THE CONVERSATION
Academic rigor, journalistic flair

Credit card fraud: what you need to know

July 10, 2017 2.12am EDT

Online frauds on credit cards are on the rise especially during holidays. Mighty Travels/Flickr, CC BY-SA

Author

Bruno Buonaguidi
Researcher, InterDisciplinary Institute of Data Science, Università della Svizzera italiana

Languages

Read this article in English

If you are the owner of a credit or a debit card, there is a non-negligible chance that you may be subject to fraud, like millions of other people around the world.

Starting in the 1980s, there has been an impressive increase in the use of credit, debit and pre-paid cards internationally. According to an October 2016 Nilson Report, in 2015 more than US$31 trillion were generated worldwide by these payment systems, up 7.3% from 2014.

In 2015, seven in eight purchases in Europe were made electronically.

Thanks to new online money-transfer systems, such as Paypal, and the spread of e-commerce around the world – including, increasingly, in the developing world - which was slow to adopt online payments – these trends are expected to continue.

Thanks to leading companies such as Flipkart, Snapdeal and Amazon India (which together had 80% of the Indian e-commerce market share in 2015) as well as Alibaba and JingDong (which had upwards of 70% of the Chinese market in 2016), electronic payments are reaching massive new consumer populations.

This is a goldmine for cybercriminals. According to the Nilson Report, worldwide losses from card fraud rose to US$21 billion in 2015, up from about US$8 billion in 2010. By 2020, that number is expected to reach US$31 billion.

Commuters sit at a bus stop adorned with an advertisement of Indian online marketplace Snapdeal. Abhishek Chinnappa/Reuters

Such costs include, among other expenses, the refunds that banks and credit card companies make to defrauded clients (many banks in the West cap consumers' liability at US$50 as long as the crime is reported within 30 days for credit cards and within two days for debit cards. This incentivises banks to make significant investments in anti-fraud technologies.

Cybercrime costs vendors in other ways too. They are charged with providing customers with a high standard of security. If they are negligent in this duty, credit card companies may charge them the cost of reimbursing a fraud.

The types of frauds

There are many kinds of credit card fraud, and they change so frequently as new technologies enable novel cybercrimes that it's nearly impossible to list them all.

But there are two main categories:

- **card-not-present (CNP) frauds:** This, the most common kind of fraud, occurs when the cardholder’s information is stolen and used illegally without the physical presence of the card. This kind of fraud usually occurs online, and may be the result of so-called “phishing” emails sent by fraudsters impersonating credible institutions to steal personal or financial information via a contaminated link.

- **card-present-frauds:** This is less common today, but it’s still worth watching out for. It often takes the form of “skimming” – when a dishonest seller swipes a consumer’s credit card into a device that stores the information. Once that data is used to make a purchase, the consumer’s account is charged.

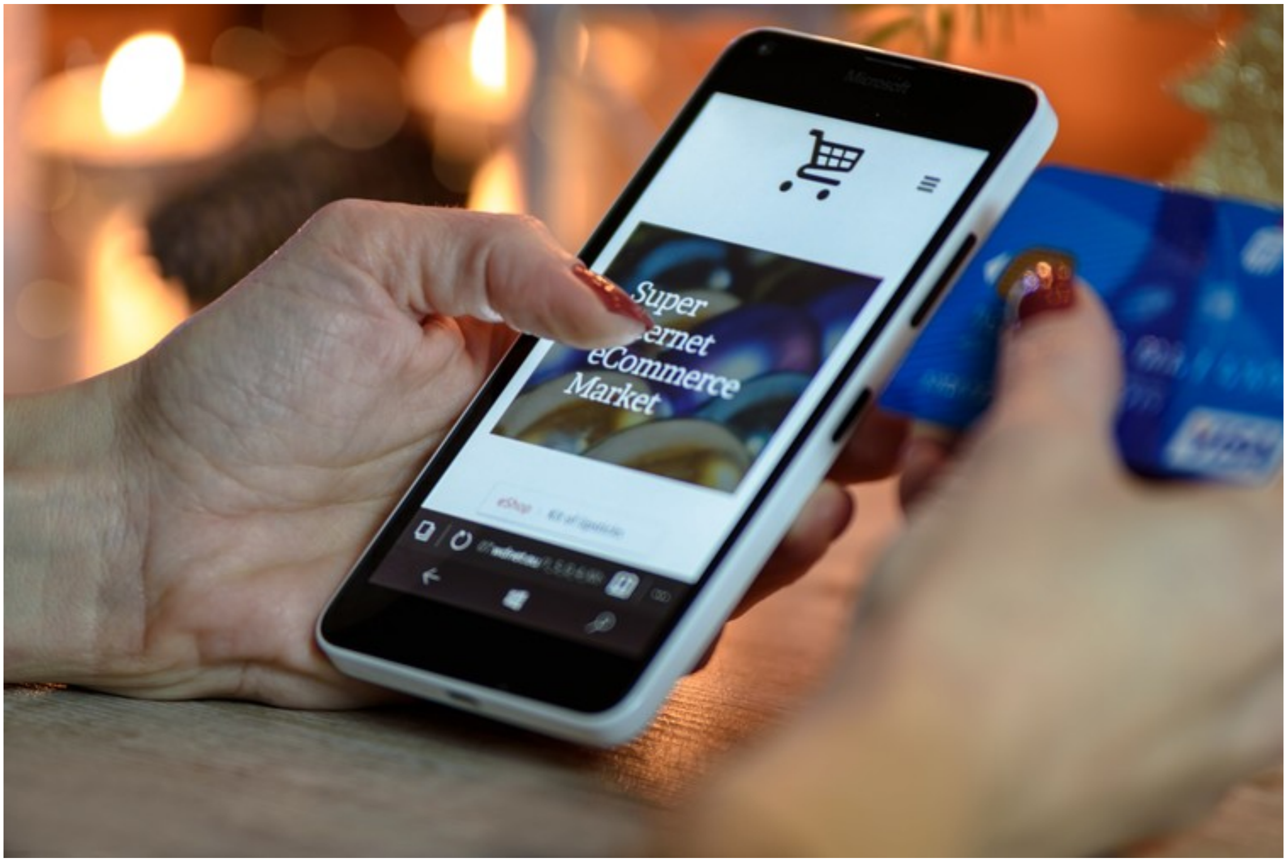
Credit card machine are sometimes used in the fraud called ‘skimming’ in which your card details are duplicated.
Izcool/Wikimedia

The mechanism of a credit card transaction

Credit card fraud is facilitated, in part, because credit card transactions are a simple, two-step process: authorisation and settlement.

At the beginning, those involved in the transaction (customer, card issuer, merchant and merchant’s bank) send and receive information to authorise or reject a given purchase. If the purchase is authorised, it is settled by an exchange of money, which usually takes place several days after the authorisation.

Once a purchase had been authorised, there is no going back. That means that all fraud detection measures must be done during in the first step of a transaction.



Buying online is practical and fast…yet risky when we do not known the vendors or their websites well. Photo Mix/Pexels

Here's how it works (in a dramatically simplified fashion).

Once companies such as Visa or Mastercard have licensed their brands to a card issuer – a lender like, say, Barclays Bank – and to the merchant's bank, they fix the terms of the transaction agreement.

Then, the card issuer physically delivers the credit card to the consumer. To make a purchase with it, the cardholder gives his card to the vendor (or, online, manually enters the card information), who forwards data on the consumer and the desired purchase to the merchant's bank.

The bank, in turn, routes the required information to the card issuer for analysis and approval – or rejection. The card issuer's final decision is sent back to both the merchant's bank and the vendor.

Rejection may be issued only in two situations: if the balance on the cardholder's account is insufficient or if, based on the data provided by the merchant's bank, there is suspicion of fraud.

Incorrect suspicions of fraud is inconvenient for the consumer, whose purchase has been denied and whose card may summarily be blocked by the card issuer, and poses a reputational damage to the vendor.

How to counter frauds?

Based on my research, which examines how advanced statistical and probabilistic techniques could better detect fraud, sequential analysis – coupled with new technology – holds the key.

Thanks to the continuous monitoring of cardholder expenditure and information – including the time, amount and geographical coordinates of each purchase – it should be possible to develop a computer model that would calculate the probability that a purchase is fraudulent. If the probability passes a certain threshold, the card issuer would be issued an alarm.

The company could then decide to either block the card directly or undertake further investigation, such as calling the consumer.

The strength of this model, which applies a well-known mathematical theory called optimal stopping theory to fraud detection, is that it aims at either maximising an expected payoff or minimising an expected cost. In other words, all the computations would be aimed at limiting the frequency of false alarms.

My research is still underway. But, in the meantime, to reduce significantly the risk of falling victim to credit card fraud, here are some golden rules.

First, never click on links in emails that ask you to provide personal information, even if the sender appears to be your bank.

Second, before you buy something online from an unknown seller, google the vendor’s name to see whether consumer feedback has been mainly positive.

And, finally, when you make online payments, check that the webpage address starts with **https://**, a communication protocol for secure data transfer, and confirm that the web page does not contain grammatical errors or strange words. That suggests it may be a fake designed solely to steal your financial data.

Cyber security Cybercrime credit cards Online fraud