FAST TRANSACT

Welcome Packet

www.fasttransact.com

FAST TRANSACT

Pay Anytime, Anywhere, Any Way.

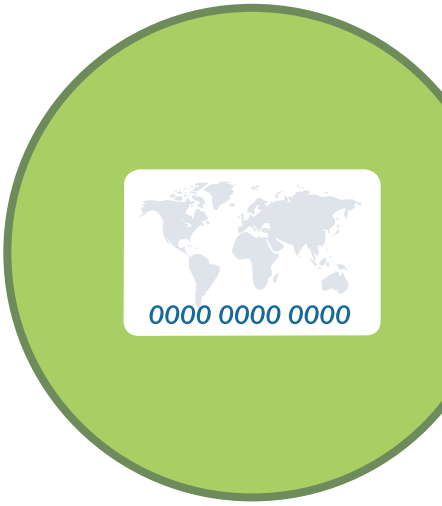
Welcome to FastTransact

It is our pleasure to extend a warm welcome to you!
Congratulations! You have joined thousands of Merchants nationwide who recognize the tremendous benefits of accepting credit cards. We are confident that you will be impressed with our prompt, friendly, knowledgeable and dedicated service to our Merchants. Please take the time to read through the welcome packet, card association operating manuals, and bank's terms and conditions. We recommend you to save them for further reference. These documents contain valuable information to assist you in the processing of credit cards.

Accepting payment cards can be as easy as taking cash.
At FastTransact, we simplify the technical and regulatory aspects of card acceptance by explaining rules and procedures clearly. Our goal is to make payment processing work seamlessly for you.

Our Welcome Kit contains:

- **Important Contacts**
- **PCI Information**
- **Card Acceptance Guidelines for Merchants**
- **Chargeback Guidelines**
- **Processing Bank Terms and Conditions**
- **Frequently Asked Questions**
- **How to Read your Statement**



Thank you for your business and welcome aboard!

FAST TRANSACT
Pay Anytime, Anywhere, Any Way.

Customer Contact Information:

Customer Service/Technical Support/Statement Questions and Supplies

FastTransact
Kirk Johnson Building – 2nd Floor
16 West King Street
Lancaster, PA 17603
800.687.8505
customerservice@fasttransact.com

Sales

FastTransact Sales
800.687.8505

Corporate Headquarters

FastTransact
11480 Commerce Park Drive
Suite 300
Reston, Virginia 20191
800.687.8505

Risk Department

risk@fasttransact.com
202.903.2610

Visit us on the web at:

http://www.fasttransact.com

Other Important Contacts:

Voice Authorization

ELAVON
Visa/MasterCard:
866.508.5855

FNBO
Visa MasterCard/AMEX:
800.228.2443

FIRST DATA/WELLS FARGO
Visa MasterCard:
800.228.1122

DISCOVER
800.347.1111

FNBO Discover
800.813.1703

AMEX
800.528.5200

Card Association

Visa:
http://usa.visa.com/business/accepting_visa/index.html

MasterCard:
https://www.mastercard.us/en-us/merchants.html

Amex:
https://www.americanexpress.com/us/content/merchant/support-services.html

Discover:
http://www.discovernetwork.com/merchants/

Frequently Asked Questions:

What does a "call message" mean?

A "call message" is an alert from your customer's bank that additional steps should be taken to receive a valid authorization message. This requires a call to the voice authorization center. *(See important contacts)*

When do I get paid for the transactions that I just entered?

Typically, clients receive payment within three business days.

Can I view my statement online?

Yes, statements are available online via login. Please contact our customer service department for login information if you did not receive it upon account approval.

What is a CVC, CVV2 or CID code?

The CVC or CVV2 code is the three digits following the signature on the back of a Visa, MasterCard or Discover Card. AMEX CID code is four numbers is located on the front of the card. This code provides an additional layer of fraud protection for card-not-present transactions.

How often will I receive a statement?

All of our customers receive a statement each month. You should except to receive your statement the first week of the month for the previous month's processing activity.

If I process cards other than Visa, Discover or MasterCard, who pays me?

Additional card types such as American Express (AMEX) are paid by the respective card issuer. These types of cards will typically show as adjustments on your statement. AMEX cards will be deposited by AMEX.

Why is Address Verification (AVS) important?

AVS verifies a card holder's billing address information on mail order, telephone order or e-commerce transactions, and provides a result code to the merchant that is separate from the authorization response code. If a fraudster has obtained a card number from a receipt or from a lost or stolen card, they will not have the billing address or postal code, and this can protect you as a merchant if you require AVS match on keyed transactions.

What Is EMV?

EMV technology comes from EMVCo, a standards organization created to facilitate worldwide interoperability and acceptance of secure payment transactions. Today there are EMV Specifications based on contact chip, contactless chip, common payment application, card personalization, and tokenization. For more information, visit: **https://www.emvco.com/**

Fraud Prevention:

According to Forbes, approximately **$190 billion in the US is lost yearly to credit card fraud**. Banks lose $11 billion and customers lose about $4.8 billion, so **merchants lose almost twenty times as much as banks**. One of the most important factors in controlling fraud is understanding the customer, and implementing security measures that can adapt to the level of risk in each transaction. However, with common sense, usage of online sources, and preventive measures, you should be able to be prevent fraud. FastTransact has listed some tips on how to keep you safe.

Point of Sales System

1. **Educate** your employees on fraud
2. **Compare** signatures and ask for identification
3. **Ask** to see the card
4. **Be wary** of customers who keep the credit card separate from their wallet
5. **Watch out** for customers who are distracting
6. **Think twice** before manually entering damaged or worn cards
7. **Do not accept** "Letters of Authorization"
8. **Take note** of what the customer is purchasing
9. **Use** the Address Verification System (AVS)
10. **Know** your POS system and equipment
11. **Keep** accurate records of credit card transactions
12. When in doubt, **call**

Card not Present

1. **Be wary** of expedited shipping when billing and shipping addresses differ
2. **Make sure** IP location and credit card address match up
3. **Watch out** for suspicious email accounts
4. **Research** the addresses
5. **Restrict** the number of declined transactions
6. **Always require** the Security Code (CVV)
7. Ship your orders using tracking numbers and **require signatures**
8. **Set** purchase limits
9. **Verify** email address for validity
10. **Pay attention** to the time of day
11. **Check** whether the mailing address is a mailbox or ship-forward service
12. When in doubt, **call Customer Service**
13. **Use** Address verification (AVS)
14. **First-time** shopper
15. **Larger-than-normal orders.** Because stolen cards have a limited life span, maximizing the value of each transaction processed is important to the crook
16. Orders that include **several of the same items**
17. Orders made up of **"big-ticket" items**
18. **"Rush" or "overnight"** orders

Introduction to PCI Compliance:

All Merchants (regardless of business size) are required to adopt the security standards in accordance with the **Payment Card Industry Data Security Standard (PCI/DSS)** to increase card data security and reduce fraud. The breach or theft of cardholder data affects the entire payment card ecosystem. Customers suddenly lose trust in Merchants or financial institutions, their credit can be negatively affected – there is enormous personal fallout. Merchants and financial institutions lose credibility (and in turn, business), and they are also subject to numerous financial liabilities. It is FastTransact's mission to keep your customer data safe, but we need you to do your part and register for PCI and become PCI compliant.

Important contact information

PCI Security Council
https://www.pcisecuritystandards.org/

Priority Payment Merchants
https://www.securitymetrics.com/pcidss/FastTransact

FDR Merchants
https://login.pcirapidcomply2.com/portal-core/home

Elavon Merchants
https://login.pcirapidcomply2.com/portal-core/home

Cynergy Merchants
https://www.securitymetrics.com/pcidss/FastTransact

For PCI Data Security Standards information and requirements, visit the following websites:

PCI Security Standards Council
https://www.pcisecuritystandards.org/#

American Express
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=pci&ln=en&frm=US

Discover Network
http://www.discovernetwork.com/fraudsecurity/disc.html

MasterCard SDP
http://www.mastercard.com/us/merchant/security/what_can_co/SDP/merchant/index.html

Visa CISP
http://usa.visa.com/merchants/risk_management/cisp.html

10 practical steps from the PCI Data Security Standard:

1. Educate
Employees should be trained annually on both online and physical security threats as well as the best practices for protection of cardholder data.

2. Update
Keep your employee manuals up-to-date with the information on the proper handling of sensitive information, including card data.

3. Screen
Pre-employment screening is a basic and essential practice for any business owner, especially for those employees that have access to sensitive customer or financial data.

4. Protect
Make sure your business has a firewall, anti-virus, malware and spyware detection software. And don't forget to regularly update the software.

5. Control
Tightly control downloads, software installations, the use of thumb drives and public Wi-Fi connections on computers used for payment card processing.

6. Be Aware
Pay attention to fraud prevention alerts from your virus and malware services; make sure you install updates as soon as they become available.

7. Separate
Designate a separate computer for processing all your online financial transactions. Try to keep this computer separate from social media sites, email and general Internet browsing, which can cause changes to the computer that can then make it more susceptible to vulnerabilities.

8. Change
Change your password regularly, and especially after you have outside contractors do hardware, software or Point of Sale System installations or upgrades. Make sure that you use complex passwords to make them more difficult to guess (include upper case letters, numbers and special characters).

9. Back up
Regularly back up your computers and the key data you want to protect, whether it's to a local machine or an offsite facility, so your business can be up and running again quickly in the unfortunate event of an unauthorized attack.

10. Learn
Check out the PCI security standards council website for more information on the Data Security standards, education and training resources available to you.

Happy Processing!