

## Fraud Prevention FAQs

1. How can I prevent fraud?
2. How can I prevent Internet, Mail-Order (MO) and Telephone-Order (TO) fraud?
3. Why should I require CID on my Web site?
4. Why should I require a signature when delivering mail or telephone orders?
5. Why is data security so important and how can I protect my business and customers from hacking attacks?
6. Where can I report suspected merchant fraud?
7. Where can I meet other merchants that may have the same Card Not Present (CNP) fraud concerns that I have?
8. What are some signs of suspicious behavior?
9. What do I do if I suspect a Card is fraudulent in a Card Present situation?
10. What are some tools offered by Discover® Network to help prevent fraud?

### 1. How can I prevent fraud?

There isn't a single simple solution or tool to preventing fraud. It takes an assortment of many tools to prevent fraud. The best protection comes from knowledge and understanding of the latest tools and trends impacting the marketplace. Discover Network offers its merchants numerous tools to assist in the fight against fraud. Reading through the FAQs listed below will help you determine what your business needs to do to reduce your fraud risk. Awareness is the first step towards fighting fraud!

### 2. How can I prevent Internet, Mail-Order (MO) and Telephone-Order (TO) fraud?

Here are some guidelines for preventing Internet and MO/TO fraud:

**Request Cardholders for the following information during the order taking process:**

- Cardholder Name, exactly how their name appears on their Discover Network issued card
- Card Account Number is at least 16 digits
- Card Expiration Date, four-digit number MM/YY
- CID (Card Identification Data), the three-digit number located on the back of the card in the signature panel
- Card billing address along with the ship-to address (when necessary)
- Home, business or other telephone number where the cardholder can be reached

**For each transaction, be sure to:**

- Request and validate the Card Identification Data (CID) (the three-digit code on the back of the card in the signature panel). The CID can be submitted in the electronic authorization request or can be used when calling our authorization center
- Verify the customer's billing address, either electronically or by our automated phone system (Address Verification System - AVS)
- Check your delivery service contract for who is responsible for merchandise not delivered
- Get a signature for each delivery
- Keep all delivery records
- All declines are final. Do not force through any sales for which you have received any declined response to your authorization request
- If the sale is on a credit card, do not refund in cash or by check. Refund sales on the same card account that the purchase was made on

- Include your common DBA and customer service number on the cardholder's transaction statement
- Clearly communicate any and all delivery charges, restocking or other fees
- Clearly explain any return policies and offer documentation of this policy with each sale
- When working on a chargeback, document efforts to satisfy the customer
- Respond to all chargebacks, even the small ones (remember, this is your customer)
- Duplicate charges, or installment plans, unless otherwise stated, require an authorization for each sale

### **3. Why should I require CID on my Web site?**

In addition to the requirements in the Merchant Operating Regulations, Section 5.1.1, CID provides the assurance that the card was in the possession of the cardholder at the time of purchase. It is the best defense against online fraud.

### **4. Why should I require a signature when delivering mail or telephone orders?**

In addition to the requirements in the Merchant Operating Regulations, Section 5.1.5, requiring a signature from the cardholder will give proof that the proper person received the shipment. The signature may be verified in the event of a chargeback situation.

### **5. Why is data security so important and how can I protect my business and customers from hacking attacks?**

In today's world, credit card information is being illegally obtained in many different ways. One of the primary sources for obtaining this information is by hacking vulnerable businesses lacking proper data security. The best way to protect yourself is to develop a solid information security strategy for your business. Some basics include the highest and most technologically advanced Secure Sockets Layer (SSL), Firewalls, cryptography tools and anti-virus software. The rule with data security is that you cannot be too careful. The best way to fight this growing epidemic is to work with a highly regarded company that specializes in data security. Learn more about our Data Security guidelines and our DISC program by visiting [www.DiscoverNetwork.com](http://www.DiscoverNetwork.com).

### **6. Where can I report suspected merchant fraud?**

Please contact our Merchant Fraud Prevention Department at 800-347-3083.

### **7. Where can I meet other merchants that may have the same Card Not Present (CNP) fraud concerns that I have?**

The Merchant Risk Council is one organization of this type.

### **8. What are some signs of suspicious behavior?**

Here are some tips to help you detect possible fraudulent situations:

#### **Customer Behaviors**

- Makes random purchases without paying attention to size, value or price
- Presents you with a credit card taken from a pocket instead of a wallet
- When asked, claims to have left photo identification at home or in the car
- Arrives at or about closing time and tries to hurry you through the sale
- Purchases a large item and refuses delivery
- Displays no interest in the warranty on expensive items
- Is overly slow and deliberate when signing the sales draft, perhaps because the signature is being forged



#### Card Characteristics:

- Card is missing the stylized "D" character
- Seems counterfeited or it seems as though the information (i.e. expiration date, hologram, account number, embossed name etc.) thereon is altered
- The signatures on the card and the sales draft are different
- The validation date has expired
- Security features have been tampered with

#### 9. What do I do if I suspect a card is fraudulent in a Card Present situation?

If you suspect fraud: Call 1-800-347-1111 and ask for a Code 10 authorization if you have any reason to suspect the transaction or are suspicious of the customer.

#### 10. What are some tools offered by Discover® Network to help prevent fraud?

There are many fraud prevention tools offered to Discover Network Merchants. These tools can be ordered by clicking on an item below or by calling 1-800-347-2000, Option 3. Here are a few of the Fraud Prevention tools available:

- **Fraud Awareness Training Guide (#12797)** - A seventeen page fraud awareness training guide covering security and fraud prevention and accepting Discover Network card transactions.
- **Card ID Features - All Cards (#33844)** -A helpful two-sided slick that provides card identification features for the four major credit card types.

#### Other Important Reminders:

- Your approval number does not eliminate the possibility of a fraudulent sale
- You are the first line of defense against fraud
- Discover Network is here to assist you in the fight against fraud!

For more extensive information on fraud prevention, including identifying the Discover Network brand and handling suspicious situations, please refer to your Discover Network Merchant Operating Regulations or [DiscoverNetwork.com](http://DiscoverNetwork.com).