2017

PSP Card Services Welcome Kit

PSP
Card Services
Corporation

Dear Merchant,

We want to thank you for choosing PSP Card Services to partner with to provide you with your business needs.

Our teams work tirelessly to:

-   find the newest and most current technologies,
-   provide you with relevant information on your monthly statements that you can understand,
-   24/7 customer care and support and
-   dedication to meet the needs and requirements of your business as it grows and changes in your respective marketplace.

In your Merchant Contract, you chose to have your monthly merchant statements sent by email or mail. You also have access to your statement online, using the user name and temporary password that has been sent to you upon completion of your on-boarding with PSP Card Services.

The next step is the installation of your new terminal. Installing is easy, by connecting a phone line or ethernet wire and plugging in the AC Adaptor.

Included in your welcome kit is a terminal quick reference guide, along with information we feel you will find useful when it comes to processing payments for your business.

Should you have any questions, our staff is dedicated to your success and are happy to take your call, please reach out to our help desk at 1-844-780-9293 which provides you with 24/7/365 support to meet all your needs.

Alternatively, we invite you to check out our website www.pspcardservices.com where you can find the latest news and events of what is going on with PSP Card Services.

We look forward in working with you and connecting with you.

Best Regards,

The PSP Card Services Team
Customer Service Phone Number: 1-844-780-9293
Customer Service Phone email: support@pspcardservices.com

Contents

Customer Support Numbers

Terminal Customer Service

Phone: 1-8777.358.6797; option 2
Email: support@pspcardservices.com

Chargebacks, Security Breaches and All Other Inquiries

Customer Service Phone Number: 1-844-780-9293

Customer Service Phone email: support@pspcardservices.com

Mail: 400 Applewood Cres, Suite 200, Vaughan ON, L4K 0C3

Updates to Your Merchant Account

Should you experience changes in your business, please contact PSP Card Services so that we are made aware of these changes and update your merchant account accordingly. This ensures that there are no issues with the processing of payments to your merchant account.

Changes may include: Bank Account Information, Changes in Ownership, Tax Changes, Legal Name Change, address, phone, email change or change in preference in monthly statement preference.

Recommended Card Processing Procedures

Please review these steps with your staff, where appropriate, so that all that accept payments are aware of the required steps and security procedures to protect both the merchant and the consumer.

1. Either insert the card for the transaction or, where applicable, tap the card on the terminal.
2. Obtain authorization from the terminal.
3. If required, obtain signature on the receipt of the transaction.
4. If required, have consumer remove card from the terminal.

Card Payment Policies

Include Taxes in the Transaction Amount

Taxes need to be included in the total transaction amount to the card holder. Taxes should not be collected separately as many Card Issuers – i.e. VISA, MasterCard – must have written records of taxes paid for goods and services.

Refunds

Any returns or adjustments on behalf of a customer must be completed on the original card used in the original purchase of goods or services. Visa does not accept a cash refund to a purchase made on one of their credit or debit transactions. It is advised that cash refunds are not provided on any refunds or adjustments made on goods or services.

For Merchants that Have Tip Options – Zero Percent Tip

For debit or credit transactions, the amount entered on the terminal should be the authorized amount that has been presented to the customer.

Delivery of Goods and Services

At the time of a transaction, unless otherwise specified between the consumer and merchant, goods should be immediately delivered and/or provided to the customer. For purchases where card is not present, the purchaser must be made aware of the delivery date and expected date of delivery.

Estimated tips should not be added to a charge to a customer. A merchant must provide the consumer with a zero-percent tip option.

Best Practices – Card Payment Procedures

Identification

A merchant may ask a cardholder for Identification, however, it is not a stipulation of payment acceptance. If a card is unassigned, a merchant may ask for ID and for the purchaser to sign the card. As a merchant, you may cross reference the validity of this signature against one piece of government identification and another form of identification.

Authorization limits and Splitting a Sale

A Merchant is not authorized to split the cost of a single transaction on a single cardholder account in two or more sales receipts with the intent of avoiding authorization limits. One sales receipt per transaction, using the full transaction amount is a requirement for each sale made.

Depositing of Transaction for Invalid Merchants

Submitting transactions on behalf of a business without a valid merchant agreement is considered laundering. This is considered a form of fraud. It creates high chargeback rates and the risk of forcing a merchant out of business.

Transactions on a Merchant's Own Card

Making transactions on your own card is not allowed. A merchant should not process their own personal transactions for personal credit benefits.

Chargebacks

What is a Chargeback?

A chargeback is a reversal of a sales transaction. If a chargeback has occurred you must provide all necessary documentation to PSP Card Services within 12 business days to correctly process the chargeback. PSP Card Services issues a $25 chargeback fee is applied each time a charge back is made.

Why does a Chargeback happen?

A chargeback may occur if a customer disputes a charge on their card statement, in cases of fraud, a process error, an issue in authorization or non-fulfillment of copy requests if fraud or illegible.

How to Avoid a Chargeback?

A chargeback can be avoided at the Point of Sale with any of the following situations,

- Declined authorization. If a transaction was declined, do not repeat the request, ask the consumer for a different form of payment
- Transaction amount. Transaction amounts must match the amount presented to the consumer, do not estimate an amount, especially when it comes to adding a tip on behalf of a consumer.
- Expired card. A card is not to be accepted after it's set Expiry date, unless you have received authorization approval for the transaction.
- Card not Present. If the cardholder is present but the card is not, then do not accept the transaction. It could be fraudulent.
- Receipt. Provide your consumer with a receipt. One that is legible so the transacted amount is made clear to the consumer.

Resolving a Chargeback

The key to resolving a chargeback is providing the required information in a timely manner to rectify the situation. Documentation will be collected during the time of the chargeback. Ensure that you keep all necessary documentation when it comes to transactions and that they are properly documented, i.e. a void transaction should have a clear VOID notice on the receipt so that it is not mistakenly entered. Ensure your return, refund or cancellation policies are made clear and aware to your consumers to avoid confusion or chargeback issues.

Another key to avoid chargebacks is to ensure that all staff that are handling the processing of payments are trained and understand how and when to process transactions.

PCI Compliance

It is in the best interest of both the merchant and the consumer to ensure all necessary safeguards are in place to protect data and prevent fraud.

Any merchant that stores, processes or transmits cardholder information must meet PCI standards, regardless of merchant size or provider type.

- **Firewall.** Ensure your computer has the most current firewall installed.

- **Passwords.** Implement a password system at your company that ensures default passwords or common passwords are not used. Instead case sensitive, numerical and non-generic passwords that are harder for hackers to guess are best.

- **Protect transacted data.** Once a transaction has taken place, ensure that the data received is encrypted or unreadable.

- **Transfer encrypted data over a wireless network.** All sensitive information being transmitted over a wireless network must be encrypted to ensure it is not diverted or altered.

- **Anti-virus software.** Ensure all anti-virus software are current and running.

- **Restrict data access**. Limit those who control sensitive information. It should be on an as-needed basis for the employee's role within your organization.

- **Multiple persons, multiple user id's. If** multiple employees are accessing sensitive information, ensure a unique user ID and password is set for each of them vs. one generic user ID and password.

- **Physical data access.** Ensure that those that need to have access to data, have the appropriate controls in place so that others are unable to access the data.

- **Tracking activity.** Being able to track user activity is another key measure to limit data access.

- **Always test your security systems in place.** By constantly maintaining and updating your security systems are you able to protect yourself against the newest forms of hacking and virus'.

- **Corporate policy.** Creating a work environment that enforces a corporate policy of security and sensitivity of data promotes compliance to security standards.