

Protecting Your Business From Fraud Calls

Minnesota Relay is a free public service that connects people who are deaf, deaf/blind, hard of hearing, or speech disabled with standard telephone users – such as your business. This is accomplished via a relay center staffed with specially trained communication assistants (CAs) who act as translators between a person with hearing loss or a speech disability, and a hearing person. Thousands of Minnesotans use Minnesota Relay everyday to make personal and business calls.

Some businesses have not accepted relay calls because they are concerned that they will be defrauded.

However, if a business accepts telephone orders from the general public, then customers with a hearing or speech disability who call through a relay service must be afforded the same convenience. In a Public Notice released on June 18, 2004, the FCC issued a reminder to businesses that “Title III of the Americans with Disabilities Act of 1990 (ADA) does not permit merchants to treat persons with a hearing or speech disability differently than they treat others.” Not only are businesses missing an opportunity to gain a new customer if they refuse to accept a relay call, they are also breaking the law.

Although almost all relay calls are from legitimate users, scam artists are using an internet based form of relay service, called IP Relay, to defraud businesses. IP Relay is accessed using a computer and internet connection instead of a TTY (text-telephone) and telephone line.

Unlike telephone numbers, which can easily be traced to a particular location, computer IP addresses are virtually anonymous. It is this anonymity, coupled with the fact that Internet calls do not incur long distance charges, that makes IP Relay so attractive to scam artists. Posing as a deaf person, these fraudsters cold call businesses all day in search of unsuspecting merchants. Using stolen or manufactured credit card numbers and counterfeit cashier’s checks, the international scam artists attempt to purchase large quantities of auto parts, computer equipment, office supplies, clothing, bibles and more.

It is important for businesses to be aware of “red flags” that may indicate that a phone order is fraudulent, and employ sound fraud prevention practices to ensure that they do not become a victim of this crime.

Red Flags

- Caller wants the order immediately, and asks for overnight or expedited shipping
- Caller places large orders for multiple items
- Caller exhibits a lack of knowledge of the product and/or does not ask questions about the product
- Caller is not concerned about the price
- Caller wants to use multiple credit cards, sometimes with numbers that are close together
- Caller may send follow-up e-mail with poor English grammar or spelling
- Caller sends a check for more than the purchase price and asks you to wire back the difference

How to Protect Your Business

- **Know who you're dealing with.** In any transaction, independently confirm the buyer's name, street address and telephone number.
- **Don't accept a check for more than your selling price, no matter how tempting.** Ask the buyer to write the check for the correct amount. If the buyer refuses to send the correct amount, return the check. Don't send the merchandise.
- **If the buyer insists that you wire back funds, end the transaction immediately.** Legitimate buyers don't pressure you to send money by Western Union or a similar company.

Note: Do not assume that a cashier's check has cleared and is not counterfeit even if your bank says that funds are "available." Your bank may indicate that the check has cleared, but it also must clear the institution that issued the cashier's check. A merchant may believe that the check is good and wire back money as instructed and/or ship the merchandise. Soon after, the merchant may be notified by the bank that the check was fraudulent, and the bank will hold the merchant responsible for the full amount of the check. *If you accept a cashier's check for merchandise and you have any question about the legitimacy of the transaction, you may choose to delay shipment by an additional period of time, such as a week, to be sure the check has truly cleared before you ship the merchandise.*

- **If you accept payment by check, ask for a check drawn on a local bank, or a bank with a local branch.** That way, you can make a personal visit to make sure the check is valid. If that's not possible, call the issuing bank and ask if the check is valid. Get the bank's phone number from directory assistance or an Internet site that you know and trust, not from the person who gave you the check.
- **If you accept payment by credit card, ensure that the credit card is valid.** Also make sure that the person using card is authorized to do so.
- **Resist any pressure to "act now."** If the buyer's offer is good now, it should be good after the check clears the issuing bank.

If You Receive a Fraudulent Call

If your business receives a suspicious call via IP Relay, it is crucial that you document all information about the transaction. Whenever a situation such as this arises, make sure to report the fraud.

The FCC is working with IP Relay providers to prevent the misuse of this important communications service. To file an IP Relay complaint with the FCC, call 1-888-225-5322 (voice) / 1-888-835-5322 (TTY) or go to www.fcc.gov/cgb/complaints. To report fraudulent IP Relay activity, contact the Federal Trade Commission at 877-FTC-HELP or www.ftc.gov.

It is important to recognize fraud in order to prevent it. By doing so, your business can comply with the Americans with Disabilities Act by welcoming calls made by relay users, ensuring that everyone who wants to do business with you is able to do so.