Search all Customer Profiles by to return only Customer Profiles with resulting matches, including by name, email, or Reference ID. Create, Update, and Delete options are available to Customer to manage and maintain each Customer Profile
 - Customer can store up to 5 Stored Credentials in the eWallet per Customer Profile and designate one as the default card, which will be used for current and future Card transactions using Virtual Wallet Customer can update this information for any existing Card stored in the eWallet of a Customer Profile: Cardholder Name, Zip Code, Expiration Date.
- D. Customer Obligations for Customer Profile and eWallet. In addition to Customer's obligations for the PINACLE Merchant Gateway, Customer has the following additional obligations when using Customer Profile and/or eWallet.
- Customer must not store any sensitive Card information or Card data on Customer's own systems unless necessary and compliance with PCI DSS.
 - Customer is responsible for the accuracy of all data entered by Customer into the eWallet and Customer Profile, including updating or modifying such information as necessary.
 - Customer is responsible for defining and maintaining its Reference IDs. Customer agrees to not enter or upload into free form fields data related to Card account numbers, Card expiration dates, Card validation codes, Social Security numbers, individually identifiable health information or other private data.
 - By electing to use the eWallet feature to include Stored Credentials, Customer acknowledges and agrees that it will comply with all applicable laws and Network Rules regarding Stored Credentials, eWallets, and/or recurring transactions, including, but limited to:
 - Providing cardholders whose Cards are being used for Customer's payment transactions with clear and accessible customer service contact information (including an email/URL and/or phone number), Customer's refunds and returns policies, and Customer's privacy policy.
 - If Customer accepts recurring payments, Customer must provide the cardholder whose Card is being used for such recurring payment a simple and easily accessible online cancellation procedure, if end-users sign up for payments online.
 - Customer must obtain each Card owner's express informed consent through an agreement that provides all material information related to the purchase transaction; the Customer; and the terms and conditions of the Customer's storage of the Stored Credentials. Customer must retain a copy of this written agreement to the terms of the Stored Credential arrangement.
 - Customer may use a Stored Credential only as agreed with the Card owner. The agreement must include the following:
 - The account number that will be used to make payment (last four digits only).
 - How the Card owner will be notified of any changes to the agreement.
 - Transaction amount or a description of how the transaction amount will be determined.
 - The transaction currency.
 - How the Stored Credential will be used.
 - Timing and frequency of transactions. If the Stored Credential will be used for unscheduled transactions, the event that will prompt the transaction.

- The expiration date of the agreement, if applicable.
 - The length of any trial period, introductory offer, or promotional period.
- All requirements related to specific transaction types must be clearly displayed when the Card owner gives consent to Customer to create a Stored Credential and must be displayed or provided separately from the general purchase terms and conditions.
- Any recurring transaction or unscheduled transaction must not include any finance charges, interest, or imputed interest.