# Credit Card Scams

by P W

Having had a web business since 1997, I've gotten used to scam artists trying to extract cash or free products from me. Most of these scammers are from Nigeria and Indonesia, where credit card fraud is considered a sport, much like soccer, only the participants get paid better. Their most common ploy is to place a large order for bike parts. One guy ordered 14 sets of Mavic wheels from us. He sent me three credit card numbers and asked me to split the charge amongst the three cards. All three cards had the same first 12 numbers. Only the last 4 numbers were different. Of course the cards were not his.

What he does is start with a Visa number that he knows is good and then finds a Visa/Mastercard vender who will cooperate with him. He has the vender try a series of numbers and expiration dates starting from the good number that he already has. So if the good card has 6335 as the last 4 numbers, he tries to run a small charge using 6336 as the last four numbers. He also has to try many expiration dates. It's a time consuming process, but potentially very profitable. If that works, he just voids that charge and he knows he can use that credit card number for a scam. He just keeps repeating the process until he has a whole pile of CC numbers that he knows is good.

Next, he needs to find a sucker to take his order and ship it. Since the card numbers are good, a vender in the US might just run the charges, (let's say it's a $12,000 purchase spread over 4 cards) and ship the goods via Fedex or UPS. It could be three weeks before the US vender gets a notice from his bank that the charges have been disputed by the rightful card owner, who, it turns out lives in Illinois, not Nigeria. But by then the goods have arrived in Nigeria, and there's simply no way to get them back. The vender is out not only the cost of the goods, but the shipping charges as well. And the rightful owner of the card is out some $50 or so, plus a lot of time dealing with the issue and getting a new account number.

What this means to the average consumer, is that in order to have a crook use your credit card number, the crook never has to actually see your card. The crook doesn't even have to know who you are or where you live. He doesn't care. He doesn't need to care, because lots of venders just type in the credit card number given by a customer and never check that the customer's address is correct, or ask for the "V" code on the back of the card (the last three numbers in the signature box on the back). So anybody with a credit card can become the victim of a scam, even if you never even use the card.

My advice is to regularly check your credit card balance online to see if there are any charges that you didn't make. And if you accept credit cards in your business, I recommend that you never ship outside the USA to any address other than the billing address of the credit card. Confirm with your CC provider that the address the customer gives you is correct, and be sure to get the "V" code from the back of the card. And, never, ever, ship to Nigeria or Indonesia without first being paid in full via Western Union. Don't ship until you have the cold cash in your warm hand! Don't accept foreign cashier's checks either, they can be forged easily, and it will be weeks after you have deposited the cashier's check before you find out that it is no good.

The risk of dealing with people from Nigeria and Indonesia is very high simply because the governments there are so corrupt. If you were able to contact the police in either country, chances are they know the scammer already. The scammer may well be related to the local police chief. So don't waste your time trying to contact the government to report the problem. I've sent faxes to

local police depts in both countries detailing the activities of credit card scammers in their towns. I've never heard back.

But you can have some fun with these jerks. When I get the order, (they always come in via email) I immediately call the issuing bank and report the card numbers. Then after a few hours, I email the scammer back, saying that one or more of the card numbers he gave me were declined by the bank. Within a few hours I'll have another email from the crook, giving me several more credit card numbers, usually with the same first 12 digits. I call the bank and give them the numbers. Of course, as soon as I call the numbers in to the bank, the accounts are closed and the true card owners notified.

Then I email the scammer again and say that the new card numbers have also been declined. What would he like me to do? Would he like to pay via Western Union, or a cashier's check? Or does he have another credit card he would like to use?

Invariably, another email comes in with several more card numbers and the process goes on. Eventually, I tell the crook that everything is now fine and the order has shipped. Now the crook gets very excited and wants to know the tracking number for the order. Emails will arrive every hour or so asking for the tracking number. If I reply, it's to say that the computer we use for shipping is out of order at the moment so I can't give him the number, but perhaps if he calls me later in the day I can give it to him.

A few hours later the phone rings. It's the scammer, wanting the tracking number. But the line seems bad and gosh but I can't hear him very well. Could he perhaps call back? He calls again. This gets repeated several times until I get bored and ask him for some more credit card numbers so I can call the bank and have those accounts closed, like I did with all of the other numbers he sent previously.

Click.

As of June 2005, these scams are so common I'm getting 3 or 4 large orders a day from these creeps. As you can well imagine, I don't have time to spend wasting their time. I just delete every one that comes in. I've also been getting emails from people who have either been scammed, or been targeted by scammers. And I've learned about a few more scams. One that is slowly catching on is the wire transfer scam. A Nigerian will place a large order and ask to pay via wire transfer. You might think this is pretty safe, since nobody but you can do a transfer from your account to another. But the internet is making life very easy for thieves these days. You know how you can set up with your fitness center or whatever to have them automatically get their monthly fee transferred from your bank account to theirs? Somehow these scammers can set up with your bank to do the same thing, or at least something similar, as long as they have your account number and the identification number of your bank. What happens is, you give the scammer your bank account number and any other info that he would need to wire you money. And then he can go to this web site, http://www.qchex.com. From there he pretends to be you. He creates an account with QCHEX and places an order with some other vender promising to pay with a QCHEX check. The unsuspecting vendor receives the QCHEX check, and ships the order. You never see a wire transfer to your account from the Nigerian. What you do see is a QCHEZ check drawn on your account. You call your bank and say, "What's this?". The bank explains it to you. You tell them you have never heard of QCHEX. The bank returns the QCHEX check to the unsuspecting vendor, who is out the value of the check since he has already shipped the goods to Nigeria.

Bottom line. Never give your bank details to anyone you are not absolutely sure is a legitimate business.

Lastly, I am not a clearing house for internet scams. Nor am I here to give you advice on what to do if someone attempts to scam you. I can't respond to emails about this subject. I offer this article simply to help others. It's all I can do.

P W

# New Credit Card Scam 2008

This one is pretty slick since they provide YOU with all the information, except the one piece they want.

Note, the callers do not ask for your card number; they already have it.. This information is worth reading. By understanding how the VISA & Master Card Telephone Credit Card Scam works, you'll be better prepared to protect yourself.

One of our employees was called on Wednesday from 'VISA', and I was called on Thursday from 'Master Card'. The scam works like this: Caller: 'This is (name), and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for $497.99 from a Marketing company based in Arizona?'

When you say 'No', the caller continues with, 'Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?'

You say 'yes'. The caller continues - 'I will be starting a Fraud investigation. If you have any questions, you should call the 1- 800 number listed on the back of your card (1-800 -VISA) and ask for Security.'

You will need to refer to this Control Number. The caller then gives you a 6 digit number. 'Do you need me to read it again?'

Here's the IMPORTANT part on how the scam works. The caller then says, 'I need to verify you are in possession of your card'. He'll ask you to 'turn your card over and look for some numbers'. There are 7 numbers; the first 4 are part of your card number, the next 3 are the security Numbers that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card. The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, 'That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?' After you say No, the caller then thanks you and states, 'Don't hesitate to call back if you do, and hangs up.

You actually say very little, and they never ask for or tell you the Card number. But after we were called on Wednesday, we called back within 20 minutes to ask a question. Are we glad we did! The REAL VISA Security Department told us it was a scam and in the last 15 minutes a new purchase of $497.99 was charged to our card.

Long story - short - we made a real fraud report and closed the VISA account. VISA is reissuing us a new number. What the scammers want is the 3-digit PIN number on the back of the card Don't

give it to them. Instead, tell them you'll call VISA or Master card directly for verification of their conversation. The real VISA told us that they will never ask for anything on the card as they already know the information since they issued the card! If you give the scammers your 3 Digit PIN Number, you think you're receiving a credit. However, by the time you get your statement you'll see charges for purchases you didn't make, and by then it's almost too late and/or more difficult to actually file a fraud report.

What makes this more remarkable is that on Thursday, I got a call from a 'Jason Richardson of Master Card' with a word-for-word repeat of the VISA scam. This time I didn't let him finish. I hung up! We filed a police report, as instructed by VISA. The police said they are taking several of these reports daily! They also urged us to tell everybody we know that this scam is happening.