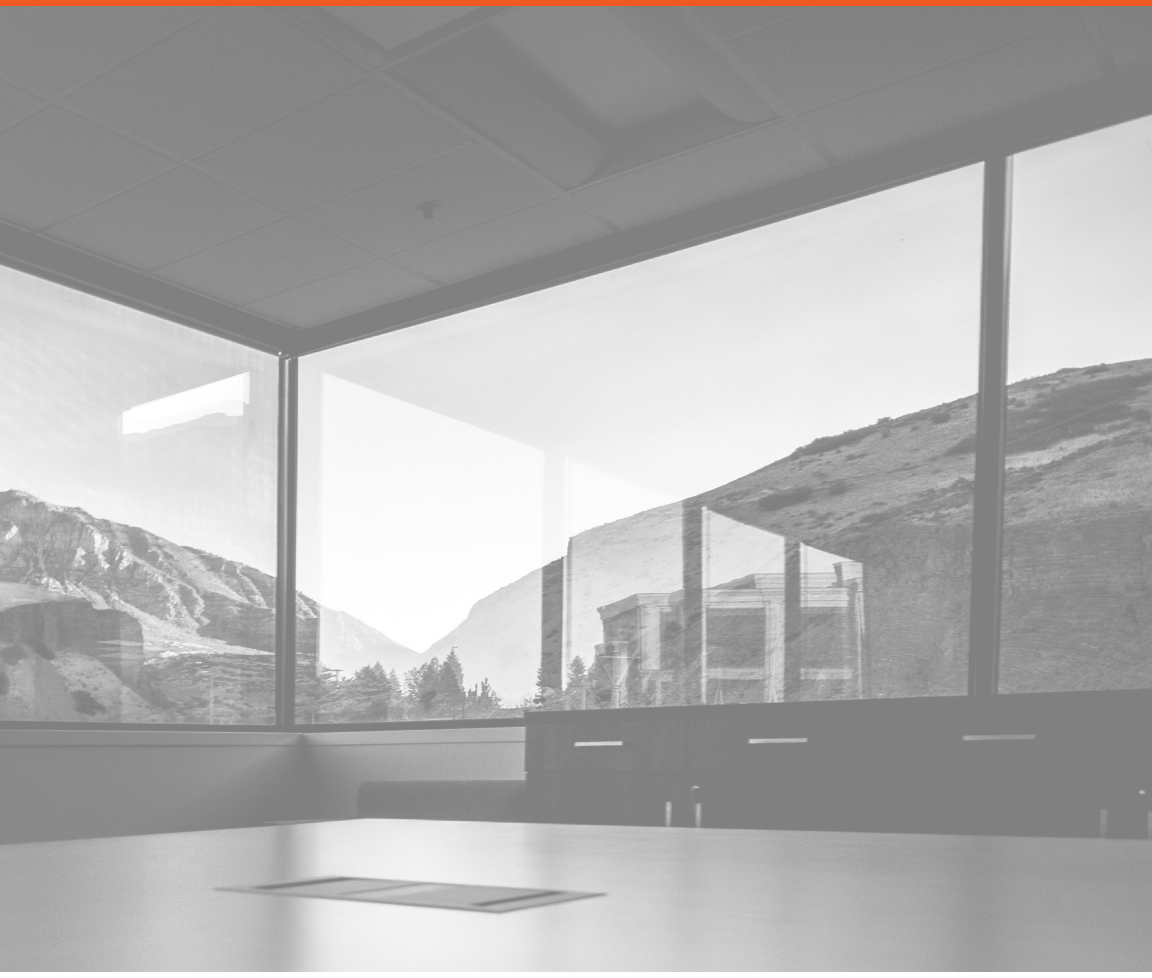
MERCHANT HANDBOOK

About CMS

Thank you for choosing Complete Merchant Solutions. We are your full-service electronic payments solutions provider. We facilitate payment processing for all major credit and debit cards, ACH, remote deposit capture, as well as other non-cash



payment methods. Our customizable solutions include a wide variety of integrated point-of-sale software, terminals and machines, e-commerce, and wireless payment processing solutions to serve all types and sizes of merchants.

Protecting Your Terminal

The following suggestions will help prevent damage to your credit card terminal:

- Keep your terminal away from liquids, food, and heat.
- Do not drop your terminal.
- Do not put anything in the slots of the terminal that do not belong.
- Store the terminal behind a locked door when your facility is closed or not in use.
- Do not open the back of the terminal for any reason.
- Do not take out the battery for any reason.
- Plug the terminal into a surge protector.

Not following the above suggestions may result in deleted transactions/batches or damage to the terminal. CMS will not be liable for those transactions if the terminal is not handled correctly.

Suggestions to prevent the terminal from being stolen or from unauthorized transactions being processed:

- Be aware of the terminal's position within the store.
- Have the terminal out of sight from store windows and doors.
- Do not lend your terminal to any friends, relatives, or other individuals.
- If you have a wireless terminal, have a carrying case to keep it concealed and protected from harm.
- If a wireless terminal needs to be in your car unattended, please keep it hidden from sight.

Fraud Protection

Credit card fraud is an unfortunate part of the current merchant life cycle. We recommend you implement the following practices to help mitigate the risk of fraud:

- Do not complete a transaction if the authorization request was declined. Do not repeat the authorization request after receiving a decline.
- If you receive a “call” message, call the authorization center and follow instructions.
- Ensure you obtain a signed receipt for all card-present transactions. Always compare the signature on the receipt with the signature on the back of the card.
- Ensure that all transactions entered in error, are voided immediately.
- If your establishment has policies regarding merchandise returns, refunds, or service cancellation, disclose these policies to the cardholder at the time of the transaction.
- When refunding a customer, always process the credit on the same card that was used for the original sale.

If you believe that a transaction is questionable, contact us at **1-877-267-4324 option 2** for assistance.

Suspicious Customer?

“CODE 10 ERROR”

You should make a Code 10 call to the voice authorization center whenever you are suspicious about a card, cardholder, or a transaction. The term “Code 10” is used so the call can be made at any time during a transaction without arousing a customer’s suspicions. You can notify the Authorization Center at:

Visa | Mastercard | Discover

1-800-228-1122

Code 10 Error Procedures

Code 10 Authorization procedures apply only to situations where the card is physically present but can be used regardless of the dollar amount of the card sale or the applicable Floor Limit.

- Call the Authorization Center and ask for a Code 10 Authorization (select option 3 or 4). This will automatically direct you to the security area of the Issuer.
- Security personnel will ask you a brief series of “Yes” or “No” questions about the card or the presenter and may ask you to request confirming identification from the presenter.
- If the security representative is able to confirm the identity of the presenter as a valid cardmember or authorized user of the card, an authorization decision for the card sale will be given and the presenter will not be aware that anything unusual has transpired.
- Some Issuers may request that you retain the card. If you are instructed to retain the card, your employee should do so, but only if permitted by your policies and only by peaceful and reasonable means.

Emphasize to your sales staff that they can make Code 10 calls even after a cardholder leaves the store. A Code 10 alert at this time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.

Data Security

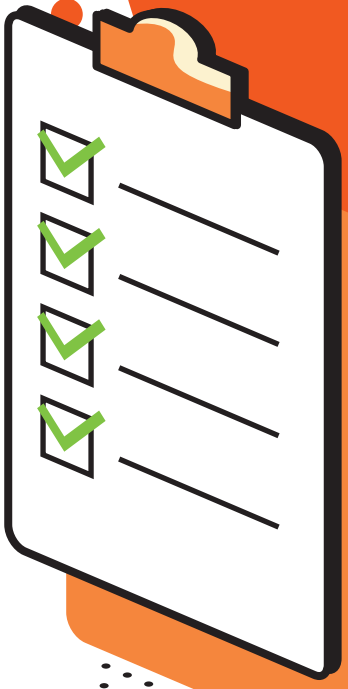
The electronic payments industry is closely regulated when it comes to data security, which only makes sense as it manages and transmits sensitive, personal, and financial data. The purpose of the regulations is to protect all parties in the electronic payments chain (i.e., cardholders, merchants, processors, and banks) from security breaches that can result in identity theft and fraud. The Payment Card Industry Data Security Standard (PCI DSS) sets the standard for maintaining the highest level of security measures and controls to protect sensitive data. CMS makes security a priority and completes an annual PCI DSS certification to ensure we are diligent in remaining compliant with all government and industry regulations.

CMS strives to assist all of our merchants in protecting customer data in today's technology driven world. Our PCI DSS Compliance Program is designed to evaluate how your business secures cardholder data, protecting you and your business from data breaches. The certification evaluates a merchant's ability to:

- Protect the confidentiality and integrity of sensitive information until it is destroyed.
- Protect against anticipated threats or hazards to the security or integrity of sensitive information.
- Protect against unauthorized use of sensitive information that could result in harm to someone.

The information about our PCI DSS program, to enroll and start your security questionnaire, will be sent separately.

Consumer Protection



Providing great products or services is the foundation of your business. Satisfied customers mean more repeat business and growth for your company. As a part of great customer support, review your marketing - product website, YouTube videos, social media - to ensure there are no practices within your business that causes or is likely to cause substantial injury to consumers; cannot reasonably be avoided by consumers; and, is not outweighed by any benefits to your customers. These tenants are the fundamentals of what is known as UDAP - Unfair or Deceptive Acts or Practices - and is enforced by the Federal Trade Commission.

Avoid misleading claims or statements about your products or services and include disclosures when necessary. Disclosures should be easy to find, easy to read, and easy to understand. CMS takes consumer protection seriously and considers our merchants as partners in meeting the requirements of applicable laws or regulations.

IRS Reporting and TIN Validation

The Housing Assistance Tax Act of 2008 includes the enactment of Section 6050W of the Internal Revenue Code that requires reporting entities to annually report payment card and third-party network transactions to the Internal Revenue Service (IRS) for each calendar year. This IRS mandate also requires all merchant service providers to validate the legal name and Tax Identification Number (TIN) for every merchant in their portfolio on an annual basis.

At the beginning of every year, you will receive form 1099-K reporting your total gross sales of credit card transactions for the previous year. It is critically important for you to furnish your correct TIN (Taxpayer Identification Number) and correct business name to us to avoid a 28% withholding as mandated by the IRS. Additional monthly fees may be assessed if you fail to validate your information.

Chargeback Overview

A chargeback is a process that allows cardholders, and occasionally an issuing bank, to file a dispute regarding a charge. Once the cardholder initiates the complaint, an investigation is performed by their issuing bank. There are many reasons why chargebacks occur, some of the most common reasons for chargebacks are:

- The customer claims they did not receive a product or service.
- Your customer does not recognize the charge or description on his or her credit card statement.
- The product or service was defective, damaged, or not as it was described.
- The customer was the victim of fraud–his or her credit card was stolen or used without their consent.
- A refund was requested and not received. You will receive documentation that notifies you of any chargeback(s).

You must fill out and submit all required documentation for each chargeback. Funds will be withdrawn from your account while the disposition of the chargeback is being determined. Do NOT issue a refund once you have been notified of a chargeback. If the chargeback is deemed to be valid, the consumer retains the funds. If the chargeback is deemed to be invalid, the funds will be re-deposited to your account.

E-Sign Consent

E-Sign Consent

Complete Merchant Solutions (CMS) wants merchants to understand how to access and use information about their merchant accounts. One step CMS is taking to make information more easily accessible is providing information that can be easily accessed online by logging into the Nexio Merchant Portal. By continuing to use our services, you agree to the e-sign consent to accept and receive communications electronically from CMS, third-party vendors, and our affiliates.

Digitally Received Documentation Delivery and Acceptance

Under this consent, CMS may provide documentation via email, text messaging, or by providing an online dashboard or reporting software. These documents may include but are not limited to, monthly statements, retrieval requests, chargeback notifications, and tax documentation.

Documentation Retrieval

To access, retain, and print any digital document, you will need the following:

- A computer, tablet, or mobile device with internet access. Computers require the following: Access to any web browser that is current and up to date, including 256-bit encryption.
- An email account that can send and receive email. This will be used to send login information to any online reporting tool(s) that are provided. If you use a filter to help block spam, you may need to adjust this filter to accept emails from our systems. If you desire to download and save the documents on a personal computer, sufficient storage space will be needed.

Paper Delivery of Communications

At any time you may request your monthly documents to be delivered in paper format via USPS. To request a paper copy of the documentation at no charge, please contact our Customer Support team at **877-267-4324.** They will be able to provide instructions on how to request a paper copy.

Updating Your Account Information

If you need to update your contact information, please proceed with the following:

- Our sponsor banks require you to submit a signed Address, Phone, Email Change Request form. This form can be found in our Knowledge Base located at kb.nexiohub.com. The article can be located by searching "How to Change Your Address, Phone, Email with your Merchant Account."
- Please provide a photocopy of the signer's driver's license. This is only used for verification of the signature and is often provided as a picture from your cell phone.

The signer on the account should complete the form including the Signature of Authorized Principal at the bottom of the form.

Once the form is completed, please email a copy to support@cmsonline.com. This copy should include a clear picture for each of the change forms and a driver's license for each signer. You may also fax the information to **1 (877) 537-9485.**

cms
AFFORDABLE. RELIABLE. SECURE.

Complete Merchant Solutions

727 North 1550 East 3rd Floor, Orem, UT 84097
Telephone: 1-877-267-4324
FAX: 1-877-537-9485
www.cmsonline.com

Sales

1-877-267-4324 Option 4
sales@cmsonline.com

Customer Support

1-877-267-4324 Option 2
support@cmsonline.com

Technical Support

1-877-267-4324 Option 2
support@cmsonline.com

Risk

1-877-267-4324 Option 3
risk@cmsonline.com

After Hours Support

1-877-267-4324 and follow the prompts. Please have your merchant identification number available.

ACCREDITED BUSINESS BBB Rating: A+ as of 3/10/2020 Click for Profile

Inc. 5000

PCI DSS COMPLIANT

INV 50