Avoid these popular scams that can cost merchants BIG!

My shipping service scam

What happens?
The buyer asks you to use their shipping account because they can get a discount, they have a preferred vendor they have worked with for years, or their shipping service is cheaper or more reliable.

In another variation of the scam, the buyer may also ask you to wire the shipping fees to their preferred shipper.

Real reason they want you to use their shipping service
If you use the buyer's shipping account, they can easily contact the shipping company and reroute the order to another address. Then, the buyer can open up a complaint asking for a refund because they didn't receive their order. Now you aren't able to prove that the buyer received their order and you are out your product, the shipping costs, and your money.

Real reason they want you to wire the money to their shipper
They want you to wire the money to a bogus shipping company so they can steal your money. After you have wired the money you will find out that the order was made with a stolen card or bank account and you may be held liable for returning the funds to the legitimate customer whose account was stolen.

How to avoid this scam

1. Only use your shipping account.
2. Never wire money to someone you don't know – you can't get it back easily.
3. If a customer asks you to use their shipping service, review their order for fraud carefully. They may have used a stolen card or bank account to fund the purchase.
4. Ship to the address on the Transaction Details page.

Pre-paid shipping label scam

What happens?

You receive an order from a customer who asks you to use their pre-paid label to cover the shipping charges. They may tell you that they can get their labels at a discounted price.

Real reason they want you to use their shipping label

By providing the label, the customer controls where the package is sent to. They may send the package to another country, a PO Box or some other untraceable location. To be covered under PayPal's Seller Protection policy, you are required to ship to the address on the Transaction Details page. The shipping label may also have been purchased with a stolen credit card.

How to avoid this scam

1. If the customer asks you to use their pre-paid label, review their order for fraud carefully. They may have used a stolen card to make the purchase.
2. Do not accept shipping labels from your customers.
3. Ship to the address on the Transaction Details page.

Package rerouting scam

What happens?

1. A buyer places an order and provides an incorrect or fake shipping address.
2. The shipping company tries to deliver the package but isn't able to.
3. The buyer monitors the online tracking information and notices that the shipper couldn't deliver the package.
4. The buyer contacts your shipping company and asks them to send the package to their correct address. The shipping company delivers the package to the new location.

Real reason they rerouted the package

The buyer rerouted the package so they could file a complaint saying that they never received it. Because the shipment was rerouted, you can't prove the item was delivered to the address on the Transaction Details page. The buyer gets to keep the item and, because the package wasn't delivered to the address on the Transaction Details page, you aren't covered by Seller Protection. Unfortunately, you lost the product, shipping fees, and the money. To make it worse, you might also have to pay your shipper an additional rerouting fee.

How to avoid this scam

1. Contact your shipping company and block buyers from rerouting packages.
2. Validate the buyer's address before shipping.
3. Only ship to the address on the Transaction Details page.

Overpayment scams

What happens?

You receive an order and your customer sends you a PayPal payment or check that is more than the purchase price and then asks you to wire them the difference. They may tell you that they accidentally overpaid you, the extra money is for the shipping costs, they're giving you a bonus for your great service, or the money is for the stress they've caused you. They may even ask you to wire the shipping fees to their shipper.

Real reason they overpaid you

This scammer may have used a stolen credit card, bank account number, or checking account to pay you. Just because a payment has been deposited into your account, doesn't mean the money is yours to keep. If the legitimate account holder reports unauthorized activity, the money can be withdrawn from your account. If that happens, you'll lose the money you wired to the fraudster, the product you shipped, shipping costs, and your payment.

How to avoid this scam

1. Don't wire money to someone you don't know. A legitimate buyer won't overpay you for an order.
2. If a customer overpays you and asks you to wire them the difference, consider canceling the order- it's very likely to be fraudulent.
3. Don't wire money to the bogus shipping company – it's part of their scam to get your money.
4. Follow the Seller Protection policy and ship to the address on the Transaction Details page to protect yourself from unauthorized transactions.

Reshipping packages scam

One of the more popular work-from-home scams is reshipping electronics, clothing, and other items out of the United States. Victims find these "job opportunities" on online job posting advertisements, online dating websites, and spam emails.

What happens?

You receive items (electronics, jewelry, clothing, etc.) in the mail and are asked to ship them out of the country. The packages may be addressed in someone else's name (stolen credit card victim's name). The "employer" will provide you with a shipping label (also paid for with a stolen credit card). The "employer" will ask you for personal information such as Social Security number and bank account details so they can "direct deposit" your check. Generally you will never get paid.

Real reason you were chosen

1. Most merchants will not ship items out of the country.
2. Fraudsters need you to act as an intermediary to help get the goods out of the country. It also helps them avoid getting caught.
3. They use your personal information to steal your identity or takeover your account.

How to avoid this scam

1. If it's too good to be true, it probably is. Know who you are dealing with and don't reship packages.
2. If you didn't realize you were involved in a scam until the packages started arriving, refuse delivery or return to sender.
3. Report scams to the Internet Crime Complaint Center or contact your Postmaster.
4. Never give your private personal or financial information to anyone you don't know.

Learn more about work-at-home scams on the Better Business Bureau's web site.

Employment scam - New business opportunity

What happens?

Someone contacts you about a great new business opportunity. They need an employee or partner to sell cameras (or some other expensive product) for them and you will get paid. The scammer may even say they found you through eBay's Trading Assistant program. They will ask you to:

- List some products for sale on eBay or on your website.
- Use the money from the orders to pay their supplier. They will contact the supplier in advance to let them know you will be sending them money.
- Update your PayPal account address to their address. They will usually give you an address that looks like a regular address but it's a P.O. box.

After you pay the supplier, you will start receiving complaints from your buyers stating that they didn't receive their merchandise. Instead they received an empty box (from the scammer).

Next you contact the supplier. The supplier informs you that your partner said you would be sending money for gold bouillons, so they shipped the gold bouillons (not cameras) to your PayPal account address. Then, you remember that your partner asked you to change your PayPal account address to their address so they could pick-up the gold.

You paid the supplier for the cameras, so you file a complaint against the supplier. Unfortunately, you learn that you may be liable for the money since the supplier delivered the merchandise to your PayPal account address.

Real reason you were chosen

Scammers trick innocent and trustworthy people into sending them money and merchandise.

How to avoid this scam

1. If it's too good to be true, it probably is. Know who you are dealing with.
2. Don't list someone else's address on your PayPal account.
3. Verify your suppliers and don't send money to someone you don't know.
4. Only ship items to the address on the Transaction Details page.
5. Be on alert if you are asked to ship a lot of packages overseas or to the same post office box.
6. If you are a victim of this scam, contact PayPal at 1-888-221-1161 and say "Fraud" during the voice prompts. You should also contact your local police department or authorities to file a report.

Employee theft from your PayPal account

What happens?

You give your employee access to your PayPal account so they can do their job. Instead the employee transfers the money to their account, their friend's accounts, or to an offshore account. When you ask where the money went, they may tell you it was for a customer refund, used to pay a supplier, or used for payroll.

How to avoid this scam

1. Conduct thorough background checks and review your employee's account activity on a regular basis. The sooner you catch the problem, the better.
2. If you need an employee to manage your finances, make sure no one person has control over your account. When it comes to your finances, you should have checks and balances in place. Know where you are vulnerable.
3. Only give employees access to the information they need to do their job. Use PayPal's manage users functionality to set-up employee privileges. You can decide how much access to give each of your employees.

Return Abuse

What happens?

You sold something and the buyer files a complaint with PayPal stating that the product was damaged, you sent the wrong order, or the product was broken. When this happens, PayPal will ask the buyer to send the product back to you. When you receive the returned item, you may notice that an item that the buyer said was broken is in perfect condition or the buyer used the item before sending it back to you.

Real reason

The buyer may have been telling the truth – packages get damaged in shipment from time to time. However, the buyer may have also used the product, found it for a less expensive price somewhere else, or is trying to avoid your return policy.

How to avoid this

1. Pack your item securely to prevent shipping damage.
2. Communicate with your customers. Inform them of any flaws up front and provide many pictures so customers know exactly what they're buying. If you are selling a technical product, send installation instructions so the buyer can use the product.
3. Provide a customer friendly return policy so the buyer doesn't feel like they need to make up a reason for returning the order.
4. If you sold something on eBay and feel that your buyer is misusing the returns process, report it. If you sold something on your own website and feel that the buyer is misusing the return process, you can appeal your claim by contacting PayPal.
5. Create a list of customers you don't want to do business with again. The list should include information such as name, address, email and phone.
    - If you have your own website, the list could also include IP addresses, computer or device IDs, and credit card information.
    - Monitor new orders against your negative list.
    - If you're a smaller business, you can create a negative list using Excel or a Macro.
    - If you're a larger business, you can use a third-party rules system or develop your own in-house solution.

Affiliate Scams

What happens?

Your business uses affiliate marketers to help increase your sales. Affiliate marketers are paid based on their performance. Each time the affiliate refers a customer to your web site and it results in a sale for your business, they get paid. You may notice that one affiliate is generating higher sales than your other affiliates.

Real reason affiliate did so well

Fraudulent affiliates take advantage of your revenue share program by placing orders using stolen credit cards. Since you didn't realize the orders were fraudulent, you paid the affiliate. Months later you realize the affiliate was a fraudster because your customers filed complaints that their cards were stolen. As a result of this scam, you may incur the following types of losses: affiliate fees, cost of your product, shipping fees, transaction fees, chargeback fees, and your time.

How to avoid this

1. If you offer an affiliate program, make sure that you know who your partners are.
2. If you're partnering with a third party that refers affiliates, understand how the third party verifies and approves their affiliates.
3. Pay your affiliates 60 or 90 days after the order date. Most chargebacks and buyer complaints will happen within this time frame. The longer you can wait to pay the affiliate the better.
4. Watch for spikes in sales on products that come with higher affiliate payouts.
5. Review your orders for fraud. See our fraud prevention page for ways to help detect fraud.