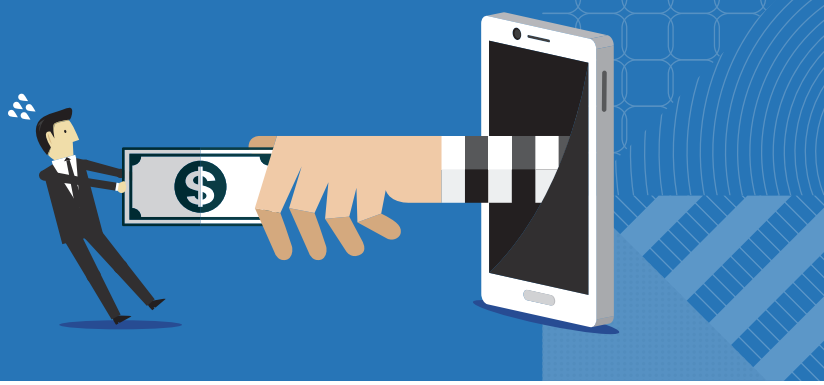
# Sorry, Wrong Numbers.



## THAT CALL NOTIFYING YOU OF UNAUTHORIZED CARD ACTIVITY MAY BE A SCAM

CONTRIBUTED BY ALAN BRILL, SENIOR MANAGING DIRECTOR, KROLL CYBER SECURITY AND INVESTIGATIONS

You walk through the door, juggling numerous shopping bags as you step over the packages that were delivered that day. The phone rings. You drop everything, literally, to answer. The caller addresses you by name and begins the conversation with:

"This is Louise Saganaw from [insert name of credit card] security calling. We have noticed unusual activity on your account. Do you have a moment to speak with me?"

Of course you do. You know your activity level is higher than normal because it's that time of year, but you want to make sure the charges on your account are actually yours. After all, credit card theft and fraud are rampant, and you've heard the stories about major data breaches. The caller continues:

"Did you spend $300 10 minutes ago at Chalmun's Cantina and Gift Shop in Tatooine?"

Um, no. The caller offers to help, once she verifies your personal information:

"If you can provide me with your card number, expiration date, and security code, along with your date of birth and social security number, I can remove that charge and put a fraud alert on your account if you would like."

You provide the information, and after a few seconds, the caller assures you that the charge has been removed and your account placed under a special protective watch. It's nice to know that your credit card company is watching out for you. Or so you think.

A week later, you get a second call from the credit card company. This time the caller asks about a series

of transactions in China. You've never been to China, much less charged nearly $5,000 there. The customer service representative says a travel notification was placed on your account a week ago. Not coincidentally, the notification was placed shortly after the previous call that you thought was from the same credit card company. The call where you provided all the personal information that the caller needed to take over your account.

You have been the target of a fraud. The first caller – who faked the information on the caller ID of the phone – didn't know you had that specific credit card. It was simply a guess. Once you admitted to having that brand of card, the fraudster ran through her script, got the information she needed, called the card company to notify them of "your" travel plans, and sent the card information to associates who charged goods and services at vendors in China.

Fraudsters are very creative. They study how businesses work, and one way they get your information is to tell you that you have already been the victim of a data theft – even though you haven't. Since you're worried that you'll be charged for a purchase you never made, you're ready to help the card company fight fraud. Instead, you're helping a fraudster commit it.

It's easy to fall for this scam because credit card companies often do call card holders when suspicious activity is detected. So, what should you do if you get a call? Here are some tips:

1. Don't assume the caller is actually from the bank or credit card issuer. Even if your phone's Caller ID gives the name of the card or the bank, remember that criminals can easily make the caller ID anything they want.
2. Listen to what the caller has to say, then tell them that you'll call the customer service number on the back of your card or on your card statement. Legitimate customer service representatives should encourage you to do so. Fraudsters may tell you that regular customer service can't help, providing a special "Fraud Department" number to call.
3. Don't let the caller bully you into providing your personal information. They may threaten that the charges cannot be removed if they don't get the information they need right away. Keep in mind that if there are fraudulent charges on your account, you have 60 days from the first statement that contained the mistake to dispute it.
4. Sign up to receive transaction notifications on all your accounts. Set the threshold at one cent ($0.01) so that you always receive alerts. Card thieves often make a couple of small charges – perhaps a dollar or less – to verify that the card is valid. If you receive alerts for such transactions, you can call customer service immediately and have them invalidate your card and send you a new one.

While these scam happens year-round, they become even more popular during the holidays. Scammers know that people are shopping more, particularly online, and that your awareness of card fraud is heightened as a result. They also know you may be more distracted than usual and provide information without thinking about it. One rule of thumb is to never give out your personal information to any unsolicited caller, regardless of how helpful they appear to be.

Don't help a fraudster to have a great holiday season. If you realize that you have fallen for one of these calls, immediately call your bank or credit card's customer service center for assistance. Then call the IDShield Investigators at 888.494.8519 for recommendations on next steps to protect your identity.