Credit Cards

This document provides detailed information about setting up CounterPoint for credit card processing, including step-by-step configuration instructions.

6/28/2010

Table of Contents

Overview

CounterPoint includes electronic draft capture (EDC) capabilities that allow you to process credit cards, debit cards, and checks under the CounterPoint Merchant Program (CMP) through Radiant Payment Services (RPS) or RBS Lynk.

The addition of the Credit Cards Option allows you to process EDC transactions through a variety of other processors, including First Data North, First Data South, TSYS Acquiring Solutions (formerly Vital), and Paymentech.

These processors allow you to take advantage of the full range of credit card processing features that CounterPoint offers and to ensure compliance with current credit card standards. Regardless of which processor you use, CounterPoint provides your business with an integrated solution for processing credit cards and other EDC transactions.

This document explains the process of configuring your CounterPoint system to process credit cards and other EDC transactions, including detailed configuration instructions for each supported card processor. This document also provides troubleshooting information to assist you in solving common and processor-specific problems you may encounter.

For general information about setting up your CounterPoint system to process EDC transactions, refer to Draft Capture in the CounterPoint Electronic Documentation. Other documents that contain additional information about credit card processing include Device Codes, Registers, Drawers, and Setting up Point of Sale Devices. These documents are referenced throughout the following pages, where appropriate.

Credit card processing features

CounterPoint offers the following credit card processing features:

- Comprehensive electronic credit card processing capabilities, including authorization, reporting, and settlement
- Check guarantee services through Certegy (formerly Equifax) and TeleCheck

  NOTE: All check transactions are routed through the card processor (not “split-dialed”) to improve response times and ensure CPGateway compatibility. However, Paymentech does not currently support check processing.
- Debit card processing
- Retail, Mail-order/Telephone-order (MOTO), and Ecommerce support
- Purchase cards (Level II)
- Address verification for Visa, MasterCard, AmEx, and Discover transactions
- Optional Card Verification Value/Card Verification Code/Card Identification (CVV2/CVC2/CID) support for “card not present” transactions

  NOTE: CVV2/CVC2/CID uses the extra 3 or 4 digits printed on the back of the credit card to help verify the authenticity of the card.
- CPGateway support for 2-second credit card processing over the Internet
- Direct authorization of American Express transactions using CPGateway
- Electronic Benefit Transfer (EBT) food stamps through TSYS, First Data North, and RBS Lynk using CPGateway
- Dial-up processing

CounterPoint Merchant Program

The CounterPoint Merchant Program (CMP) is a service that allows merchants to process credit cards through Radiant Payment or RBS Lynk without requiring the purchase of the Credit Cards Option.

In addition to out-of-the-box credit and debit card processing, the CMP offers address verification and card identification services, check authorization, support for Purchase cards (Level II), and reduced CPGateway fees.

Other processors

The Credit Cards Option allows you to process EDC transactions through one of CounterPoint's other supported processors. Like the CMP, these processors ensure compliance with rapidly-changing credit card standards and allow you to take advantage of CounterPoint's entire range of credit card processing features.

These processors offer the most favorable rates for each industry classification (i.e., **Retail**, **MOTO**, and **Ecommerce**). They also support address verification (AVS/AAV) and card identification (CVV2/CVC2/CID) services, check authorization through Certegy and TeleCheck, Purchase cards (Level II), and CPGateway.

The Credit Cards Option supports the following additional processors:

- First Data North
- First Data South
- TSYS Acquiring Solutions (formerly Vital)
- Paymentech

Industry types

CounterPoint supports the most favorable rates for the following industry types:

Industry	Features
Retail	• Best processing rates for card swipe ("card present") transactions • Address verification • Debit card processing • Optional CVV2/CVC2/CID
Mail-order / Telephone-order (MOTO)	• Transactions presumed to be "card not present" (no card swipe) • Address verification • Optional CVV2/CVC2/CID
Ecommerce	• Transactions presumed to be from website or other secure electronic source (no card swipe) • Point of Sale and Order Entry orders imported from CPOnline are handled as secure, fully-qualified ecommerce transactions • Address verification • Optional CVV2/CVC2/CID

Cardholder Information Security Program

In June 2001, Visa initiated the Cardholder Information Security Program (CISP) to define and promote credit card security standards that reduce the risks and costs associated with credit card fraud. In December 2004, Visa—in collaboration with MasterCard and with the endorsement of Discover and American Express—published version 1.0 of the Payment Card Industry (PCI) Data Security Standard, which outlines a set of guidelines that merchants must follow in order to be considered PCI-DSS-compliant. These guidelines stipulate, among other requirements, that credit card numbers must be masked on printed receipts and that full card numbers may not be retained on non-secured computer systems.

PCI-DSS compliance is essential to ensure that sensitive credit card information is secure and that you are protected from any liability that could arise from the fraudulent use of cardholder data obtained from your computer systems.

In January 2006, Visa certified CounterPoint V7 to be compliant with CISP and Payment Application Best Practices (PABP) standards. CounterPoint is listed on Visa's website (www.visa.com/cisp) as a **Validated Payment Application**.

CounterPoint includes documentation to guide merchants in setting up fully PCI-DSS compliant systems, including advice for adhering to CISP requirements that are not related to CounterPoint. Refer to the PCI-DSS Compliance Guide for more information about setting up a fully PCI-DSS-compliant system.

CPGateway also meets all PCI-DSS compliance standards. Radiant is named on Visa's website (www.visa.com/cisp) as a **PCI DSS-Compliant Service Provider** for CPGateway.

Configuring CounterPoint properly is only part of an overall PCI-DSS compliance strategy. Attaining PCI-DSS compliance requires you to evaluate your business practices to make certain that you have the appropriate policies in place and that your staff is vigilant to the risks of credit card fraud.

To ensure that you are following all published guidelines regarding PCI-DSS compliance, download and review the PCI Data Security Standard from www.visa.com/cisp. If you are not taking the necessary steps to adhere to the requirements outlined in the PCI Data Security Standard, your business is open to dangerous and potentially expensive liability.

NOTE: While Radiant can assist you and your Authorized Radiant Business Partner in configuring CounterPoint to be PCI-DSS compliant, we cannot function as an independent auditor or advisor regarding your general PCI-DSS compliance.

Refer to www.counterpointpos.com/cisp for additional information about PCI-DSS compliance.

Address verification and card identification

Address verification is the process of sending cardholder address information to the processor when the physical card is not swiped, reducing the risk of fraud and the potential for chargebacks against the merchant's account. The address verification data sent to the processor typically includes a 20-character address and a 9-digit ZIP Code.

Merchants can enable address verification for manually-entered Visa, MasterCard, American Express and Discover transactions.

NOTE: Address verification is also available for American Express transactions that you authorize directly with American Express through CPGateway, regardless of which Preferred Processor you use.

Refer to American Express address and CID verification, below, and Direct authorization of American Express transactions, on page 14, for more information.

CounterPoint also supports card identification (CVV2/CVC2/CID) services. CVV2/CVC2/CID provides supplemental information for an address verification transaction by sending the extra three or four digits printed on the credit card to the processor. Sending these extra digits for manually-entered transactions further reduces the risk of fraud and the potential for chargebacks.

CVV2/CVC2/CID is only available for manually-entered transactions for **Retail**, **MOTO** and **Ecommerce** merchants.

Except for American Express transactions, address verification and CVV2/CVC2/CID do not affect whether a transaction is authorized. These services are simply safeguards to help the merchant avoid fraud.

However, in order to obtain the lowest rate for manually-entered transactions, you must supply the requested address verification information. If you enter a credit card number manually and you do not provide the cardholder's address, you will be charged a higher rate for the transaction.

NOTE: In this version, you can configure CounterPoint to require only a ZIP Code for address verification purposes. You can also enable card verification services without first enabling address verification, allowing you to verify each credit card's security digits without requesting the customer's address.

American Express address and CID verification

To use address verification with American Express transactions that are authorized directly through American Express, you must sign up for the Automated Address Verification (AAV) service. To use CID verification with these transactions, you must enroll in the Card Identification Number Fraud Reduction program.

To register for these services, contact American Express at the following number:

Merchant Customer Service: 800-528-5200

Refer to Direct authorization of American Express transactions on page 14 for more information about authorizing American Express transactions directly.

Ticket Entry and Order Entry with address verification

In Ticket Entry and Order Entry, after a credit card pay code, charge amount, credit card number, and expiration date have been entered and verified (but before that information is cleared from the screen), if the credit card number was entered manually, address verification is active, and the amount is positive, the default address verification fields are set to the appropriate bill-to or ship-to address.

If your store is configured to allow address entry, the user will be prompted to do so. If CVV2/CVC2/CID is active, the user is also prompted to enter the additional three or four digits required for CVV2/CVC2/CID verification.

NOTE: An authorized user can press F2 at either prompt to skip the entry of address verification and CVV2/CVC2/CID information.

If an address verification and CVC2/CVV2/CID transaction is approved, additional information may be returned by the processor to indicate the verification status. If the address verification or CVV2/CVC2/CID information did not match, the mismatch is recorded and reported so the user can take the appropriate action.

NOTE: If a CID mismatch occurs for an American Express transaction, the transaction will not be authorized and you will receive no CID verification status information.

Purchase cards

CounterPoint supports Level II Purchase cards, Corporate cards, Business cards, and Commercial cards—which are generically referred to as “purchase cards.”

Purchase cards are Visa and MasterCard cards that look like normal credit cards to the merchant, but are processed in a special way so that the cardholder (typically a larger business or a government agency) receives additional information on monthly statements that indicate the types of goods and services that were purchased.

To ensure that you receive the preferential rate for purchase cards, you **MUST** record a non-blank PO number with each purchase card authorization. If a blank PO # is sent with a purchase card authorization, the processor will charge a billback fee—which is typically 0.5% to 1.0% of the transaction amount—for incomplete data.

To configure CounterPoint to meet this requirement, set the Require P.O. number for purchase cards ? field in Setup / Point of Sale / Stores / Draft Capture to Yes.

Check authorization

CounterPoint supports check authorization through Certegy (formerly Equifax, formerly TeleCredit) and TeleCheck, as well as the use of optical check readers in Point of Sale to read Magnetic Ink Character Recognition (MICR) encoded fields. These features are available with all CounterPoint processors, except Paymentech.

NOTE: CounterPoint provides support for Certegy's "Guarantee" service (response is OK 999999) as well as their "Verification" service (response is APPROVED 999999).

For merchants processing under the CMP, or with First Data North, First Data South, or TSYS, all check authorizations are obtained through the processor, which, in turn, obtains the authorization from Certegy or TeleCheck. This system ensures faster authorizations, better performance, and a higher degree of reliability.

NOTE: CounterPoint does not currently support check processing with Paymentech.

Contacting Certegy

To configure check processing through Certegy, you will need your 10-digit Certegy Station Number, which you can obtain by contacting Certegy at one of the following numbers:

Sales: 800-633-9454

Support: 800-215-6280

NOTE: You do not need to obtain a Certegy Station Number if you are processing with RBS Lynk.

Contacting TeleCheck

To configure check processing through TeleCheck, you will need your 8-digit TeleCheck Merchant Number, which you can obtain by contacting TeleCheck at one of the following numbers:

Sales: 800-835-3243

Support: 713-331-6442

Debit cards

CounterPoint allows you to accept both ATM-type debit cards and Visa/MasterCard check/debit cards as methods of payment. However, for a debit card to be accepted as tender, the card must be swiped and a PIN must be entered using a PIN pad device. You cannot manually enter a debit card transaction or process a debit card transaction without a PIN, and there is no voice authorization facility for debit cards.

Further, you can only accept debit cards as a method of payment if you are set up with your processor under the **Retail** industry type. You may **NOT** accept debit cards if you are set up under the **MOTO** or **Ecommerce** industry types.

PIN pads must meet the DUKPT encryption standards. Card readers must be programmed for Track 2 to be able to process debit cards.

In order to process debit card transactions with CounterPoint, you must obtain one of the supported PIN pads listed below. You can obtain pre-programmed PIN pads directly from PNC, TSYS, or TASQ Technology.

CounterPoint supports the following PIN pads for use with debit cards:

- VeriFone MX800 series
- VeriFone Omni 7000 series
- VeriFone Everest
- VeriFone 1000SE
- VeriFone 1000
- VeriFone 2000

NOTE: If you do not use a PIN pad/card reader to process debit cards (i.e., if you are using a Zon machine, instead), you can only accept debit cards as Cash, Check, or Credit pay types. You must define your card reader and PIN pad in Setup / Point of Sale / Device codes and assign them to a register in Setup / Point of Sale / Registers before you can accept a Debit card pay code in Point of Sale.

CPGateway

CPGateway is a service provided by Radiant Systems that allows you to obtain secure credit card, debit card, and check authorizations from your processor using the Internet, instead of dialing out for each authorization. This method is much faster and more reliable than dial-up communications and typically provides 2-second authorizations.* CPGateway also allows you to settle credit card transactions.

CPGateway features

CPGateway supports all CounterPoint EDC features, including credit card processing for Retail, MOTO, and Ecommerce industries, Purchase cards (Level II), AVS, CVV2/CVC2, debit cards, and check guarantee services through Certegy and TeleCheck. In addition, CPGateway offers:

- Fast authorization response times – typically 2 seconds*
- Internet-based service (uses your existing Internet connection)
- Simple configuration
- Affordable fees
- Ease of use
- Reliability
- Support for multiple workstations through a single Internet connection
- Direct authorization of American Express transactions
- Electronic Benefit Transfer (EBT) food stamps through TSYS, First Data North and RBS Lynk
- Faster batch settlements
- Automatic failover to dial-up connection

Visit www.CPGateway.com for more information about the features that the CPGateway service offers or to sign up for CPGateway.

Authorizing a charge using CPGateway

To authorize a charge through CPGateway, record the sale in CounterPoint in the normal manner, and then obtain the credit card information by using an MSR card reader or by entering the card information manually.

CounterPoint connects to CPGateway over the Internet using the TCP/IP protocol and requests the authorization. CPGateway quickly obtains the authorization from your card processor and passes it back to CounterPoint.

Because your CounterPoint system connects to CPGateway through the Internet and CPGateway maintains a constant high-speed connection to your card processor, you avoid the delays that are normally associated with dial-up service and modems and typically obtain authorizations in 2 seconds.

To settle a batch via CPGateway, use Point of Sale / Draft capture / Settle. This function uses CPGateway to settle all transactions, including those that were authorized through CPGateway and any transactions that were authorized through a dial-up connection.

---

* 2-second authorization response times are typical. Response times depend on the capabilities of the card processor and can also be affected by Internet bandwidth and traffic. Response times are not guaranteed.

Direct authorization of American Express transactions

Typically, credit card transactions are authorized and settled through your processor and you are charged a separate fee for each authorization and settlement. However, if you are using CPGateway to process credit card transactions over the Internet, you can configure CounterPoint to authorize American Express transactions directly through American Express, instead of through your processor, to avoid authorization fees.

NOTE: Settlement fees still apply to American Express transactions that are authorized directly, as these transactions are still settled with your processor.

To configure CounterPoint to authorize transactions directly through American Express, you must select Yes from Use AmEx Direct and specify your American Express Service Establishment (SE) number in Setup / Point of Sale / Stores / Draft capture, as described in Step 12 – Set up draft capture, beginning on page 38.

If you are already processing American Express transactions, you can find your Service Establishment number on the monthly Merchant Financial Activity Statement that you receive from American Express. You can also obtain this number from your bank or financial institution, from PNC Merchant Services or RBS Lynk (if you are processing credit cards under the CMP), or from American Express.

You do not have to perform any additional steps to begin authorizing American Express transactions directly using CPGateway. However, if you wish to use address and CID verification for American Express transactions that you authorize directly, you must register for these services by contacting American Express at the following number:

Merchant Customer Service: 800-528-5200

Electronic Benefit Transfer food stamps

Electronic Benefit Transfer (EBT) is a system that allows recipients of Federal Food Stamp Program benefits to transfer their benefits to retailers as payment for goods purchased. EBT replaces traditional food stamps with magnetic-stripe cards that are processed in a similar manner as debit cards. EBT eliminates the labor involve in handling paper food stamps and automates the payment and settlement process.

If you are processing credit cards through TSYS, First Data North, or RBS Lynk under the **Retail** industry type, and you are using CPGateway, CounterPoint allows you to accept EBT food stamps as tender for groceries or other items that can be purchased with food stamps. You can also issue refunds to EBT accounts for the return of eligible items. However, customers cannot receive cash back for EBT transactions or access cash benefits using EBT cards.

You cannot accept EBT food stamps if you are set up under the **MOTO** or **Ecommerce** industry types, or if you are processing through First Data South or Paymentech. Further, you cannot process EBT food stamps over a dial-up connection.

To process EBT food stamps in regular Ticket Entry or Touchscreen Ticket Entry, you can either swipe the customer's EBT card, using an MSR device, or you can enter the EBT card number manually. To approve the EBT transaction, the customer must enter a PIN using a PIN pad device. The customer's PIN and account balance are verified through your credit card processor and the transaction is authorized or denied. If the transaction is authorized, the customer's remaining EBT account balance is printed on the receipt.

NOTE: Voice authorization of EBT transactions is not supported.

EBT transactions are settled through your processor during the normal CPGateway settlement process (i.e., using Point of Sale / Draft capture / Settle).

Configuring CounterPoint for CPGateway

CPGateway is compatible with your CounterPoint for Windows or CounterPoint for Unix/Linux system. CounterPoint uses TCP/IP to communicate through the Internet to CPGateway. You must have a persistent Internet connection to use CPGateway. You can access CPGateway through a dial-up connection, DSL, cable, T1, or any other service that supports the TCP/IP protocol.

You will also need an Internet Service Provider (ISP) to provide a connection to the Internet. In addition, each CounterPoint workstation must be able to access the Internet, either through its own connection or through a single shared connection.

Is CPGateway reliable?

CPGateway is designed for fail-safe operation to provide absolutely reliable credit card processing. Maximum reliability is built into the CPGateway service, including redundant servers, redundant Internet connections from your CounterPoint system to CPGateway, redundant communication lines to each card processor, redundant power systems, and so forth.

If your local Internet service fails (i.e., if your ISP or communication lines go down), CounterPoint will automatically switch to dial-up mode and contact your card processor directly. CounterPoint will also automatically use the Modem Server Option, if it is active.

All authorizations obtained from your processor through CPGateway or through a direct dial-up connection are stored in your local CounterPoint database and can be settled in the same batch.

Setting up credit card processing

The following steps outline the process of preparing, configuring, and testing CounterPoint V7 to process credit cards:

Pre-configuration steps	
Step 1	Obtain information for your processor
Step 2	Route checks
Step 3	Install latest CounterPoint software
CPGateway configuration*	
Step 4	Sign up for CPGateway
Step 5	Verify your Internet connection
Hardware configuration	
Step 6	Set up modems
Step 7	Set up MSR card readers
Step 8	Set up MICR check readers
CounterPoint configuration	
Step 9	Set the WINEDC environment variable
Step 10	Define SYNDEC.CFG
Step 11	Set up stores
Step 12	Set up draft capture
Step 13	Set up device codes and registers
Testing and confirmation	
Step 14	Test dial-up authorization
Step 15	Test CPGateway authorization*

* Skip these steps if you are not using CPGateway.

Step 1 – Obtain information for your processor

Before you configure your CounterPoint V7 system for credit card processing, you must gather certain information that is required in later steps. The information that you need depends on the processor you are using, as detailed in the following sections.

First Data North

If you are processing with First Data North, make sure that you have the following information before proceeding with the remaining configuration steps:

- Bank Code – 3 digits
- Merchant ID – 9 digits

  NOTE: Your PNC Merchant Services representative may provide a 12-digit Merchant Number, which is a combination of the 3-digit Bank Code and the 9-digit Merchant ID.

- Terminal ID (optional) – 6 digits

  NOTE: This Terminal ID is used by some multi-register/multi-location merchants. Do not to confuse this Terminal ID with the 20-character Terminal-ID that is used in CounterPoint.

- Telephone number(s) for authorization
- Telephone number(s) for settlement

American Express

If you are using CPGateway and you want to authorize AmEx transactions directly through American Express, you must also obtain the following information:

- American Express SE Number – 10 digits

EBT Food Stamps

If you are processing EBT food stamp transactions, you must obtain the following additional information:

- Food and Consumer Service Identifier (FCS ID) – 7 characters

TSYS

If you are processing with TSYS (Vital), obtain the following information from your bank or financial institution before proceeding with the remaining configuration steps:

- BIN Number – 6 digits
- Agent Number – 6 digits
- Chain Number – 6 digits
- Merchant Number – 12 digits
- SIC Code – 4 digits
- Store Number – 4 digits
- Terminal Number – 4 digits
- Time Zone – 3 digits
- "V" Number – 7 digits, plus a V prefix
- Telephone number(s) for authorization
- Telephone number(s) for settlement
- Merchant Location Number (optional) – 5 digits
- Country Code (optional) – 3 digits
- Currency Code (optional) – 3 digits

American Express

If you are using CPGateway and you want to authorize AmEx transactions directly through American Express, you must also obtain the following information:

- American Express SE Number – 10 digits

Debit Cards

If you are processing debit cards, you must obtain the following additional information:

- Reimbursement Attribute (Z is the default value for a Standard Interlink Merchant)
- Sharing Group – 1 to 30 characters
- Merchant ABA Number – 9 digits
- Merchant Settlement Agent Number (may be identified as the "FIID") – 4 characters

EBT Food Stamps

If you are processing EBT food stamp transactions, you must obtain the following additional information:

- Food and Consumer Service Identifier (FCS ID) – 7 characters

First Data South

If you are processing with First Data South, obtain the following information from your bank or financial institution before proceeding with the remaining configuration steps:

- Merchant Number – 11 digits
- Qual Code – 8 digits
- SIC Code – 4 digits
- Terminal Serial Number – 4 digits
- American Express SE Number (if you accept American Express) – 10 digits
- Discover SE Number (if you accept Discover) – 15 digits
- Diners Club SE Number (if you accept Diners Club) – 10 digits
- Carte Blanche SE Number (if you accept Carte Blanche) – 10 digits
- JCB SE Number (if you accept JCB) – 15 digits
- Telephone number(s) for authorization
- Telephone number(s) for settlement

Debit Cards

If you are processing debit cards, you must arrange with your bank to have your First Data South merchant account configured as an *auto-close* account.

Paymentech

If you are processing with Paymentech, obtain the following information from your bank or financial institution before proceeding with the remaining configuration steps:

- Client Number – 4 digits
- Merchant Number – 12 digits
- Terminal Number – 3 digits
- Telephone number(s) for authorization
- Telephone number(s) for settlement

American Express

If you are using CPGateway and you want to authorize AmEx transactions directly through American Express, you must also obtain the following information:

- American Express SE Number – 10 digits

Radiant Payment Services/RBS Lynk

If you are processing with Radiant Payment Services or RBS Lynk, obtain the following information from Radiant Systems or RBS Lynk before proceeding with the remaining configuration steps:

- BIN Number – 6 digits
- Agent Number – 6 digits
- Chain Number – 6 digits
- Merchant Number – 12 digits
- Plan Number/Category Code/SIC – 4 digits
- Store Number – 4 digits
- Terminal Number – 4 digits
- Time Zone – 3 digits
- Telephone number(s) for authorization
- Telephone number(s) for settlement
- Merchant Location Number (optional) – 5 digits
- “V” Number (optional) – 7 digits, plus a V prefix
- Country Code (optional) – 3 digits
- Currency Code (optional) – 3 digits

American Express

If you are using CPGateway and you want to authorize AmEx transactions directly through American Express, you must also obtain the following information:

- American Express SE Number – 10 digits

EBT Food Stamps

If you are processing EBT food stamp transactions, you must obtain the following additional information:

- Food and Consumer Service Identifier (FCS ID) – 7 characters

Step 2 – Route checks

Skip this step if you are not using check guarantee services.

If you are using check guarantee services from Certegy (formerly Equifax) or TeleCheck, you must arrange for your check transactions to be routed through your processor, instead of “split dialed.” To do this, complete the appropriate steps for your processor.

First Data North

If you are processing with First Data North, follow these steps to route check transactions through First Data North:

Certegy

1. Contact your Certegy service representative and obtain your 10-digit Certegy Station Number. Refer to Check authorization on page 11 for more information about contacting Certegy.
2. Contact First Data North and ask to have your account entitled for Certegy.
3. Provide First Data North with your 10-digit Certegy Station Number to use as the Service Establishment Number (SE#).

Your account must be entitled for Authorization only and will be available for use on the next business day. Until your account is entitled, you will not be able to process checks.

TeleCheck

1. Contact your TeleCheck service representative and obtain your 8-digit TeleCheck Subscriber Number. Refer to Check authorization on page 11 for more information about contacting TeleCheck.
2. Find the first two digits of your TeleCheck Subscriber Number in the TeleCheck Location Codes table on page 24 and replace them with the corresponding 3-digit Region Code to build your 9-digit TeleCheck SE number.

   For example, if your TeleCheck Subscriber Number is 05999999, your Region Code would be 324 and your TeleCheck SE number would be 324999999.

   NOTE: If the first two digits of your TeleCheck Subscriber Number appear more than once, use the Region Code that corresponds to the TeleCheck District in which you are located.
3. Contact your financial institution and ask to have your merchant account entitled for TeleCheck.
4. Provide your financial institution with your 9-digit TeleCheck SE number.

Your account must be entitled for Authorization only and will be available for use on the next business day. Until your account is entitled, you will not be able to process checks.

TSYS

If you are processing with TSYS (Vital), follow these steps to route Certegy or TeleCheck check transactions:

Certegy

1. Contact your Certegy service representative and obtain your 10-digit Certegy Station Number. Refer to Check authorization on page 11 for more information about contacting Certegy.
2. Provide your Certegy service representative with the 6-digit BIN # that you obtained from your bank or financial institution. Certegy will associate the BIN # with your 10-digit Certegy Station Number.
3. Contact your bank or financial institution and ask to have your merchant account entitled for Certegy.
4. Provide your bank or financial institution with your 10-digit Certegy Station Number to use as the Certegy SE number for your account.

TeleCheck

1. Contact your TeleCheck service representative and obtain your 8-digit TeleCheck Subscriber Number. Refer to Check authorization on page 11 for more information about contacting TeleCheck.
2. Find the first two digits of your TeleCheck Subscriber Number in the TeleCheck Location Codes table on page 24 and replace them with the corresponding 3-digit Region Code to build your 9-digit TeleCheck SE number.

   For example, if your TeleCheck Subscriber Number is 05999999, your Region Code would be 324 and your TeleCheck SE number would be 324999999.

   NOTE: If the first two digits of your TeleCheck Subscriber Number appear more than once, use the Region Code that corresponds to the TeleCheck District in which you are located.
3. Contact your bank or financial institution and ask to have your merchant account entitled for TeleCheck.
4. Provide your bank or financial institution with your 9-digit TeleCheck SE number.

First Data South

If you are processing with First Data South, follow these steps to route Certegy or TeleCheck transactions:

Certegy

1. Contact your Certegy service representative and obtain your 10-digit Certegy Station Number. Refer to Check authorization on page 11 for more information about contacting Certegy.
2. Contact your bank or financial institution and ask to have your account entitled for Certegy.
3. Provide your bank or financial institution with your 10-digit Certegy Station Number to use as the Service Establishment Number (SE#).

Your account must be entitled for Authorization only and will be available for use on the following business day. Until your account is entitled, you will not be able to process checks through First Data South.

TeleCheck

1. Contact your TeleCheck service representative and obtain your 8-digit TeleCheck Merchant Number. Refer to Check authorization on page 11 for more information about contacting TeleCheck.
2. Find the first two digits of your TeleCheck Subscriber Number in the TeleCheck Location Codes table on page 24, replace them with the corresponding 2-digit POS Code, and then add two zeros (00) to build your 10-digit TeleCheck SE number.

   For example, if your TeleCheck Subscriber Number is 05999999, your POS Code would be 24 and your TeleCheck SE number would be 2499999900.

   NOTE: If the first two digits of your TeleCheck Subscriber Number appear more than once, use the Region Code that corresponds to the TeleCheck District in which you are located
3. Contact your bank or financial institution and ask to have your merchant account entitled for TeleCheck.
4. Provide PNC Merchant Services or your financial institution with your 10-digit TeleCheck SE number.

Your account must be entitled for Authorization only and will be available for use on the next business day. Until your account is entitled, you will not be able to process checks.

Paymentech

CounterPoint does not currently support check processing with Paymentech.

Radiant Payment Services/RBS Lynk

If you are processing with Radiant Payment Services/RBS Lynk, you do not need to take any additional steps to route Certegy check transactions.

NOTE: RPS/RBS Lynk does not support check processing through TeleCheck.

TeleCheck Location Codes

The following table lists the Region Codes and POS Codes for each TeleCheck District. Use this table to build a valid TeleCheck SE number for your processor.

First two digits of Subscriber Number	TeleCheck District	Region Code	POS Code
01	Nebraska	307	07
01	Kansas / Middle America	301	01
02	Louisiana	302	02
03	South Coast	317	17
04	North West	304	04
05	Hawaii / South West	324	24
06	Wisconsin	306	06
08	West Coast / LAX	325	25
09	Pittsburgh	326	26
11	National Accounts	308	08
14	Oregon	313	13
15	Michigan	319	19
16	Minnesota	314	14
17	New England	318	18
17	New York	321	21
18	Philadelphia	323	23
18	Washington DC / Mid Atlantic	310	10
19	Chicago	309	09
19	Indiana	305	05
19	Ohio	312	12
20	Colorado / San Francisco	303	03
20	Orange County	315	15
20	Arizona	316	16
20	San Diego	311	11
21	Quebec	320	20
22	Toronto	322	22
23	Calgary	320	20
24	Winnipeg	320	20
24	Vancouver	320	20
35	National Accounts	335	35
37	National Accounts	337	37

Step 3 – Install the latest CounterPoint software

Install the latest version of CounterPoint, following the instructions outlined in the CounterPoint Installation Guide. Ensure that you have the latest Service Pack(s) installed, as well.

You can obtain the current CounterPoint Service Pack from the Support area of the CounterPoint website at http://www.counterpointpos.com/support/software_cpv7.htm.

NOTE: You must be a registered CounterPoint Subscription Service (CSS) subscriber to access the Support area of the CounterPoint website.

Step 4 – Sign up for CPGateway

Skip this step if you are not using CPGateway.

You can use CPGateway to process credit card authorizations over the Internet.

To sign up for CPGateway, visit the CPGateway webpage at www.CPGateway.com, click Register Online! and follow the on-screen instructions. As part of the confirmation process, you will receive a CPGateway Merchant #.

You may begin using the CPGateway service with this CPGateway Merchant # immediately after you sign up.

Step 5 – Verify your Internet connection

Skip this step if you are not using CPGateway.

You must ensure that your CounterPoint system has a functional Internet connection. To verify that your system can communicate with CPGateway, type the following command at a command prompt:

```
ping primary.cpgateway.com
```

The test is successful if this command returns a series of replies from the CPGateway server. The test fails if this command returns a series of Request timed out messages.

If the ping test fails, your network administrator may want to perform a traceroute to identify where the connection is failing. On Unix/Linux systems, the traceroute command must be configured to use ICMP, rather than UDP, or the traceroute may be rejected by CPGateway.

NOTE: Microsoft Proxy Server 2.0 does not allow you to ping other servers. However, you may be able to ping primary.cpgateway.com using Hyperterminal or some other software.

Firewall traffic requirements

If your CounterPoint system is located behind a firewall, you must configure the firewall to allow the following outbound traffic from your processor and workstations:

- Ping traffic (for testing purposes only – not actually used for authorizations)
- TCP traffic

To allow TCP traffic through your firewall, you must open one of the following ports, depending on the processor(s) you are using:

Processor	Port
First Data North	50000
TSYS (Vital)	50001
RPS/RBS Lynk	50003
Paymentech	50005
First Data South	50006
American Express* (direct authorizations only)	50004

* To authorize American Express transactions directly using CPGateway, you must open port 50004, regardless of which processor you are using.

Step 6 – Set up modems

Follow the manufacturer's instructions to install your modem(s) on your CounterPoint workstation(s) or on your Modem Server, if you are using the Modem Server Option.

After you have installed your modem(s), you should test each modem to ensure that it is operating correctly before attempting to use it with CounterPoint. If the test is successful, you are ready to proceed with the remaining steps. If the test fails, double check your modem settings and test the modem again.

Refer to Modem configuration and troubleshooting on page 69 for more information about configuring modems, including troubleshooting advice for specific models.

Step 7 – Set up MSR card readers

Install and test your MSR card reader(s), using the manufacturer's instructions and software. You can configure your card readers to read Track 1 or Track 2, but not both. CounterPoint SQL cannot read data from both tracks simultaneously.

NOTE: If you are processing debit cards, you **MUST** configure your card reader(s) to read Track 2.

Step 8 – Set up MICR check readers

Skip this step if you are not processing checks using MICR check readers.

As described in Check authorization on page 11, CounterPoint supports the use of optical check readers to read the MICR encoded fields on checks. Before you can use a MICR check reader with CounterPoint, however, you must first install and test the device. Depending on the manufacturer, you may also be required to program the check reader to use the appropriate format for your credit card processor and check processor.

To configure your MICR check reader(s), complete the appropriate steps for your credit card processor, as outlined in the following sections.

First Data North

If you are processing with First Data North, follow these steps to set up your MICR check reader.

1. Follow the manufacturer's instructions to connect the MICR check reader to your CounterPoint workstation, using either a serial port or a keyboard wedge.
2. Using the software that was supplied with the device, configure the check reader's communication settings and test the device to ensure that it can communicate with your CounterPoint workstation.
3. If you are using an IBM SureMark or Epson TM series device, no additional configuration is required. Proceed to Step 9 – Set the WINEDC environment variable on page 29.

   If you are using a MICR check reader from a manufacturer other than IBM or Epson, you must program the check reader to use the format required by First Data North. The appropriate format depends on the check processor you are using.

   Certegy
   If you are using Certegy, program your MICR check reader to match the following format, using the software and instructions provided by the manufacturer:

   <routingnumber>T<accountnumber>A<checknumber>

   The following table lists pre-defined Certegy formats for popular MICR check readers:

Manufacturer (Model)	Format setting
IVI (MR1000)	16
MagTek (Mini/Maxi)	1118
Checkmate (CMR400M)	FDMS VeriFone Printer

   TeleCheck
   If you are using TeleCheck, program your check reader to match the following format, using the software and instructions provided by the manufacturer:

   <routingnumber><accountnumber>

   The following table lists the pre-defined TeleCheck format for a popular check reader:

Manufacturer (Model)	Format setting
MagTek (Mini/Maxi)	0800

TSYS, First Data South, or RPS/RBS Lynk

If you are processing with TSYS (Vital), First Data South, Radiant Payment Services, or RBS Lynk, follow these steps to set up your MICR check reader:

1. Follow the manufacturer's instructions to connect the MICR check reader to your CounterPoint workstation, using either a serial port or a keyboard wedge.
2. Using the software that was supplied with the device, configure the check reader's communication settings and test the device to ensure that it can communicate with your CounterPoint workstation.
3. If you are using an IBM SureMark or Epson TM series device, no additional configuration is required. Proceed to Step 9 – Set the WINEDC environment variable on page 29.

   If you are using a MICR check reader from a manufacturer other than IBM or Epson, you must program your MICR check reader to use the format required by TSYS. The appropriate format depends on the check processor, as detailed below.

NOTE: RPS/RBS Lynk does not support check authorization through TeleCheck.

Certegy
If you are using Certegy, program your MICR check reader to match the following format (i.e., the TAC format), using the software and instructions provided by the manufacturer:

T<routingnumber>A<accountnumber>C<checknumber>

The following table lists the pre-defined Certegy format for a popular check reader:

Manufacturer (Model)	Format setting
MagTek (Mini/Maxi)	3800

TeleCheck
If you are using TeleCheck, program your check reader to match the following format (i.e., the TOAD format), using the software and instructions provided by the manufacturer:

T<routingnumber>T<accountnumber>O<checknumber>

The following table lists the pre-defined TeleCheck format for a popular check reader:

Manufacturer (Model)	Format setting
MagTek (Mini/Maxi)	0002

Step 9 – Set the WINEDC environment variable

You must set the WINEDC environment variable to the appropriate value for your processor to ensure that the correct credit card software is loaded when you start CounterPoint. You can set the WINEDC environment variable in the synrun.syn file (Windows systems) or the synsuppl file (Unix/Linux systems), which are located in your top-level CounterPoint directory. You can also set WINEDC in the System Control Panel on Windows NT/2000/XP systems, or in the AUTOEXEC.BAT file on Windows 95/98 systems.

The following table lists the WINEDC setting for each processor, for both Windows and Unix systems.

Processor	WINEDC setting (Windows)	WINEDC setting (Unix)
First Data North	WINCES	rtsces
First Data South (NaBANCO)	WINNAB	rtsnab
Paymentech	WINPMT	rtspmt
PNC Merchant Services	WINCES	rtsces
RPS/RBS Lynk	WINLNK	rtslnk
TSYS (Vital)	WINVIS	rtsvis

For Windows systems, set the WINEDC environment variable using the following command, where WINxxx is the appropriate setting for your processor:

```
SET WINEDC=WINxxx
```

For Unix/Linux systems, set the WINEDC environment variable using the following command, where rtsxxx is the appropriate setting for your processor:

```
WINEDC=rtsxxx;export WINEDC
```

Refer to Environment Variable Setup in the CounterPoint Electronic Documentation for more information about setting environment variables.

Step 10 – Define SYNEDC.CFG

CounterPoint obtains a variety of credit card processing parameters from the SYNEDC.CFG file in your top-level directory. These parameters include some of the information you gathered from your financial institution (or PNC Merchant Services) in Step 1 of the configuration process, along with any additional settings that may be required for your modem or your check processor.

To define the SYNEDC.CFG file, you must copy the appropriate WINxxx.CFG file, and then add the necessary parameters for your processor, as outlined in the following sections. You must add all parameters **before** the first tilde (~) character in the SYNEDC.CFG file. You must also start and end each parameter line with a backslash (\) and insert a backslash between each parameter. Finally, each parameter line cannot exceed 80 characters.

For example, the following parameter line defines the name, city, state, and ZIP Code for a particular merchant:

```
\MNCamptownGolf\MCMEMPHIS\MSTN\MZ38138\MP800-123-4567\
```

Refer to Draft Capture in the CounterPoint Electronic Documentation for more information about editing the SYNEDC.CFG file.

Using multiple batch number files

Except for PNC Merchant Services and First Data North, all processors use the BATCHNO.DAT file in the top-level directory to determine the next batch number to use during settlement. Certain configurations, such as multi-store WAN environments, may require a separate range of batch numbers for each store or register.

To accommodate this requirement, you must create multiple BATCHNO.xxx files in your top-level directory and specify the starting batch number for a particular store or register in each file. Each BATCHNO.xxx file must have a unique extension, to distinguish it from the other BATCHNO.xxx files. We recommend using the store number or register number to which the BATCHNO.xxx file will be assigned as the extension for each file.

Each BATCHNO.xxx file must include a unique 3-digit number, which defines the starting batch number for the corresponding store or register. For example, you might enter the number 100 in store #1's BATCHNO.001 file, 200 in store #2's BATCHNO.002 file, and so forth.

When you have created all of the BATCHNO.xxx files you need, create a SYNEDC.CFG file with a different file name for each store or register and specify the BATCHNO.xxx file to use for that store or register with the BF parameter. For example, the SYNEDC.CFG file for store 001 would include the following setting to reference the BATCHNO.001 file:

```
\BFBATCHNO.001\
```

NOTE: If you need to specify a path to the file, use forward slashes to separate directories and sub-directories (e.g., \BFC:/SYN/BATCHNO.001).

Finally, set the WINSYN environment variable for each store or register to specify the appropriate SYNEDC.CFG file. Refer to Draft Capture in the CounterPoint Electronic Documentation for more information about setting up multiple SYNEDC.CFG files.

Using multiple modem initialization strings

If you have multiple types of modems, you may need to define unique initialization strings for each workstation or store. To do this, create a SYNEDC.CFG file with a different file name for each store or register and modify the MI parameter in each file to specify the appropriate modem initialization string. Then, set the WINSYN environment variable for each store or register to specify the appropriate SYNEDC.CFG file.

Refer to Draft Capture in the CounterPoint Electronic Documentation for more information about setting up multiple SYNEDC.CFG files.

First Data North

If you are processing with First Data North, follow these steps to edit your SYNEDC.CFG file:

1. Copy the WINCES.CFG file in your top-level CounterPoint directory to SYNEDC.CFG using one of the following commands:

   Windows: COPY WINCES.CFG SYNEDC.CFG

   Unix/Linux: cp WINCES.CFG SYNEDC.CFG

2. Open SYNEDC.CFG in Notepad or another text editor.
3. If you are using purchase cards, add the following parameters to the SYNEDC.CFG file and specify the appropriate setting for each:

   MS Merchant state (e.g., \MSTN\)

   MZ Merchant ZIP Code (e.g., \MZ38138\)

   MP Merchant phone number (e.g., \MP800-123-4567\)

NOTE: You can use whatever phone number format you prefer—up to 15 characters—for the MP parameter.

   ST Store Number/Merchant Tax ID (e.g., \ST123456789012345\)

4. If you are not using purchase cards, but you wish to include a phone number to print on customers' monthly credit card statements, add the MP parameter to the SYNEDC.CFG file and specify the phone number to print.
5. If your modem requires an initialization string, add the MI parameter to SYNEDC.CFG in the following format, where xxxxx is your modem's initialization string:

   \MIATxxxxx\

   For example, if you are using a US Robotics Sportster Non-V.90 modem, you would enter the following setting:

   \MIAT&D2&K0&M0&C1&N2\

   Refer to Modem configuration and troubleshooting on page 69 for information about modem initialization strings, including a list of initialization strings for specific modems and instructions for determining the initialization string for other modems.

6. If you are processing checks with Certegy, add the following parameter:

   \CKE\

NOTE: Do not add this parameter if you are processing checks with TeleCheck.

7. Save your changes and close the SYNEDC.CFG file.

TSYS

If you are processing with TSYS (Vital), follow these steps to edit your SYNEDC.CFG file:

1. Copy the WINVIS.CFG file in your top-level CounterPoint directory to SYNEDC.CFG using one of the following commands:

   Windows: COPY WINVIS.CFG SYNEDC.CFG

   Unix/Linux: cp WINVIS.CFG SYNEDC.CFG

2. Open SYNEDC.CFG in Notepad or another text editor.
3. Add the following parameters to the SYNEDC.CFG file and specify the appropriate settings for each:

   MN Merchant name (e.g., \MNCamptownGolf\)

   MC Merchant city (e.g., \MCMEMPHIS\)

   MS Merchant state (e.g., \MSTN\)

   MZ Merchant ZIP Code (e.g., \MZ38138\)

   MP Merchant phone number (e.g., \MP800-123-4567\)

NOTE: You can use whatever phone number format you prefer—up to 15 characters—for the MP parameter.

4. Add the following parameters and specify the settings you received from your financial institution in Step 1 of this process:

   PL Plan Number/Category Code (e.g., \PL1234\)

   AG Agent Number (e.g., \AG123456\)

   CH Chain Number (e.g., \CH654321\)

   ST Store Number, followed by Terminal Number (e.g., \ST67895555\)

   CC (Optional) Currency Code (e.g., \CC321\)

   LN (Optional) Merchant Location Number (e.g., \LN54321\)

   TS "V" Number (e.g., \71234567\)

NOTE: Replace the V prefix in your "V" Number with a 7, for a total of eight digits.

   TZ Time Zone (e.g., \TZ706\)

NOTE: If your bank did not provide you with a Time Zone setting, find your time zone in the following table and specify the corresponding setting in the TZ parameter.

Time zone	Setting
Eastern Standard Time (EST)	705
Central Standard Time (CST)	706
Mountain Standard Time (MST)	707
Pacific Standard Time (PST)	708

5. If you are processing debit cards through TSYS, add the following parameters to the SYNEDC.CFG file and specify the settings you received from your financial institution:

   RA Reimbursement Attribute (e.g., \RAZ\)

   SG Sharing Group (e.g., \SGYQL8G\)

   MA Merchant ABA Number (e.g., \MA987654321\)

   ME Merchant Settlement Agent Number (e.g., \MEV027\)

6. If your modem requires an initialization string, add the MI parameter to SYNEDC.CFG in the following format, where xxxxx is the initialization string for your modem:

   \MIATxxxxx\

   For example, if you are using a US Robotics Sportster Non-V.90 modem, you would enter the following setting:

   \MIAT&D2&K0&M0&C1&N2\

   Refer to Modem configuration and troubleshooting on page 69 for information about modem initialization strings, including a list of initialization strings for specific modems and instructions for determining the initialization string for other modems.

7. If you are processing checks with Certegy, add the CK parameter and specify whether you are using Certegy East (E) or Certegy West (W). For example, if you are processing with Certegy West, enter the following setting:

   \CKW\

NOTE: You do not need to add this parameter if you are processing checks with TeleCheck.

8. Save your changes and close the SYNEDC.CFG file.

First Data South

If you are processing with First Data South (formerly NaBANCO), follow these steps to edit your SYNEDC.CFG file:

1. Copy the WINNAB.CFG file in your top-level CounterPoint directory to SYNEDC.CFG using one of the following commands:

   Windows: COPY WINNAB.CFG SYNEDC.CFG

   Unix/Linux: cp WINNAB.CFG SYNEDC.CFG

2. Open SYNEDC.CFG in Notepad or another text editor.

3. Add the following parameters and specify the settings you received from your financial institution in Step 1 of this process:

   IC SIC Code (e.g., \PL1234\)

   ST Qual Code (e.g., \ST12345678\)

   TS Terminal Serial Number (e.g., \TS1234\)

4. If you accept the following card types, add the corresponding parameters and specify the settings you received from your financial institution in Step 1 of this process:

   AS American Express SE Number (e.g., \AS1234567890\)

   DS Discover SE Number – Last 10 digits (e.g., \DS3456789011\)

   IS Diners Club SE Number (e.g., \IS1234567890\)

   BS Carte Blance SE Number (e.g., \BS1234567890\)

   JS JCB SE Number – Drop the first four digits and the last digit (e.g., \JS5678901111\)

5. If you are processing checks, add the following parameter and specify the appropriate setting for your check processor:

   CS Certegy Station Number or TeleCheck SE Number

NOTE: If you are processing checks with TeleCheck, follow the instructions outlined in Step 2 – Route checks, starting on page 21, to determine your TeleCheck SE Number.

6. If you are processing checks with Certegy, add the CK parameter and specify whether you are using Certegy East (E) or Certegy West (W). For example, if you are processing with Certegy East, enter the following setting:

   \CKE\

NOTE: You do not need to add this parameter if you are processing checks with TeleCheck.

7. If your modem requires an initialization string, add the MI parameter to SYNEDC.CFG in the following format, where xxxxx is the initialization string for your modem:

   \MIATxxxxx\

   For example, if you are using a US Robotics Sportster Non-V.90 modem, you would enter the following setting:

   \MIAT&D2&K0&M0\

   Refer to Modem configuration and troubleshooting on page 69 for information about modem initialization strings, including a list of initialization strings for specific modems and instructions for determining the initialization string for other modems.

8. Save your changes and close the SYNEDC.CFG file.

There may be additional parameters that you need to add to your SYNEDC.CFG file, depending on your configuration. The SYNEDC.CFG file includes comments that describe the parameters that are available for your processor. If your financial institution provides you with any of these additional settings, you should add them to your SYNEDC.CFG file.

Paymentech

If you are processing with Paymentech, follow these steps to edit your SYNEDC.CFG file:

1. Copy the WINPMT.CFG file in your top-level CounterPoint directory to SYNEDC.CFG using one of the following commands:

   Windows: COPY WINPMT.CFG SYNEDC.CFG

   Unix/Linux: cp WINPMT.CFG SYNEDC.CFG

2. Open SYNEDC.CFG in Notepad or another text editor.

3. Add the following parameter to the SYNEDC.CFG file and specify the appropriate setting:

   MZ Merchant ZIP Code (e.g., \MZ38138\)

4. If your modem requires an initialization string, add the MI parameter to SYNEDC.CFG in the following format, where xxxxx is the initialization string for your modem:

   \MIATxxxxx\

   For example, if you are using a US Robotics Sportster Non-V.90 modem, you would enter the following setting:

   \MIAT&D2&K0&M0&C1&N2\

   Refer to Modem configuration and troubleshooting on page 69 for information about modem initialization strings, including a list of initialization strings for specific modems and instructions for determining the initialization string for other modems.

5. Save your changes and close the SYNEDC.CFG file.

There may be additional parameters that you need to add to your SYNEDC.CFG file, depending on your configuration. The SYNEDC.CFG file includes comments that describe the parameters that are available for your processor. If your financial institution provides you with any of these additional settings, you should add them to your SYNEDC.CFG file.

Radiant Payment Services/RBS Lynk

If you are processing with Radiant Payment Services or RBS Lynk, follow these steps to edit your SYNEDC.CFG file:

1. Copy the WINLNK.CFG file in your top-level CounterPoint directory to SYNEDC.CFG using one of the following commands:

   Windows: COPY WINLNK.CFG SYNEDC.CFG

   Unix/Linux: cp WINLNK.CFG SYNEDC.CFG

2. Open SYNEDC.CFG in Notepad or another text editor.
3. Add the following parameters to the SYNEDC.CFG file and specify the appropriate settings for each:

   MN Merchant name (e.g., \MNCamptownGolf\)

   MC Merchant city (e.g., \MCMEMPHIS\)

   MS Merchant state (e.g., \MSTN\)

   MZ Merchant ZIP Code (e.g., \MZ38138\)

   MP Merchant phone number (e.g., \MP800-123-4567\)

NOTE: You can use whatever phone number format you prefer—up to 15 characters—for the MP parameter.

4. Add the following parameters and specify the settings you received from your financial institution in Step 1 of this process:

   PL Plan Number/Category Code (e.g., \PL1234\)

   AG Agent Number (e.g., \AG123456\)

   CH Chain Number (e.g., \CH654321\)

   ST Store Number, followed by Terminal Number (e.g., \ST67895555\)

   CC (Optional) Currency Code (e.g., \CC321\)

   LN (Optional) Merchant Location Number (e.g., \LN54321\)

   TS (Optional) “V” Number (e.g., \71234567\)

   NOTE: Replace the V prefix in your “V” Number with a 7, for a total of eight digits.

   TZ Time Zone (e.g., \TZ706\)

NOTE: If your bank did not provide you with a Time Zone setting, find your time zone in the following table and specify the corresponding setting in the TZ parameter.

Time zone	Setting
Eastern Standard Time (EST)	705
Central Standard Time (CST)	706
Mountain Standard Time (MST)	707
Pacific Standard Time (PST)	708

5. If your modem requires an initialization string, add the MI parameter to SYNEDC.CFG in the following format, where xxxxx is the initialization string for your modem:

   \MIATxxxxx\

   For example, if you are using a US Robotics Sportster Non-V.90 modem, you would enter the following setting:

   \MIAT&D2&K0&M0&C1&N2\

   Refer to Modem configuration and troubleshooting on page 69 for information about modem initialization strings, including a list of initialization strings for specific modems and instructions for determining the initialization string for other modems.

6. Save your changes and close the SYNEDC.CFG file.

Step 11 – Set up stores

When you have added the necessary settings to your SYNEDC.CFG file, make sure that you have set up your stores in CounterPoint and defined the necessary pay codes in Setup / Point of Sale / Stores / Stores.

For each store, you must define at least one pay code of the type Credit crd before you can configure draft capture settings for credit card processing. You can create a separate pay code for each type of credit card you will accept, or you can define a single pay code for all credit cards.

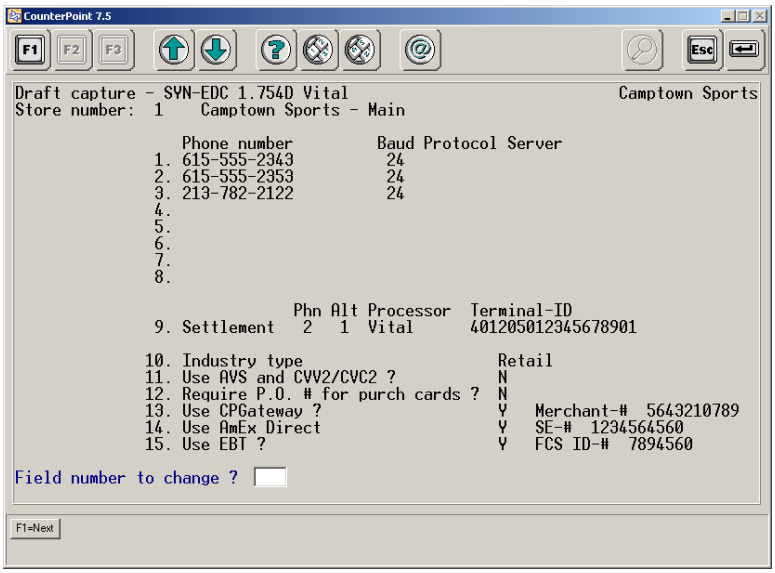
If you are processing checks, you must define a Check pay code, as well. If you are processing debit cards, you must also define a Debit card pay code. Finally, if you processing EBT food stamp transactions, you must define an EBT pay code.

Refer to Stores in the CounterPoint Electronic Documentation for more information about setting up your stores, including instructions for defining pay codes.

Step 12 – Set up draft capture

When you have defined the necessary pay code for each method of payment you accept, follow these steps to define your draft capture settings:

1. Start CounterPoint and select Setup / Point of Sale / Stores / Draft Capture.



2. Enter the Store number of the store for which you want to define draft capture settings.
3. Enter a Phone number to use for the authorization or settlement of draft capture transactions, and then specify the Baud rate to use with that phone number.
4. If you are processing with First Data South (NaBANCO) through the Western Union packet network, enter W in the Protocol field. Otherwise, leave this field blank.
5. If you are using the Modem Server Option, enter a Sever Group ID to assign to the phone number in the Server field. The Server Group ID identifies the phone number that the Modem Server should dial.

   Refer to Modem Server in the CounterPoint Electronic Documentation for more information about Server Group IDs.

   NOTE: You can define up to eight phone numbers for your processor.
6. In the Phn field, enter the number that corresponds to the primary phone number to dial for batch settlement.
7. In the Alt field, enter the number that corresponds to the alternate phone number to dial for batch settlement, in case the primary phone number is unavailable.
8. Enter the Terminal-ID to use for batch settlement. The value you should enter in this field depends on the processor you are using. Refer to the appropriate section for your processor following these steps (beginning on page 43) for more information about determining the Terminal-ID value to use.

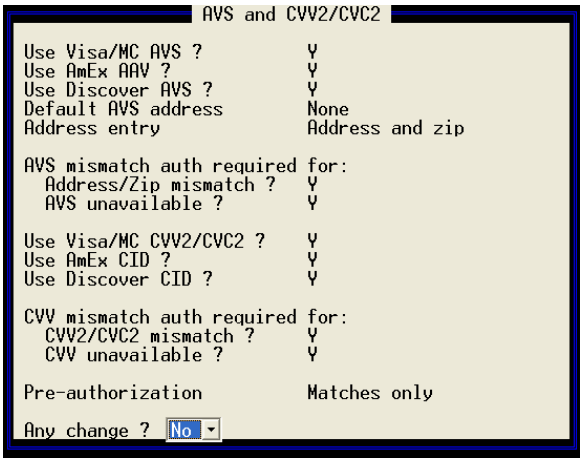
9. Select the appropriate Industry type for your business to obtain the most favorable processing rates.

   Refer to Industry types on page 6 for more information about the available Industry type options.

10. If you want to use address verification and CVV2/CVC2/CID for “card not present” transactions, do the following:

    Select the Use AVS and CVV2/CVC2 ? field to display the AVS and CVV2/CVC2 window.

    NOTE: If you are processing with NaBANCO, you cannot access the Use AVS and CVV2/CVC2 field.



    Select Yes from Use Visa/MC AVS ? to enable Address Verification Service (AVS) for Visa and MasterCard transactions.

    Select Yes from Use AmEx AAV ? to enable Automated Address Verification (AAV) for American Express transactions.

    Select Yes from Use Discover AVS ? to enable address verification for Discover transactions.

    Select Bill-to, Ship-to, or None as the Default AVS address.

    Select one of the following Address entry options to specify whether users must enter address information for transactions for which you have enabled address verification:

    - Address and zip – Select this option to require users to enter each customer’s address and ZIP Code.
    - Zip only – Select this option to allow users to skip the Address field on the Address Verification window in Ticket Entry or Touchscreen Ticket Entry and enter each customer’s ZIP Code only.
    - None – If you set the Default AVS address field to Bill-to or Ship-to, you can select this option to require users to enter address information only if a default address is not on file for a customer.

    NOTE: Users can press F2 in Ticket Entry and Touchscreen Ticket Entry when they are prompted to enter a customer’s Address and/or Zip to skip address entry.

If you are processing with First Data North, TSYS (Vital), RBS Lynk, or PNC Merchant Services, select one of the following Pre-authorization ? options to specify whether you want to pre-authorize each transaction to verify the cardholder's address before authorizing the charge:

- None – Select this option to disable the pre-authorization of credit card transactions.
- Matches only – Select this option to only allow pre-authorized transactions for which the provided address matches the cardholder's AVS information. With this setting, CounterPoint sends a zero-dollar transaction to the processor. If the provided address matches the cardholder's AVS information, CounterPoint obtains an authorization for the actual charge amount.
- Matches and unavailable – Select this option to allow pre-authorized transactions for which the provided address matches the cardholder's AVS information, and to allow users to proceed with transactions when the appropriate AVS service is unavailable.

Select Yes from Address/Zip mismatch ? and/or AVS unavailable ? to require a security override to proceed with a credit card transaction when the supplied address and ZIP Code don't match or when address verification is unavailable.

NOTE: You can authorize users to perform security overrides for mismatched address verification information from the Point of Sale Authorizations screen in Setup / System / Users.

Select Yes from Use Visa/MC CVV2/CVC2 ? to request CVV2/CVC2 information for Visa and MasterCard transactions, in addition to or instead of address verification information.

Select Yes from Use AmEx CID ? to request CID information for American Express transactions, in addition to or instead of address verification information.

Select Yes from Use Discover CID ? to request CID information for Discover transactions, in addition to or instead of address verification information.

Select Yes from CVV2/CVC2 mismatch ? and/or CVV unavailable ? to require a security override to proceed with a credit card transaction when the supplied CVV2/CVC2 or CID digits don't match or when the CVV2/CVC2/CID service is unavailable.

NOTE: You can authorize users to perform security overrides for mismatched CVV2/CVC2/CID information from the Point of Sale Authorizations screen in Setup / System / Users.

Select No from Any change ? to save your settings, close the AVS and CVV2/CVC2 window, and return to the Draft capture screen.

Refer to Address verification and CVV2/CVC2/CID on page 9 for more information about the features and advantages of using AVS and CVV2/CVC2.

11. If you are processing purchase cards, select Yes from Require P.O. # for purch cards ? to ensure that you receive the preferential rate for purchase cards.

WARNING! This setting is **very important** if you are using purchase cards! A non-blank PO # **MUST** be recorded for each purchase card authorization. If a blank PO # is sent, your processor will charge a billback fee (typically 0.5% to 1.0% of the transaction amount) for incomplete data.

12. If you are using CPGateway, leave Use CPGateway ? set to No until you finish your draft capture settings and device codes, and you have successfully tested dial-up authorizations.

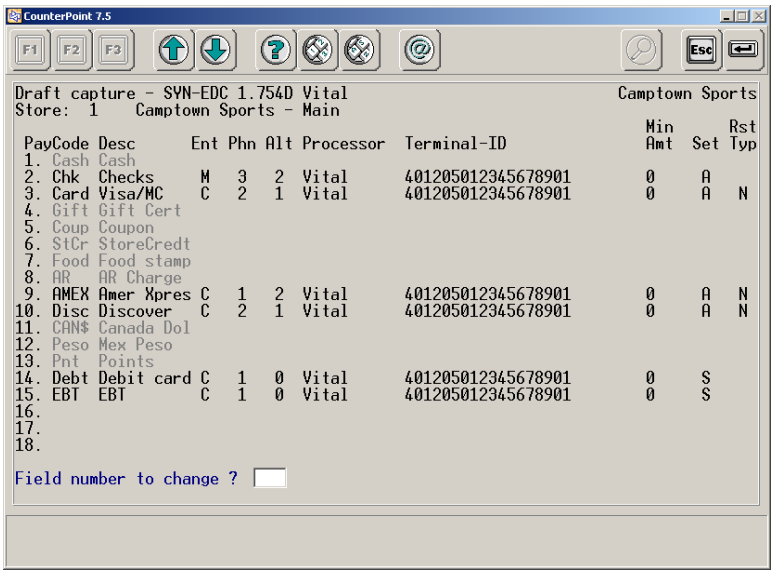
13. If you are using CPGateway, select Yes from Use AmEx Direct to authorize American Express transactions directly through American Express, and then enter your 10-digit American Express SE number in the SE-# field.

    NOTE: If you select Yes from Use AmEx Direct, you **MUST** specify an SE-# value.

14. If you are using CPGateway and you are processing EBT food stamp transactions, select Yes from Use EBT ?, and then enter your 7-character Food and Consumer Service Identifier in the FCS ID-# field.

    NOTE: The Use EBT ? and FCS ID-# fields are available only if your Industry type setting is Retail and you are using a processor for which CounterPoint supports EBT food stamps (i.e., TSYS, First Data North, or RBS Lynk).

15. Press Enter at Field number to change ? to proceed to the second Draft capture screen.



16. To define draft capture settings for the credit card, debit card, check, and EBT pay codes you have defined, do the following:

    Select a credit card, debit card, check, or EBT pay code to edit, and then select either Card/check reader or Manual from the Ent field to define the entry method for transactions processed with the pay code.

    NOTE: You cannot select Manual for Debit card pay codes.

    In the Phn field, enter the number that corresponds to the primary phone number to dial to obtain authorizations for the pay code.

    In the Alt field, enter the number that corresponds to the alternate phone number to dial to obtain authorizations for the pay code, in case the primary phone number is unavailable.

Enter the Terminal-ID to use to obtain authorizations for the pay code. The value you should enter in this field depends on the processor you are using and the type of pay code you are defining. Refer to the appropriate section for your processor following these steps (beginning on page 43) for more information about determining the Terminal-ID value to use.

Enter the minimum amount for which authorizations are required in the Min Amt field.

NOTE: For Debit card and EBT pay codes, the Min Amt field is set to 0 by default and cannot be changed.

From the Set field, select Authorize and Settle to electronically authorize and settle transactions processed with the pay code or Authorize only to electronically authorize, but not settle, charges for the pay code.

If you select Authorize only, you must deposit credit card slips at your bank to receive payment for credit card transactions.

NOTE: For Check pay codes, this field is set to Authorize only (A) by default. For Debit card and EBT pay codes, this field is set to Authorize and Settle (S) by default. These values cannot be changed.

For a credit card pay code, select Yes from the Rst Type column if you want to restrict the pay code to a particular type of card, and then select the cards you want to allow from the Cards allowed window.

NOTE: Repeat this step for each credit card, debit card, check, and EBT pay code to configure draft capture settings for all of the appropriate pay codes.

17. Press Enter at Field number to change ? to save your draft capture settings.

NOTE: Repeat these steps for each store for which you want to define draft capture settings.

First Data North

If you are processing with First Data North, use the same Terminal-ID value for credit cards and for checks, regardless of which check processor you are using.

Use the table below to build a valid Terminal-ID—using the information you obtained from PNC Merchant Services or your financial institution—in the following format:

P.BBBMMMMMMMMMTTTTTT

Terminal-ID Element	Value
P.	2-character merchant type indicator: E. Retail merchant M. MOTO or Ecommerce merchant T. Multi-transaction retail merchant W. Multi-transaction MOTO or Ecommerce merchant NOTE: Always use E. for the settlement Terminal-ID.
BBB	3-digit Bank Code
MMMMMMMMM	9-digit Merchant ID
TTTTTT	Optional 6-digit Terminal ID for multi-register/multi-location merchants

For example, if you are a multi-location retail merchant with a Bank Code of 333, a Merchant ID of 987654321, and a multi-location Terminal ID of 9999999, your Terminal-ID for credit card authorization and check verification (i.e., credit card and check pay codes), would be:

T.333987654321999999

NOTE: You would use the same Terminal-ID for credit card settlement, but substitute E. for the merchant type indicator (i.e., E.333987654321999999).

TSYS

If you are processing with TSYS (Vital), use the same Terminal-ID value for credit cards and for checks, regardless of which check processor you are using.

Use the table below to build a valid 18-digit Terminal-ID—using the information you obtained from your financial institution—in the following format:

BBBBBBMMMMMMMMMMMM

Terminal-ID Element	Value
BBBBBB	6-digit BIN #
MMMMMMMMMMMM	12-digit Merchant Number

For example, if your BIN # is 401205 and your Merchant Number is 012345678901, your Terminal-ID for credit card authorization and settlement, and for checks, would be:

401205012345678901

NOTE: Use this Terminal-ID for all credit card—including Visa, MasterCard, American Express, and all other credit card types—and check pay codes.

First Data South

If you are processing with First Data South (formerly NaBANCO), simply use the 11-digit Merchant Number you received from your financial institution as the Terminal-ID for credit card authorization and settlement, and for checks.

Paymentech

If you are processing with Paymentech, you will use the same Terminal-ID value for all credit card transactions.

Credit cards
Use the table below to build a valid 19-digit Terminal-ID—using the information you obtained from your financial institution—in the following format for all credit card transactions:

CCCCMMMMMMMMMMMMTTT

Terminal-ID Element	Value
CCCC	4-digit Client Number
MMMMMMMMMMMM	12-digit Merchant Number
TTT	3-digit Terminal Number

For example, if your Client Number is 0001, your Merchant Number is 999999999999 and your Terminal Number is 421, your Terminal-ID for credit card authorization and settlement would be:

0001999999999999421

Radiant Payment Services/RBS Lynk

If you are processing with Radiant Payment Services or RBS Lynk, use the same Terminal-ID value for credit cards and for checks.

Use the table below to build a valid 18-digit Terminal-ID—using the information you obtained from your financial institution—in the following format:

BBBBBBMMMMMMMMMMMM

Terminal-ID Element	Value
BBBBBB	6-digit BIN #
MMMMMMMMMMMM	12-digit Merchant Number

For example, if your BIN # is 401205 and your Merchant Number is 012345678901, your Terminal-ID for credit card authorization and settlement would be:

401205012345678901

Step 13 – Set up device codes and registers

When you have defined draft capture settings for each of your stores, you must define device codes for each modem, MSR card reader, PIN pad (if you are processing debit cards and/or EBT food stamps), and MICR check reader (if you are processing checks) that you will be using to process EDC transactions. Use Setup / Point of Sale / Device codes to define the necessary device codes for these devices.

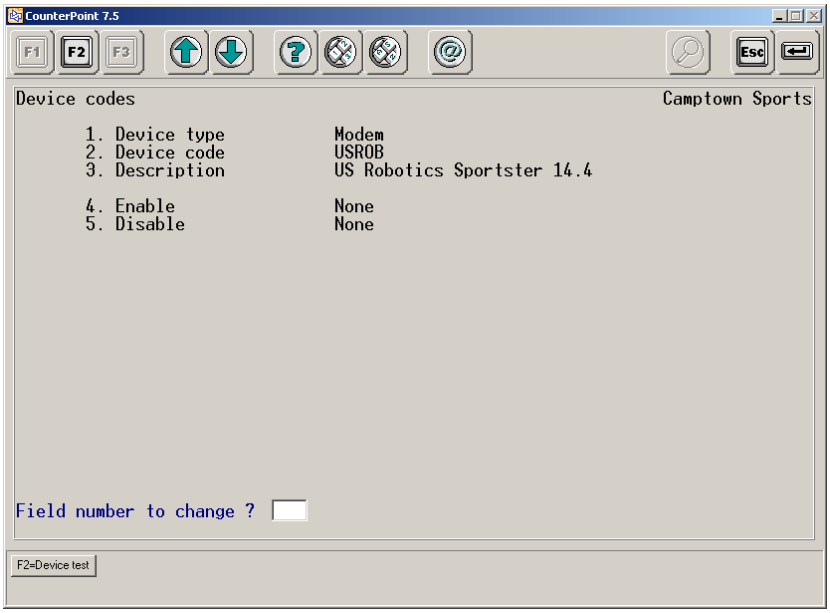
When you are finished setting up your device codes, use Setup / Point of Sale / Registers to assign the appropriate device codes to the workstation to which the corresponding devices are connected.

Refer to Device Codes in the CounterPoint Electronic Documentation for detailed information about setting up various types of device codes. Refer to Registers for information about assigning device codes to each CounterPoint workstation.

Modems

Use Setup / Point of Sale / Device codes to define a device code for each of your modems, and then use Setup / Point of Sale / Registers to assign each Modem device code to the appropriate workstation.

CounterPoint supports a broad range of modems from a variety of manufacturers, many of which are listed in Modem configuration and troubleshooting on page 69. For example, the following screen illustrates valid device code settings for a US Robotics Sportster 14.4 Non-V.90 modem.

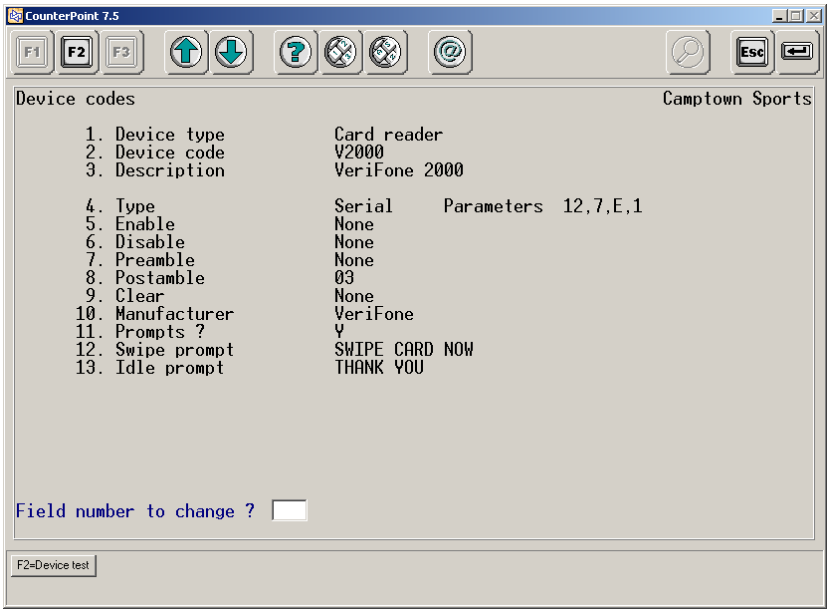


Each Modem device code should include the appropriate Enable and Disable codes for the type of modem you are defining. Refer to Modem configuration and troubleshooting on page 69 and the manufacturer's recommendations for more information about determining the appropriate Enable and Disable codes for a particular modem.

Card readers

Use Setup / Point of Sale / Device codes to define a device code for each MSR card reader that is connected to a CounterPoint workstation, and then use Setup / Point of Sale / Registers to assign each Card reader device code to the appropriate workstation.

CounterPoint supports MSR card readers from a variety of manufacturers. For example, the following screen illustrates device code settings for a VeriFone 2000 card reader.



For each Card reader device code you define, do the following:

- Select Serial or Keyboard from the Type field to specify the device type.
- For Serial devices, specify the appropriate communication Parameters (i.e., baud, data bits, parity, and stop bits). Leave the Parameters field blank if the communication parameters for the card reader will be set externally.

NOTE: For VeriFone 1000/1000SE/2000 MSRs, enter 12, 7, E, 1 in the Parameters field.

For VeriFone Everest/Omni MSRs, enter 96, 8, N, 1 in the Parameters field.

For VeriFone MX800 series MSRs, use the Set externally setting.

- Enter any necessary Enable and Disable codes, Preamble or Postamble values, or Clear code that the device requires. The Enable, Disable, and Clear fields are only available for Serial devices.

  For Track 1 readers, enter a Preamble value of 25 and a Postamble value of 3F. For Track 2 readers, enter a Preamble of 3B and a Postamble of 3F.

  NOTE: VeriFone card readers require a Postamble, which can be any hexadecimal value.

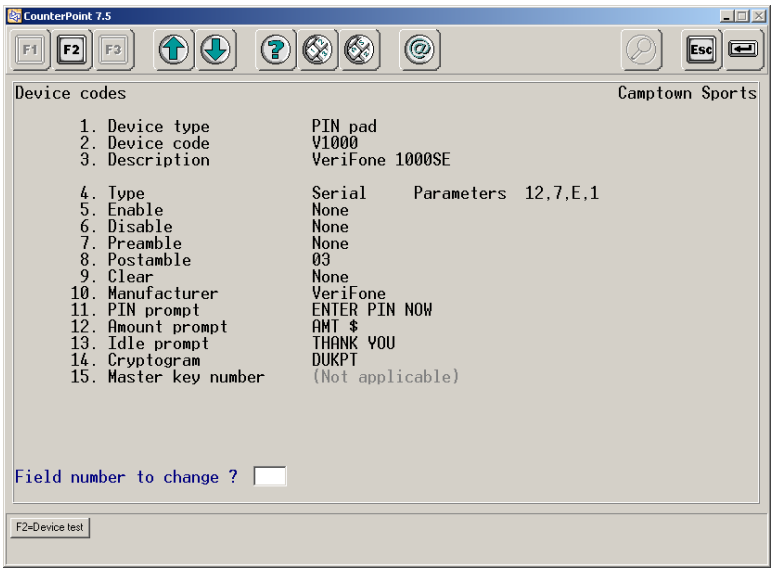
- For Serial devices, select the Manufacturer, either VeriFone or Other.
- Specify whether you want the card reader to display text prompts to the customer from the Prompts ? field, and then enter the Swipe prompt and Idle prompt values that you want to appear on the card reader.

PIN pads

Skip this section if you are not processing debit cards or EBT food stamps.

Use Setup / Point of Sale / Device codes to define a device code for each PIN pad you are using to process debit cards and/or EBT food stamps, and then use Setup / Point of Sale / Registers to assign each PIN pad device code to the appropriate workstation.

CounterPoint supports the PIN pads listed on page 12 for use with debit cards and/or EBT food stamps. The following screen illustrates a valid device code for a VeriFone 1000SE PIN pad.



For each PIN pad device code you define, do the following:

- Specify the appropriate communication Parameters (i.e., baud, data bits, parity, and stop bits) for the device. Leave the Parameters field blank if the communication parameters for the card reader will be set externally.

NOTE: For VeriFone 1000/1000SE/2000 MSRs, enter 12, 7, E, 1 in the Parameters field.

For VeriFone Everest/Omni MSRs, enter 96, 8, N, 1 in the Parameters field.

For VeriFone MX800 series MSRs, use the Set externally setting.

- Enter any Enable and Disable codes, Preamble or Postamble values, and/or Clear code that the device requires.

NOTE: VeriFone PIN pads require a Postamble, which can be any hexadecimal value.

- Select the appropriate Manufacturer option for the device, either VeriFone or Other.
- Enter the PIN prompt, Amount prompt, and Idle prompt values to specify the text you want to appear on the PIN pad at each stage of the PIN entry process.

NOTE: The PIN prompt and the Amount prompt are displayed alternately when the PIN is requested. Each prompt is displayed for a few seconds until the customer enters the PIN, at which point the prompts are replaced by asterisks.

- Leave the Cryptogram field blank to use DUKPT encryption.

VeriFone Everest Plus PIN pad

If you are using a VeriFone Everest Plus PIN pad, you must load the VeriFone Multi-Pay application onto the device to configure it to work with CounterPoint. Follow these steps:

1. Download Multi-Pay application (MultiPayEverest.zip) from the Other Downloads page in the Support area of the CounterPoint website (www.counterpointpos.com/support).

NOTE: You must be a current CSS subscriber to access and download files from the Support area of the CounterPoint website.

2. Extract the MultiPayEverest.zip file into a temporary directory.
3. Connect the Everest PIN pad to the COM1 port on your computer.

NOTE: If you need to connect to the COM2 port instead, edit the d.bat file (located in the directory to which you extracted the MultiPayEverest.zip file) and change the -p1 parameter to -p2 (or another valid COM port)

4. On your PIN pad, hold down the 7 key and the Enter key simultaneously. The message PSWD? appears on the display.
5. Enter 166831 (the default password) on your PIN pad.
6. Press the Enter key twice. The message Function? Downld appears on the display.
7. Press the Enter key again. The message Port? Port 1 appears on the display. Press the Up Arrow key on the right-hand side of the PIN pad (above the EBT key) until Port 3 appears on the display.
8. Press the Enter key. The message AutoBaud Check appears on the display while the device is waiting to load the Multi-Pay application.
9. On your computer, open a command prompt, go to the temporary directory to which you extracted the MultiPayEverest.zip file, and then run d.bat to load the Multi-Pay application on the PIN pad.

   While the Multi-Pay application is loading, the command prompt window and the PIN pad both display the file name and packet count for the application. When the application is loaded, the message Function? Downld appears on the PIN pad display.

10. Press the Clear key to restart the PIN pad.

VeriFone Omni 7000 PIN pad

If you are using a VeriFone Omni 7000 PIN pad, you must load the VeriFone Multi-Pay application onto the device to configure it to work with CounterPoint. Follow these steps:

1. Download Multi-Pay application (MultiPayOmni7000.zip) from the Other Downloads page in the Support area of the CounterPoint website (www.counterpointpos.com/support).

NOTE: You must be a current CSS subscriber to access and download files from the Support area of the CounterPoint website.

2. Extract the MultiPayOmni7000.zip file into a temporary directory.
3. Connect the Omni 7000 PIN pad to the COM1 port on your computer.

NOTE: If you need to connect to the COM2 port instead, edit the MP07K02R.bat file (located in the directory to which you extracted the MultiPayOmni7000.zip file) and change the -p1 parameter to -p2 (or another valid COM port).

4. On your PIN pad, hold down the 7 key and the Enter key simultaneously. The message Enter Password? appears on the display.
5. Enter 166831 (the default password) on your PIN pad. The options Help and Download appear on the display.
6. Press the F4 key to select the Download option. The message Select COM Port? appears on the display, along with the COM1, COM2, and COM3 options.
7. Press the F3 key to select the COM3 option. The message Download Type? appears on the display, along with the Partial and Full options.
8. Press the F4 key to select the Full option. The message Unit Receive, COM3 AutoBaud, Clear to Abort appears on the display while the device is waiting to load the Multi-Pay application.
9. On your computer, open a command prompt, go to the temporary directory to which you extracted the MultiPayOmni7000.zip file, and then run MP07K02R.bat to load the Multi-Pay application on the PIN pad.

   While the Multi-Pay application is loading, the command prompt window displays the file name and packet count for the application and the PIN pad displays a progress bar of asterisks. When the application is loaded, the Help and Download options appear on the PIN pad display.
10. Press the Clear key to restart the PIN pad.
11. In the SYNRUN.SYN file, located in the CounterPoint top-level directory, set the environment variable CPVPRESET to Y. Refer to Environment Variable Setup in the CounterPoint Electronic Documentation for more information on using environment variables.

VeriFone MX800 series PIN Pad

If you are using a VeriFone MX800 series PIN pad, you must first load the VeriFone MX800 Series Service Pack and Form Agent software onto the device. Follow these steps to do this:

1. Download the VeriFone MX800 Series Service Pack and Form Agent software (mpmxseries.2008-12-08.zip) from the Other Downloads page in the Support area of the CounterPoint Web site (www.counterpointpos.com/support).
2. Extract the mpmxseries.2008-12-08.zip file to a temporary directory.
3. Connect your MX800 series PIN pad to the COM1 port on your computer.

NOTE: If you need to connect to the COM2 port instead, edit the down_sp.bat and down_fa.bat files (located in the directory to which you extracted the mpmxseries.2008-12-08.zip file) and change the -p1 parameter to -p2 (or another valid COM port).

4. On your PIN pad, hold down the 7 key and the Enter key simultaneously. The message Enter Password? appears on the display.
5. Enter 166831 (the default password) on your PIN pad. The options Help and Download appear on the display.
6. Press the F4 key to select the Download option. The message Select COM Port? appears on the display, along with the COM1, COM2, and COM3 options.
7. Press the F3 key to select the COM3 option. The message Download Type? appears on the display, along with the Partial and Full options.
8. Press the F4 key to select the Full option. The message Unit Receive, COM3 AutoBaud, Clear to Abort appears on the display while the device is waiting to load the Multi-Pay application.
9. On your computer, open a command prompt, go to the temporary directory to which you extracted the mpmxseries.2008-12-08.zip file, and then run down_sp.bat to load the Service Pack onto the PIN pad.

   While the Service Pack is loading, the command prompt window displays the file name and packet count for the application and the PIN pad displays a progress bar of asterisks. When the Service Pack is loaded, the Help and Download options appear on the PIN pad display.
10. Press the F4 key, the F3 key, and the F4 key again, and then run down_fa.bat to load the Form Agent software onto the PIN pad. When the application is loaded, the Help and Download options appear on the PIN pad display.
11. Press the Clear key to restart the PIN pad.
12. In the SYNRUN.SYN file, located in the CounterPoint top-level directory, set the following environment variables:

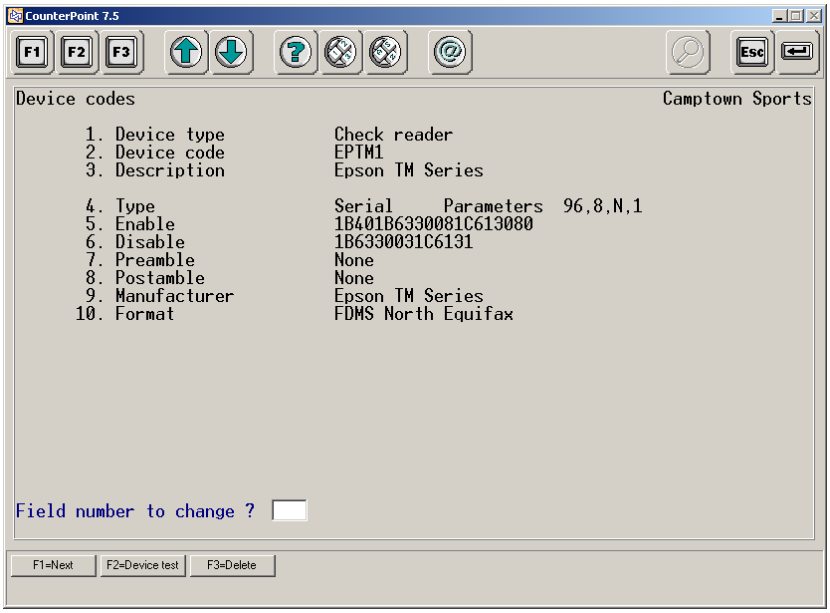
    - CPVPRESET=Y
    - TRACKS=2

    Refer to Environment Variable Setup in the CounterPoint Electronic Documentation for more information on using environment variables.

Check readers

Use Setup / Point of Sale / Device codes to define a device code for each MICR check reader you are using to process check transactions, and then use Setup / Point of Sale / Registers to assign each Check reader device code to the appropriate workstation.

CounterPoint supports MICR check readers from a variety of manufacturers, including IBM, Epson, MagTek, and others. Each check reader you define requires specific device code settings. For example, the following screen illustrates valid device code settings for an Epson TM series check reader.



For each Check reader device code you define, do the following:

- Select Serial or Keyboard from the Type field to specify the type of device you are configuring.
- For Serial devices, specify the appropriate communication Parameters (i.e., baud, data bits, parity, and stop bits). Leave the Parameters field blank if the communication parameters for the card reader will be set externally.

  Refer to the manufacturer's recommendations for more information about setting communication parameters for your check reader.
- For Serial devices, enter any Enable and/or Disable codes that the device requires.
- For Serial or Keyboard devices, enter any Preamble and/or Postamble values that the device requires.

  NOTE: The Certegy/CheckMate check reader requires a Preamble value of 02 and a Postamble value of 03. The Soricon MR2000 check reader requires a Postamble value of 0D.
- Select the appropriate Manufacturer option for the device, either IBM SureMark Series, Epson TM Series, or Other.
- Select the appropriate Format for the device. The Format you select depends on the credit card processor and check processor you are using, as described below:

First Data North

If you are using Certegy with First Data North, select FDMS North Equifax from the Format field for all MICR check readers, regardless of the manufacturer.

If you are using TeleCheck with First Data North or PNC Merchant Services, select FDMS North TeleCheck from the Format field for all MICR check readers, regardless of the manufacturer.

TSYS/First Data South/Radiant Payment Services/RBS Lynk

If you are using Certegy, select Equifax from the Format field for all MICR check readers, regardless of the manufacturer.

If you are using TeleCheck, select TOAD from the Format field for all MICR check readers, regardless of the manufacturer.

NOTE: RPS/RBS Lynk does not support check authorization through TeleCheck.

Step 14 – Test dial-up authorization

Using Point of Sale / Tickets / Enter, swipe a card and obtain a dial-up authorization to confirm that your CounterPoint system is processing credit card transactions correctly. If you are unable to obtain a live authorization from your credit card processor, verify your settings in Setup / Point of Sale / Stores / Draft capture and try to obtain an authorization again.

If you are still unable to obtain an authorization, step through the configuration process again, double-checking your processor information, your WINEDC and SYNEDC.CFG settings, your device codes, and your draft capture settings.

If you are processing checks, you should also test a check transaction to ensure that your check reader(s) and your draft capture settings for your check pay codes are working.

NOTE: No additional configuration or testing should be necessary if you are using the Modem Server Option. However, you should make sure that your Modem Server is running in Point of Sale / Draft capture / Modem server before you attempt to authorize live transactions. Refer to Modem Server in the CounterPoint Electronic Documentation for more information about setting up and using the Modem Server Option.

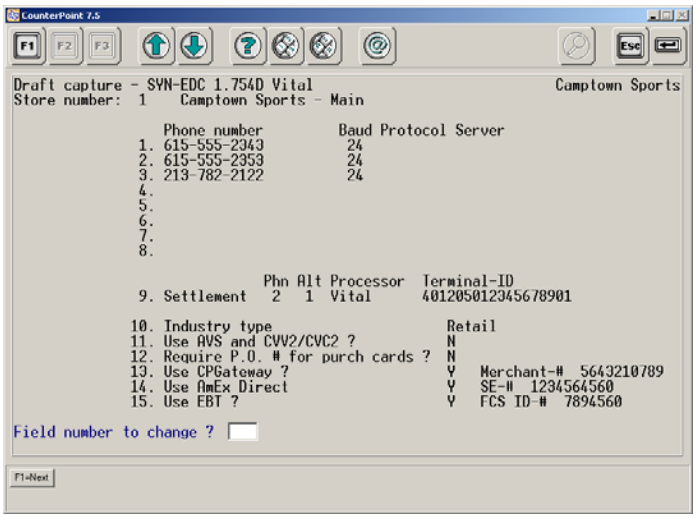
Step 15 – Test CPGateway authorization

Skip this step if you aren't using CPGateway.

If you are using CPGateway, follow these steps to test your connection to CPGateway and confirm that you can obtain credit card authorizations over the Internet.

Configure draft capture for DEMO CPGateway operation

From Setup / Point of Sale / Stores / Draft capture, select Yes from the Use CPGateway ? field, and then enter DEMO in the Merchant-# field.



Reconfirm your Internet connection

In an earlier step, you confirmed that your CounterPoint workstation could access the Internet. If you have changed your workstation's configuration at all since that step, you may wish to reconfirm that your workstation can still connect to the Internet.

Test a DEMO transaction

Using Ticket Entry, enter a test transaction. You should receive a message from CPGateway that the simulated transaction was authorized (e.g., OKDEMO), or that it was declined (e.g., DECLINE DEMO). Either of these messages indicates a successful test.

NOTE: About 80% of test authorizations are successful.

Make sure that you void any tickets for transactions that you authorize using the DEMO CPGateway Merchant-# to prevent them from being settled with live transactions.

Configure draft capture for live CPGateway operation

From Setup / Point of Sale / Stores / Draft capture, select Yes from the Use CPGateway ? field, and then enter your actual CPGateway Merchant #, which you obtained from www.CPGateway.com in Step 4 of the configuration process.

Test a live transaction

Using Ticket Entry, enter a live transaction and authorize it through CPGateway to ensure that you can obtain a live authorization from your processor through the Internet.

Test automatic dial-up failover

If you are using CPGateway and a dial-up connection (either a locally-connected modem or the Modem Server Option), CounterPoint will automatically failover to your dial-up connection if there is a problem with your Internet connection. To test dial-up failover, you must first disable your Internet connection.

When you are sure that your Internet connection is disabled, enter another CPGateway test transaction in Ticket Entry. CounterPoint should automatically failover to your dial-up connection and obtain an authorization directly from your processor. You will experience some delay as your workstation makes multiple attempts to locate the CPGateway host.

You may perform an additional test using the CPGateway status utility. Select Point of Sale / Draft capture / CPGateway status, press F2 to disable CPGateway, and then enter another test transaction in Ticket Entry. Again, CounterPoint should automatically failover to your dialup connection. When the test is complete, press F2 again from Point of Sale / Draft capture / CPGateway status to re-enable CPGateway.

WARNING! Remember to restore your Internet connection when you complete this test!

NOTE: During actual operation, if your Internet service is down for an extended period of time, you may wish to disable CPGateway until the service is restored. Select Point of Sale / Draft capture / CPGateway status and press F2 to disable CPGateway. When your Internet connection is available again, repeat this step to re-enable CPGateway.

The default Internet connection timeout setting is 10 seconds. You can change the connection timeout setting and control how many times CounterPoint will retry the TCP/IP connection by creating a file named CPGATE.CFG in the top-level CounterPoint directory and adding the following parameters:

Parameter	Description
CONNECTTIMEOUT	Connection timeout in seconds.
MAXCONNECTATTEMPTS	Number of times (1 or greater) to retry the TCP/IP connection for each server.

Remove test authorization transactions

You may use Ticket Entry to void the tickets that you authorized during testing to prevent them from being settled with actual transactions.

Alternatively, if you feel that you need to test settlement of the authorized transactions, you may use Point of Sale / Draft capture / Settle to settle those transactions.

Additional topics

Changing EDC configuration defaults

CounterPoint uses the file CPGATE.CFG in your top-level CounterPoint directory (e.g., C:\SYN) to set configuration defaults and to track additional EDC information. For most installations, these defaults do not need to be changed.

If you need to change the default values, you may use a text editor to edit CPGATE.CFG. If CPGATE.CFG does not exist in your company directory, you may create it, making sure to include the required first line [EDCConfig] and the configuration defaults that you need to change.

Values can be changed from the default by entering the appropriate label and value in the [EDCConfig] section of the file, such as:

```
MaxConnectAttempts=1
```

MaxConnectAttempts
The default value is 1 attempt per server.

The number of times that CounterPoint will attempt to contact each CPGateway server is controlled by this setting. With setting of 1, CounterPoint will attempt to reach primary.cpgateway.com once, then will attempt secondary.cpgateway.com once, then failover to a dial-up connection.

ConnectTimeout
The default value is 10 seconds. After CounterPoint establishes a TCP/IP connection, it will wait a certain amount of time until it receives an acknowledgement from the CPGateway server. The wait time is controlled by this setting.

If CPGateway does not respond within the time limit, CounterPoint will try the secondary path. If the secondary does not respond within the time limit, CounterPoint will prompt for dial-up operation.

We do not recommend changing ConnectTimeout. If you do need to change it, be aware that setting it too low could cause timeouts even when the Internet connection is temporarily slow or congested.

NOTE: In actual operation, if you have an extended outage of Internet service, you may wish to use Point of Sale / Draft Capture / CPGateway status to disable CPGateway until your service is restored.

ReceiveTimeout
The default value is 60 seconds.

LastConnectFailure (in a [servername] section)
This is the timestamp of the last failure for any server (either a CPGateway server or dial-up server). These timestamps enable CounterPoint to choose the server most likely to be operational; CounterPoint moves those servers that failed most recently to the end of the list. CounterPoint attempts any/all CPGateway servers, then any/all dial-up servers.

ConnectErrorExpiration
The default is 14400 seconds (4 hours). This setting is used to order server names that have had failed connections.

Adjusting TCP/IP settings

You may be able to optimize your TCP/IP settings. If you believe that your TCP/IP settings require optimization, visit www.dslreports.com/tweaks for information on testing performance and tools that assist you in modifying configurations.

There are also TCP/IP settings that you can adjust using the Windows Registry, but these are relatively small amounts and will not significantly affect your timing.

Keeping the Internet alive on a dial-up connection

You can use any method to connect to the Internet.

You can use a dial-up ISP connection for your primary Internet connection. One method to ensure continuous dial-up connectivity is described below:

1. Set up your dial-up networking properties to Autoconnect so that no manual intervention is required.
2. Create a shortcut to launch the dial-up system.
3. Copy the shortcut to the same directory from which the batch file runs.

Run a script along the lines of the sample below to start the dial-up process if the Internet connection drops. This sample script tests connectivity every 60 seconds, and re-establishes the connection if it is not connected. For this script, the shortcut should be named DIALUP and should be located in the same directory from which the batch file runs.

```
:BEGIN
SLEEP 60
PING PRIMARY.CPGATEWAY.COM
IF ERRORLEVEL 0 GOTO BEGIN
PING WWW.YAHOO.COM
IF ERRORLEVEL 1 GOTO NOCONN

:NOCONN
START /W DIALUP.LNK
SLEEP 60
GOTO BEGIN
```

Allowing access to CPGateway but not the Internet

There are a number of different ways to configure your system so that users can access CPGateway without unrestricted access to the Internet, including:

- Using a firewall or router to restrict a workstation to a single port
- Using a workstation firewall for outgoing traffic only
- Restricting specific IP addresses

Using a firewall or router to restrict a workstation to a single port

If your firewall or router can restrict particular workstations to particular ports, you can program the device so that a workstation can pass CPGateway transactions through the appropriate port (50000 for First Data North/PNC, 50001 for TSYS, 50003 for RBS Lynk, 50005 for Paymentech, and 50004 for American Express direct) but the workstation's browser will not be able to surf the web (port 80). Many less expensive routers do not have the ability to restrict by port.

Using a workstation firewall for outgoing traffic only

You can install a personal firewall on each workstation and configure the workstation so that it only allows outgoing traffic to primary.cpgateway.com and secondary.cpgateway.com, or only to the ports listed above.

There are a number of personal firewalls available as free downloads, including ZoneAlarm (www.zonelabs.com) and SyGate Personal Firewall (www.sygate.com).

Restricting specific IP addresses

While you can restrict access by specific IP address, this approach is not recommended because the IP addresses for primary.cpgateway.com and/or secondary.cpgateway.com could change in the future (although this is very unlikely). If these addresses change, you would not be able to access CPGateway until you reconfigured your system.

Listed below are two approaches to restricting IP addresses:

Setting up a DNS server on your LAN
To set up a DNS server on your LAN (Local Area Network):

1. Ping primary.cpgateway.com and secondary.cpgateway.com to determine the IP address of the workstation.
2. Set up a DNS server on your LAN that contains IP addresses for primary.cpgateway.com and secondary.cpgateway.com only.
3. Ensure that each workstation is configured to use the LAN's DNS server only.

Modifying the workstation host files
To modify the workstation host files:

1. Ping primary.cpgateway.com and secondary.cpgateway.com to determine the IP address of the workstation.
2. Check each workstation's TCP/IP settings and ensure that no DNS servers are defined.
3. Modify the host file so that it only contains entries for primary.cpgateway.com and secondary.cpgateway.com.

FAQ (Frequently Asked Questions)

Do I need the Credit Cards Option to process credit cards in CounterPoint?

No. Included in CounterPoint is credit card processing under the CounterPoint Merchant Program (CMP) with PNC Merchant Services (using the First Data North platform) or RBS Lynk. The Credit Cards Option is required only to work with other processors.

To sign up for CMP, the merchant or the dealer simply calls the phone number published by Radiant Systems, and the merchant is able to sign up. The CMP processor will issue a Terminal-ID that is compatible with CounterPoint and does not require the purchase of the Credit Cards Option.

Under the CMP, the merchant is entitled to a contracted rate for credit card processing. Most merchants will find that the contracted rate is very competitive.

What other processors can I use with CounterPoint software?

CounterPoint supports the following processors:

CMP	CMP is the CounterPoint Merchant Program
First Data North	Also called CES, Cardnet, or FDMS North
Radiant Payment Services	
RBS Lynk	
TSYS	Formerly Vital and VisaNet
Paymentech	Formerly Gensar and Transnet
First Data South	Also called NaBANCO or FDMS South

Can I authorize and settle directly with American Express?

If you are using CPGateway, you can configure CounterPoint to authorize AmEx transactions directly through American Express. With this configuration, AmEx transactions are still settled through your processor.

If you are not using CPGateway, AmEx transactions are authorized and settled through the processor, not directly with American Express.

Does CounterPoint support leased lines?

No. Credit card processing software in CounterPoint only supports dial-up lines and the CPGateway Internet service.

Is a separate copy of Credit Cards Option required for each store in a Multi-Site configuration?

A separate Credit Card Option must be purchased for each CounterPoint system.

Does CounterPoint handle debit cards?

Debit cards are fully supported for all CounterPoint merchants. Refer to Debit cards on page 12 for additional information about this feature.

The processor is using a 300-baud phone line. Isn't that slow? I don't want my customers waiting in line for their transaction to be authorized.

There is very little data being transmitted during credit card processing. Even at 300 baud, the entire data transmission takes only a few seconds. The majority of the time is spent dialing and connecting. Actual data transmission is only a fraction of the total transaction time.

I want my customer to sign the receipt when it is printed. Does CounterPoint support this feature?

Yes, when using Credit Card processing, CounterPoint pre-defined forms print a sales draft receipt that includes an area for the customer's signature.

Does CounterPoint support card readers that read track 1 and track 2 data?

CounterPoint can read data that comes from track 1 or track 2. The software cannot read data that comes from both tracks simultaneously.

This does not mean that you cannot use a reader capable of reading both tracks at the same time. However, you must configure the reader to read either track 1 or track 2. Consult your card reader manual for information on configuring the reader.

If your card reader is programmed to read track 1, CounterPoint can capture the customer name from the card. The customer name from the card can be printed on Point of Sale forms by selecting the appropriate print field (under the Pay#: group.) If you are processing debit cards, you must use track 2.

Is CounterPoint compatible with April 1996 CPS standards introduced by Visa?

CounterPoint credit card processing follows the standards for general **Retail**, **MOTO**, and **Ecommerce** industry types. There are other classes of processing for travel, dining, entertainment, and so forth. CounterPoint does not and has not ever met the standards for these other forms of processing. For example, when you charge at a restaurant, the authorization can allow an overage for a tip, or at a hotel, you can hold a card open for days until the guest checks out. CounterPoint's general retail capabilities do not support these options.

When the merchant sets up processing with the processor, a certain class of processing is selected based on the type of business. A retailer is typically set up for the general **Retail** industry type.

Does CounterPoint support the Multi-Transaction Option?

The Multi-Transaction Option or Retain Connection Option provides the ability to authorize multiple credit card transactions without establishing a separate connection for each. The amount of time the line will remain open is dependent on the processor. Some users may need to get different Terminal-IDs to enable this capability or possibly notify their processor that they want this capability. Some processors, such as First Data North, offer the multi-transaction option as an additional service. Some processors offer it as part of their standard service. Some processors don't offer the service at all.

NOTES: The retain connection option is available in CounterPoint by setting RCY in SYNEDC.CFG. If this option is enabled, CounterPoint does not hang up at the completion of the call, which allows the next transaction to use the open line before the processor terminates the call.

- In our testing with First Data North, the line for phone number 800/545-3334 was held open for 30 seconds ONLY. The line for phone number 800/950-1292 was held open up to 60 seconds.
- The maximum time the connection will be retained with TSYS is 12-15 seconds.
- Under Unix, the multi-transaction option only works for Digiboard's intelligent port products. CounterPoint testing was performed on one of the PC/Xe series (where X is 2, 4, 8, or 16 depending on the number of ports it supports). The multi-transaction option for Unix should also work with other Digiboard intelligent products, but not the non-intelligent products such as the ClassicBoard. It should also work with other vendors' intelligent products. If multiple registers are sharing the same modem, all registers can benefit from this configuration.
- Under Windows, you can set up each register with a separate modem attached to a standard com port (1 – 4), and benefit from the retain connection option on a single register by reducing transaction times on subsequent authorization requests.
- Under Windows, multiple registers using separate modems can share the same phone line to save on telephone costs. But you will not achieve any speed improvements, and each register will have to \wait for a free line, so you can slow things down by putting too many workstations on one line.
- Modem Server Option is available which allows multiple registers to access up to 4 modems on one workstation that acts as the Modem Server.

Does CounterPoint support address verification services (AVS/AAV)?

Address verification (AVS/AAV) support is provided for all CounterPoint merchants. Refer to Address verification and CVV2/CVC2/CID on page 9 for more information about this feature.

Does CounterPoint support preferred rates for Purchase and Corporate (commercial) cards?

CounterPoint provides support for Level II Purchase cards for merchants who process under the CounterPoint Merchant Program, and for other merchants who process with First Data North, TSYS, or Paymentech. Refer to Purchase cards on page 10 for more information about this feature.

Troubleshooting

Setup problems

Draft capture routines not available

Problem
I receive the message Draft capture routines not available when I try to access credit card functions.

Solution
You must set an environment variable in order to use credit card software. See Environment Variable Setup for information on how to set this environment variable.

In addition, you must set up the appropriate configuration file for your processor, as described in Step 10 – Define SYNEDC.CFG on page 30.

If you are not processing under the CounterPoint Merchant Program (CMP), you must also have purchased and registered the Credit Cards Option under System / Registration.

Credit Cards Option not installed or Terminal-ID is invalid

Problem
When I try to enter my Terminal-ID for the CounterPoint Merchant Program (CMP) in Setup / Point of Sale / Stores / Draft capture, I receive one of the messages below. My PNC Merchant Services representative tells me that I have a valid Terminal-ID.

In Setup / Point of Sale / Stores / Draft Capture:

> Credit Cards Option is not installed. Settlement Terminal-ID is invalid.
>
> *OR*
>
> Credit Cards Option is not installed. One or more Terminal-IDs is invalid.

In Point of Sale / Draft Capture / Authorize or Point of Sale / Draft Capture / Settle:

> Credit Cards Option not installed – Terminal-ID not valid

Solutions

- Download and install the current CounterPoint Service Pack, which you can obtain from our website at http://www.counterpointpos.com/support/software_cpv7.htm. Instructions for installing the Service Pack are included on the website.

  NOTE: You must be a registered CSS subscriber to access the Support area of the CounterPoint website and download Service Packs.

- If the merchant is processing with First Data North and does not wish to process under the CMP (i.e., through PNC Merchant Services), as described in CounterPoint Merchant Program on page 8, the merchant must purchase and register the Credit Cards Option.

Credit card number and expiration date display

Problem
When I swipe a credit card at the card number prompt in ticket entry, the card number and expiration date display on the same line.

Solution
The card number prompt is not the correct place to swipe the card. If you are properly set up for credit card processing, you should see a message at the bottom of the screen Swipe the card now or press F2 for manual entry. If you do not see this message, you do not have a card reader defined for this register in Setup / Point of Sale / Registers.

Press F2 to use the card reader

Problem
At the card number prompt, I have to press F2 in order to use the card reader.

Solution
If you see the message F2=card reader at the bottom of the screen, you have specified to use manual card entry for this pay code in Setup / Point of Sale / Stores / Draft Capture. Specify to use a card reader instead.

Invalid card number message

Problem
When I swipe the card, I see a character, such as %, in front of the card number. This causes the system to return an Invalid Card Number message.

Solution
If you are receiving a character (other than a B' in front of the card number), you need to enter a preamble that tells the card reader to ignore the character. Select Setup / Point of Sale / Devices, and select the card reader that is attached to the Register. At preamble, enter the hex code of the character that displays in front of the credit card number.

Invalid card swipe data

Problem
The message Above transaction may contain invalid card swipe data is printed on the Draft Capture Pre-settlement List.

Solution
This message indicates the card swipe data for this transaction is longer than the ISO defined standard allows. If your card reader is programmed to read track 1, the card swipe data field can contain no more than 76 characters. If your card reader is programmed to read track 2, the card swipe data field can contain no more than 37 characters. If you receive the message Above transaction may contain invalid card swipe data on your Pre-settlement List, this could indicate a problem with the card reader, the SYNCOM environment variable, or the device setup in CounterPoint. Refer to the programming guide for the card reader, and see Environment Variable Setup and Device Codes for additional information.

Authorization problems

In general, error messages displayed to the screen after connecting to the processor are message that are issued by the processor. If the resolution is not listed in this document, it is most likely that the problem will be resolved by directing your question to the processor. Radiant will most likely not have any information regarding the specific messages that the processor might issue.

Normally, a merchant is provided a helpdesk number where there are people who should be able to explain the messages. If you have spoken with the helpdesk and were not able to resolve the issue, CounterPoint Support might be able to provide you a phone number you can use to contact the processor.

Captured XXXXX error

Problem
I receive the message Captured XXXXX from the processor when trying to authorize a transaction.

Solution
You are calling into a host based system. CounterPoint requires a terminal based system. Contact your bank or financial institution. CounterPoint Credit Card software only works with terminal based systems.

“Your Name Goes Here” and “Your City” prints on receipts

Problem
On the customer’s receipt, it says the transaction took place at YOUR NAME GOES HERE and YOUR CITY instead of the end user’s place of business.

Solution
Edit the SYNEDC.CFG file to replace the name, city, state, zip and time zone with the appropriate settings.

Settlement problems

In general, error messages shown on the Settlement Journal preceded by PROCESSOR are text messages transmitted by the processor and reported on the journal. If the resolution is not listed in this document, it is most likely that the problem will be resolved by directing your question to the processor. Radiant will most likely not have any information regarding the specific messages that the processor might issue.

Normally, a merchant is provided a helpdesk number where there are people who should be able to explain the messages. If you have spoken with the helpdesk and were not able to resolve the issue, Radiant Support might be able to provide you a phone number you can use to contact the processor.

I-error messages

Problem
I received the message I-error when attempting to settle credit card transactions.

Solution
You have set up draft capture (using Setup / Point of Sale / Draft capture) such that during the settlement process it is dialing the authorization phone number. It must be set up to dial the correct phone number for settlement.

Processor is not receiving merchant information

Problem
The processor is not receiving the merchant's name, city, zip code, or merchant ID.

Solution
WINxxx.CFG has not been copied to SYNEDC.CFG and/or edited with the appropriate merchant information.

Deleting transactions from the Pre-Settlement List

Problem
On the Pre-Settlement list, there is a transaction that I do not want to settle. How can I delete it?

Solution
If you do not wish to include a transaction in the EDC file for settlement, you must select Point of Sale / Draft Capture / Enter, call up the record, and change the amount to zero. This voids the transaction.

Invalid account error

Problem

When settling, I encounter the error, Invalid account error, batch 1 not processed, error encountered invalid account.

Solution

The settlement date cannot exceed the expiration date of the credit card. For example, if a transaction takes place on the 29th of the month, the credit card used has an expiration date of the 30th, and you do not settle until the 31st, you may receive this message. The transaction is no longer valid because the card has expired.

No transactions are being written

Problem

No transactions are being written to the EDC transaction file for a particular pay code.

This problem indicates one of the following conditions:

- The Terminal-ID for the pay code is set to Simulate.
- The pay code is configured to Authorize only, not to Authorize and settle.
- You are running CounterPoint in Demo mode.

Solutions

- If the Terminal-ID for the pay code is set to Simulate, no transactions are written to the EDC transaction file. Make sure the Terminal-ID for each pay code is set to the appropriate value for your processor in Setup / Point of Sale / Stores / Draft Capture.
- If the pay code is configured to Authorize only, no transactions are written to the EDC transaction file. Make sure that the Set field in Setup / Point of Sale / Stores / Draft Capture is set to Authorize and settle (S) for the pay code.
- If you are running CounterPoint in Demo mode, you must specify a valid Temporary key or Permanent key in System / Registration to allow transactions to be written to the EDC transaction file.

Noise on line errors

Problem

I encounter the Noise on line message when trying to settle transactions.

Solutions

- Invalid Terminal-ID for settlement. Set your Terminal-ID according to the Terminal-ID section of this document for your processor.
- Invalid SYNEDC.CFG for this processor. Define the appropriate SYNEDC.CFG settings for your processor, as outlined in Step 10 – Define SYNEDC.CFG on page 30.
- Try a different phone number.

Surcharges on bank statements

Problem
Surcharges are appearing on my statement from the bank for credit card processing.

Solutions

- All processors charge a surcharge for credit card transactions that are entered manually (not swiped). In addition, some banks may charge an additional fee on top of the processor surcharge for credit card transactions that are entered manually.

  So if you are using CES and CES charges 1% for manually entered credit card transactions, your bank may charge an additional 1% for manually entered credit card transactions. If the manually entered transactions add up to $1000, you will be charged $20 in surcharges.

  The solution is to use a serial, keyboard or VeriFone card reader whenever possible to avoid surcharges.

- All processors charge a surcharge for transactions if the data is not sent in the correct format, or if parts of the data are invalid. If this is the reason for the surcharge, the next time a batch is settled, ask the processor to capture the data and fax you and/or the CounterPoint Support Department a print screen of the data explaining the problem.

  The CounterPoint Support Department can provide phone numbers for each processor's technical support department, if necessary.

Processor-specific problems

First Data North problems

Problem
When authorizing American Express transactions, I encounter the message Processor:re-enter – American Express or Processor:reenter....

Solution
American Express has a minimum charge amount of $1.00.

Problem
I encounter the error Referral INV TR2 or INV SETTL TR 001 when settling.

Solutions
- Make sure the card reader is configured to read track 1 or track 2, but not both. Track 3 cannot be used.

  If you are using a keyboard transparent reader, you can determine which track is being read by swiping the card at the operating system prompt. The card number should appear only once in the data stream. If it appears more than once, the card reader is reading more than one track and should be re-configured.
- The credit card datastream contains a preamble and postamble. Configure CounterPoint to remove the extra characters from the datastream by using Setup / Point of Sale / Device codes to define the preamble/postamble hexadecimal characters for the card reader device.

  For example, if you are using a Cherry keyboard, and your card reader is programmed to read track 1, 25 is the preamble to be defined (to be removed).

  If you are using some other keyboard transparent card reader that is programmed to read track 2, 3B is the preamble to be defined (removed) and 3F is the postamble.

Problem
When I attempt to authorize 2-3 different credit cards on one ticket, or when I attempt to authorize an order deposit (or a layaway deposit) and a sale on one ticket, it takes 2 – 6 minutes to receive the authorization code.

Solution
Add the appropriate prefix to the Terminal-ID in Setup / Point of Sale / Stores / Draft capture:

E. Retail merchant
M. Mail Order/Telephone Order or Ecommerce merchant
T. Multi-transaction Retail merchant
W. Multi-transaction Mail Order/Telephone Order or Ecommerce merchant

If you are using multi-tran (more than one transaction per phone call), the Terminal-ID should include the T. or W. prefix. You must also add the following setting to your SYNEDC.CFG file:

/RCY/

Modem configuration and troubleshooting

We are often asked why customers have problems authorizing/settling credit card transactions in CounterPoint, particularly when using newer modems.

There is no easy answer to this question. Successful credit card processing depends on both hardware and telephone lines in addition to software.

When modems were first introduced, a baud rate of 150 was considered fast. Today, a baud rate less than 9600 is not acceptable for anything other than credit card authorization. (The amount of data transmitted during credit card authorization is so small that the baud rate doesn't make a difference.)

Telephone lines are designed to successfully handle modem communications up to 9600 baud. However, most of the modems on the market today handle communications with baud rates up to 56K. How can these modems transmit over telephone lines that are only reliable up to 9600 baud?

The answer is that today's modems are "smart" modems. Smart modems use data compression and buffering to make the data smaller than it really is, transmit it over the phone line at 9600 baud, and then decompress it on the other end. Using this technology, the actual throughput of data can be greater than 9600 baud, even though the transmission speed is only 9600 baud.

The majority of the problems encountered when using Credit Card Option are caused by this "smart" technology. Today's modems have high speeds, fax capability, voice-mail and e-mail capability, answering machine capability, error correction, data buffering, etc. If the modem is not set up properly, communications may fail. If a modem with a specific capability is trying to connect to a modem without those capabilities, or is not set up in the same way, errors can occur.

Many different brands of modems are available, and it isn't possible for Radiant to test every possible combination of equipment. When we do test a specific modem, we will continue to add to this document in order to provide the most complete list possible of modems that we know will work properly.

COM Port IRQS

Devices attached to workstations running CounterPoint should be defined for standard COM ports and IRQs. If your workstation has four COM ports available, you can define them in CMOS, Windows, and CounterPoint using the following configuration without a conflict:

COM 1	IRQ 4	Base Address 3f8
COM 2	IRQ 3	Base Address 2f8
COM 3	IRQ 4	Base Address 3e8
COM 4	IRQ 3	Base Address 2e8

Some Plug and Play modems will be installed under Windows using a non-standard IRQ (e.g., IRQ 7). These modems will not work with CounterPoint.

Winmodems

Winmodems are internal, software-based modems that use fewer chips than traditional modems.

Traditional modems contain a physical controller that specifies the protocols for hardware error correction, hardware data compression, and basic modulation (e.g., V.34, X2, K56flex, or v.90). The controller is also what interprets AT commands. Winmodems implement the controller function with software instead of hardware.

Radiant recommends that you do **NOT** attempt to use a Winmodem with CounterPoint, as many problems have been reported with Winmodems.

Setting modem INIT strings

You can use BLAST's terminal mode in Data Pump to set initialization strings:

1. From the Start / Programs menu, select Data Pump.
2. Open a phonebook listing.
3. Type ATZ to verify that you are communicating with the modem.
4. Type the initialization string you want to send to the modem.
5. If appropriate, write the new settings to the modem (normally AT&W).
6. Close the Data Pump session.

You can also echo commands directly to the modem from the operating system:

DOS: echo ATZ >com1

Unix: echo "ATZ>/dev/tty1a"

Modem brands and initialization strings

This section details initialization strings for modems that have been tested by Radiant or that have been used successfully by our dealers in the field.

Accura 14.4 External

The best init string for EDC appears to be: ATX4 S9=1 S11=55 S37=0 EQVBN&Q

Accura 28.8 or 33.6

Dealer reported init string for EDC: AT&C1&D2&K0&M0&Q0&N3&U3

NOTE: Dealer reports that the above init string is not reliable with the 56K models, especially one with v.90 compliance.

Amquest 14.4

The best init string for EDC appears to be: ATE0F4Q0V0X4&C1&D2&M0&Q6

(F4 sets the connect speed to 1200 bps. F5 sets the connect speed to 2400bps.)

Aspen 28.8
Use BLAST's terminal mode to write the following init string to the modem's memory (using AT&W): ATE0Q0V0X4&C1&D2&K0&Q6\N0%C0

In SYNEDC.CFG, use ****MIAT&Y0**** to call the init string from the modem's memory.

Best Data 33.6
Dealer reported init string for EDC: AT&P2&C1&Q0S37=3N0

The above init string sets the baud rate to 300 bps, so if you plan to use Multi-Site, you will need to issue ATS37=0 from BLAST (or whatever communications package you are using).

Boca 2400 Internal
Set the following init string: AT\N0S0=0Q0V0X4&C1&D2

(For a Boca Modem, the parameter &C1 turns off force carrier high.)

Use BLAST's terminal mode to write this init string to the modem's memory: AT&W

In SYNEDC.CFG, use ****MIAT&Y0**** to call the init string from the modem's memory.

Boca 2400 External
No initialization string needed, according to dealer reports.

Boca Modem 14.4Kbps V.32bis Model M1440E
The best init string for EDC appears to be: ATL2&Q6S37=5

Boca Modem 33,600 MV.34
Set the following init string: AT&C1&D3&K0&Q6\N0S37=5

(For a Boca Modem, the parameter &C1 turns off force carrier high.)

Use BLAST's terminal mode to write this init string to the modem's memory: AT&W

In SYNEDC.CFG, use \MIAT&Y0\ to call the init string from the modem's memory.

Boca Modem V.34 28.8
The best init string for EDC appears to be: AT&Q6S95=0

Q6 turns off error correcting stuff but leaves handshaking on (Q0 does the same thing without handshaking, but don't use it because the modems won't connect without handshaking) and S95=0 causes it to return the correct connect result codes.

Another suggested init string for the Boca V.34 modem is: ATV0&C1&D2&Q6N0S37=5-K0

Cirrus Logic Internal
The best init string for EDC appears to be: AT\Q0\N0%C0H0

This initialization string should be saved to the modem's memory via Multi-Poll or some other communications package because the "\" will cause the initialization string to be ignored in SYNEDC.CFG. "\" is used in SYNEDC.CFG to separate parameters sent to the processor during authorization and/or settlement.

When this Plug and Play modem is installed, it uses IRQ 11. CounterPoint can't use interrupt 11. The jumpers on this modem must be changed to use a standard interrupt, such as IRQ 3 or 4.

Multitech 33.6 Kps Model MT2834ZDX
Dealer reported init string for EDC: ATE0Q1&E0&E3&E12&E14&C4$MB1200$SB9600&W.

Multitech 33.6 Kps Model MT3334ZDX
The best init string for EDC appears to be: AT&D3&K0&Q6&S1%C0$MB1200.

\SIY\ should be used in SYNEDC.CFG.

Practical Peripherals
The best init string for EDC appears to be: AT&C1&M0&N0.

For a Practical Peripherals Modem, the parameter to turn off force carrier high is: &C1

Practical Peripherals Model PC 144MT (19,200bps)
Dealer reported init string for EDC: AT&K0&Q0&M0S6=5.

The default initialization string for the Practical Peripherals Model PC 144MT includes E0L2M1Q1V0X4&C1&D2&K3%C1. You can tell what the default initialization string is by typing AT&V in your communications package. If the default initialization string contains different parameters from those listed here, you may need to insert additional parameters in SYNEDC.CFG.

Practical Peripherals Model PM288MT II V.34
Set the following init string in Terminal Mode of Multi-Poll: AT&K0\N0%C0H0N0.

Use BLAST's terminal mode to write this init string to the modem's memory: AT&W.

In SYNEDC.CFG, use \MIAT&Y0\ to call the init string from the modem's memory.

US Robotics Sportster 14.4, 28.8, 33.6 Model C460-C, 33.6 Model 839 (Non-V.90 modems)
The best init string for EDC appears to be: AT&D2&K0&M0

- Adding E0 to the init string above turns Echo off.
- Adding M2 to the init string above means the speaker is always on.
- Adding &N2 to the init string above sets the connect speed to 1200 bps.
- &N12 sets the connect speed to 2400 bps.

The initialization string in SYNEDC.CFG overrides the default initialization string. The default initialization string for the US Robotics Sportster modems includes ATE0M1Q0V0X4&C1&D0&K1&M4&N0. You can tell what the default initialization string is by typing ATI4 in your communications package. If the default initialization string contains different parameters from those listed here, you may need to insert additional parameters in SYNEDC.CFG.

For some USR modems, problems with getting the modems to dial out have been solved by adding a hex ATZ (41545A) in the Disable field of the device code setup, which will clear the hardcoded init string CounterPoint sends to the modem (as well as any parameters set by other communication programs).

US Robotics Sportster 56k V.90 Modems
The best init string for EDC appears to be: AT&K0&C1&D2&M0&N2

Zoom 14.4 Internal model #110
Dealer reported init string for EDC: AT&C1&D2L3E0F1.

The dealer who uses this modem brand suggested setting the init string from AUTOEXEC.BAT using the following command: ECHO AT&C1&D2L3E0F1>COMx:; where x = COM port destination. Setting the init string in AUTOEXEC.BAT works more consistently than setting the init string in SYNEDC.CFG for this dealer.

Zoom 33.6 External
The best init string for EDC appears to be: AT&D2&Q0%C0&C1

Zoom 56K External
The best init string for EDC appears to be: ATL3&K0&M0&Q6\N0\V1+MS=69+H0%C0

Determining your initialization string

If your modem does not appear in the previous list, the following procedure will assist you in determining the proper initialization string to be entered in SYNEDC.CFG for use with CounterPoint Credit Cards Option.

In general, newer modems (anything above a 14.4 bps) require more parameters in the initialization string than older modems. Refer to the AT Commands section of your modem user manual to determine the correct parameters for your modem.

Only parameters listed below that are not the default setting for your modem should be entered in SYNEDC.CFG. If your modem manual does not tell you which settings are the defaults, you can view the active and stored profiles in BLAST's Terminal Mode using AT&V for a Practical Peripherals modem or ATI4 for a US Robotics Sportster modem.

- Use Bell 212A connection (at 1200 bps)-for a Zoom modem this may be B1 or +MS=69.
- Make sure Command characters are echoed-for a Zoom modem this is E0.
- Turn off speed negotiation-for a Practical Peripherals modem this is N0.
- Make sure responses to computer are Enabled (DTE) -for a Zoom modem this is Q0.
- Make sure responses are Verbose-for a Zoom modem this is V0.
- Make sure all responses are sent-for a Zoom modem this is X4.
- If you receive a modem command error, you may need to limit the responses. In this case, you should try X3.
- Make sure DCD indicates presence of data carrier-for a Zoom modem this is &C1.
- If this parameter is NOT a default your modem, in some cases it is best to write this parameter to the modem's memory in BLAST's terminal mode.
- Make sure DTR drop causes modem to hang up. Auto-answer is inhibited. For a Zoom modem this is &D2. For some modems it may be necessary to make sure DTR drop causes modem to do a soft reset. For a Zoom modem this is &D3.
- Disable flow control-for a Zoom modem this is &K0.
- Make sure direct asynchronous mode is selected (no error correction or speed buffering) -for a Zoom modem this is &Q0. For some modems it may be necessary to select asynchronous mode with speed buffering (no error correction) – for a Zoom modem this is &Q6.

- Let Data Set Ready (DSR) follow CD. If the default on the modem is to force DSR high (on), turn this off. For a Multi-Tech modem, this is &S1.
- Make sure data compression is disabled-for a Zoom modem this is %C0. For a Practical Peripherals modem, this is %C0 H0.
- If you are using speed buffering (asynchronous operation) in normal mode (&Q6 for a Zoom and Boca modem) you may also need to select normal (disabled) error correction operating mode – for a Boca modem this is \N0.
- Parameters with a "\" cannot be entered in SYNEDC.CFG because the "\" is used as a separator for draft capture information. Therefore, this parameter should be written to the modem's memory using BLAST's terminal mode.
- Some modems allow you to define the connection speed. If you are using1200 bps in Setup / Point of Sale / Stores / Draft Capture, you can set the S register to this speed – for a Boca modem this is S37=5. To set the connection speed to 2400 bps, use S37=6.
- For a Multi-Tech modem this is $MB1200 (1200 bps) or $MB2400 (2400 bps).
- If you receive a modem command error, you may also need to set the connect code to DCE speed instead of DTE speed-for a Boca modem this is S95=0

Troubleshooting

Problem
When trying to connect with the processor, I quickly get the response (connecting, terminating), and then it re-dials the number again with the same result.

Solution
Run the modem test in Setup / Point of Sale / Registers to ensure that the software is communicating with the modem.

The Terminal-ID is not valid for that processor.

Ensure that verbal result codes are being used. Typically, this modem command is V1. Add the command to the modem initialization string defined in the SYNEDC.CFG file for your processor. Refer to your modem manual for the correct command for your modem.

The phone number being dialed for authorization is not an authorization phone number for that processor.

Problem
If I try to authorize from Ticket Entry, the modem never tries to connect. I see transmitting, receiving.... but I never see an attempt to connect. If I perform a modem test in Register setup and then try to authorize, I am successful. What is wrong?

Solution
If force carrier high is a default setting on your modem, make sure the init string in your SYNEDC.CFG file contains the command to turn it OFF. Refer to your modem manual for information on changing this setting.

If a modem is set to force carrier high when CounterPoint attempts to perform an authorization, CounterPoint assumes that the modem is already connected to the phone line and a remote modem. Therefore, it never attempts the connect sequence.

The self-test always performs the complete test sequence without checking whether the modem is already connected, so it will leave the modem in the proper state when it is complete.

On a US Robotics modem, the command to turn off force carrier high is &D3. On a Boca modem, it is &C1. Enter the appropriate modem command in the modem init string contained in the SYNEDC.CFG file for your processor.

You can use your communications package to program your modem, as shown in the example below:

Run the package in Terminal mode

Type the following command sequences to turn off force carrier high for a Boca modem, and will write that information to the modem's RAM (this approach should work for other, similar modems):

ATE0Q0V0S0=0S2=43&S0&C1 <enter> (The screen will display modem response of 0)

ATM1X4S9=1S10=3S11=55 <enter> AT&W <enter>

These are the same commands that are sent during a CounterPoint Modem Device Test to initialize the modem.

Edit the SYNEDC.CFG file in the SYN directory and on the first line insert: \MIAT&Y0. This command, when sent to most Hayes-compatible modems, should retrieve the parameters saved in the modem's RAM. The codes may be different for your particular modem.

If you have specific sequences that you have used that work, please provide this information to the CounterPoint Support department so that we can include it in the next release of this document.

Problem
I receive the message Communications error when performing a device test.

Solution
Turn off all of the modem's "smarts," such as error correction, data compression, and fax and voice mail capabilities. The modem may have a parameter called data rate or data link (DCE/DCE) that is not set correctly. On some modems, the modem command to turn off these features is AT&N0 or AT&Q0. Enter the appropriate modem command(s) in the modem init string contained in the SYNEDC.CFG file for this processor.

Problem
I receive the message Communications time out when performing a device test or when attempting a credit card authorization.

Solution
If the modem will not dial, remove the modem using the Modems icon in the Control Panel. The fact that the modem is defined in Windows makes it unavailable for CounterPoint. This problem is usually associated only with internal modems.

If the modem is auto-detected the next time Windows starts, go to System in the Control Panel and choose the Device Manager tab. Highlight the modem, then click Properties and check Disable in this hardware profile.

Removing the modem from the hardware profile will make it unavailable to Windows for functions such as dial-up networking.

Windows Dial-Up Networking does not release the modem after the connection is terminated. If you initiate a dial-up networking connection, you will not be able to use the modem for CounterPoint credit card processing until you restart Windows. The only other solutions are to set up two modems on the workstation (one for CounterPoint and one for dial-up networking), or use a different machine for credit card processing.

Problem
The modem dials, connects, retries, connects, and finally aborts.

Solution
Make sure that the processor has the merchant set up on a terminal system, not a host system.

Turn off all of the modem's extra features such as error correction, data compression, and fax/voice mail capabilities. The modem may have a parameter called data rate or data link (DCE/DCE) that is not set correctly. On some modems, the modem command to turn off these features is AT&N0 or AT&Q0. Enter the appropriate modem command(s) in the modem init string contained in the SYNEDC.CFG file for this processor.

We recommend **NOT** using &F as part of the init string. CounterPoint sends 2 sets of hard coded init strings to the modem prior to sending the init strings from SYNEDC.CFG. &F will reset the two hard coded init strings. You may see more problems with this under Unix than under Windows.

Problem
I receive the message No carrier when performing a device test.

Solution
The modem is not set up properly, or the system does not recognize the modem.

We encountered a Cardinal internal modem that was not recognized by the credit card software. In this case, the solution was to use another modem.

Problem
Authorizations are taking 2 to 4 minutes (when using PNC as a processor, authorizations should take 15 seconds—in fact, PNC disconnects after 30 seconds).

Solution
Add the AT command for a Bell 212A to the initialization string in SYNEDC.CFG for the modems in question. For example, for a Zoom V.34 28,800 and 56k modem, the AT command would be +MS=69.

Problem
I receive the error message No response from modem.

Solution
This error has been reported with US Robotics, Boca, and Practical Peripherals modems.

US Robotics modems have a known problem where they will sometimes enter a state where they will not accept any commands, regardless of whether or not they are connected. US Robotics reports that you can correct the problem by:

On older modems, install a newer chip set.

On modems with newer chip sets that still experience the problem, download a patch from the US Robotics Web site.

You must contact US Robotics with the model & serial number of your modem to implement either of these solutions.

This problem appears to be a timing issue with some modems. CounterPoint may be sending init strings to the modem too fast and the modem cannot recognize the init strings properly.

A flag can be added to SYNEDC.CFG called SI for Slow Init. Set it as follows: \SIY\.