

## **How to avoid credit card fraud**

Accepting credit cards on your Web site provides donors and the public an efficient way to do business with you. But with opportunity comes responsibility. When you process credit card transactions online, you open the door to fraud. Thus, you need to learn how to handle sensitive information with care.

### **Are you at risk?**

If you're using your Web site to solicit donations, you might think that your risk of fraud is pretty low. After all, if no merchandise is exchanged for the money, what can you really lose?

Unfortunately, credit card and identity thieves increasingly make small donations on nonprofit sites to test if a stolen card is valid. It's called "carding." To prevent it from harming your charity, look out for a string of several denied transactions for the same small dollar amount, numerous donations that come in with similar credit card numbers or donations made with important purchase information missing. Watching for questionable donations will save you the time and effort of having to investigate and make refunds later.

Also remember that some donations have a purchase element to them — even if it's not for physical merchandise. Examples include raffle tickets and admission to fundraisers. (See "Don't let this happen to you," below.)

### **Best security practices**

Whether you create and maintain your own online purchase or donation capability or use the services of a third party, you need to understand the basics of secure online transactions and ensure they're being followed on your site. Perhaps the most important when you're transferring sensitive information, such as credit card numbers, is the Secure Socket Layer (SSL) Web protocol. Make sure your hosting company or third-party service uses this basic technology.

Also, Visa USA recommends that you ask for the following information in all "card-not-present" transactions (such as online purchases):

- The complete credit card number,
- The card's expiration date,
- The additional three- or four-digit security code (printed on the signature strip of MasterCard, Visa and Discover cards and on the front of American Express cards), and
- The billing address for the card in addition to the ship-to address.

What's more, every online transaction should go through a credit authorization process. If you've built your own online capabilities, be sure you haven't overlooked this step. Authorizing payments (either manually by calling them in or automatically through your merchant account) is separate from accepting them. If you're working with a third-party provider, ask for details on their authorization process and be sure it applies to all transactions — even the smallest donations.

### **Your responsibility**

When you collect sensitive information such as credit card numbers, you have a responsibility to handle the information safely. The best defense against outside hackers or insiders helping themselves to a donor's credit line is to not store credit card data in the first place.

If personal information does fall into the wrong hands, notify the appropriate authorities according to the laws in your state. This might include the police and your state's attorney general. Work with your legal counsel to act quickly and appropriately and to determine how to notify the affected donors.

### **All the upside, none of the fraud**

Put the right processes and procedures in place. Then, you can offer the advantage of convenient, online transactions without the worry that you'll be taken advantage of.

### **Sidebar: Don't let this happen to you**

A charitable organization was thrilled when a supporter bought 100 raffle tickets at \$100 apiece for a chance to win a BMW. But the thrill cooled quickly when the donor called his credit card company after he didn't win the car and claimed that the charge was an error. He asserted that he had purchased only one ticket. Just like that, \$9,900 disappeared.

The assumption that someone wouldn't try to scam a charity just because it's a charity is unfortunately outdated. The lesson? Verify all credit card transactions — particularly those with a big price tag attached. If this organization had simply confirmed the purchase by sending a follow-up e-mail, it could have avoided becoming a fraud victim.