Cybercrime

The real target of credit card thefts – you and your business!

With all the news of computer breaches at big retailers, business owners are concerned about the security of their systems. After all, if big businesses can't secure their customer information, how can anyone else?

Cyber-crime can impact your business even if you never incur a breach. The truth is, business owners, not the credit card owners, are the ones who really loose.

Case study

"The Con"

Your company sells widgets used in manufacturing

JohnSmithCo contacts your sales department via internet and places an order for $10,000 in widgets to be shipped to a country ending in "stan". He'll pay you in full, by credit card, but you have to arrange shipping through a company that he uses to handle the logistics.

Your sales department contacts **OutlawFreight** and they quote you $5,000 for associated shipping costs.

Your salesman tells JohnSmithCo that the total cost of the order is $15,000. JohnSmithCo gives him a credit card number. After a few days, the credit comes through and shows on your account, everything looks fine. You are instructed to wire the shipping charges to OutlawFreight and to send the product to their attention at a shipyard.

A few days later, you are notified that the credit has been backed off of your account. It turns out that the credit card number was stolen and the holder disputed the charge when it showed up on his statement.

Turns out that JohnSmithCo and OutlawFreight doesn't exist. Their addresses are actually a hair salon and municipal parking garage. You have lost your product, and worse yet, you wired away $5,000 of your money.

Why does the Con work?

Credit card holders and credit card companies often don't know that there was a breach until an unauthorized transaction is made. Also, it takes a few days to recognize and dispute the fraudulent charge, making the credit transaction appears legitimate at first.

Businesses and their employees believe the transaction is legitimate because they are brought into the scam. They have to contact the shipping company and "negotiate the cost", providing a belief they have worked for the sale, adding a sense of legitimacy. All good scams rely on this kind of "social engineering".

How to Protect Yourself?

Watch for Red Flags:

- New client that you know very little about
- A freight carrier that you know very little about
- Shipping overseas and to a country you have little experience with
- You get paid by credit card but have to "wire" money

Proactive measures?

Create and/or review information security “best practices” with your employees.

Review sales “best practices” with your employees and talk about “red flags”. Teach them how to verify clients.

Avoid “wire transfers” with unknown entities. Favor other means of secure payment.

Review the agreement with your merchant services provider. They monitor for fraudulent transactions. Sometimes, they reimburse you for loss when they miss a fraudulent charge.

Talk to your advisor at Haylor, Freyer & Coon. We can assist with:

- Cyber Liability Crime coverage
- Reviewing “best practices” procedures for Cyber Security
- Claim resolution in the event of a breach

Working together we can protect your business and reduce your risks.

Gia Diep

Director of Claims

Haylor, Freyer & Coon