ACUMINOR

Black Friday

Fraud Bonanza

relations@acuminor.com
www.acuminor.com

Acuminor
REPORTS

Report 2018:4

Black Friday is not only a day when people go on a shopping spree- it is also a day when cyber criminals go on a fraud spree. Black Friday, a phenomenon stemming from the U.S., has emerged as a well-established concept in the European market. In Scandinavia the popular discount day hit new record levels of spending in 2017, with Denmark reaching 282 million euros, Norway 373 million euros and Sweden 515 million euros. The retail bonanza has even extended to include virtually the whole week, as pre-sales start early. This has now come to be referred to as Black Week, even though the 'best' offers typically are launched on the Friday and aim to jump-start the gift-buying season.

Like shooting a sitting duck

Even though many people go to the stores during Black Friday, a significant proportion of the shopping has migrated to online retail. There are of course many positive sides to this, but it also results in substantial fraud challenges for the e-commerce sector, the financial industry and their customers.

With a high influx of consumers that share and transmit payment details, the cyber criminals hunting method more resemble that of shooting a sitting duck rather than patience and strategy.

The fraudster aims to obtain the information visible on the card (card number, date and CVC code) which can be used for remote purchases. The details can be obtained in various ways, e.g. via fraudulent e-mails and phone calls, malware or bought online on black markets. To unlawfully use someone else's card data to make a card payment is called card-not-present (CNP) fraud. The European Central Bank estimated the total value of CNP fraud in Europe to EUR 1.32 billion during 2016. Although, one should keep in mind that cases of fraud and values of fraud are commonly underestimated due to large numbers of unrecorded cases.

However, intelligence have gathered substantial information about the methods of CNP fraud. Knowing how fraudsters operate facilitates the possibility of developing prevention strategies or stop suspicious activity. Such strategies can be useful both on a corporate and individual level. Risk indicators of CNP frauds are e.g. sudden change in transaction behaviour, sudden increase in card payments and deviant (high value/frequency) transactions to e-payment service providers or virtual currency exchangers.

Things to consider when working with anti-financial crime in retail or the financial industry

There are a number of indicators of CNP fraud of which the more common ones are listed below.

Customer deviations

It can be difficult for merchants to verify that the true cardholder is the one authorising the purchase. It is therefore essential to monitor customer behaviour to detect deviant activity and being able to stop transactions. Fraudsters that have gotten their hands-on stolen card details often attempt to test the card in an online store by making a low value purchase before proceeding to buy more expensive items. If a merchant or financial institution recognises this pattern it increases the chances of preventing fraudulent activity.

If the store exists both as a physical store and an e-commerce site it can be useful to look at omni-channel data to define a customer profile. While high value purchases can be a risk indicator of a fraudulent purchase online, it does not necessarily have to trigger warning bells if the customer also make high value purchases in the physical store.

Transactions
Transactions during Black Friday/Black weekend will deviate from what you would normally see. However, by accounting for this deviation it is also possible to adjust risk settings in your transaction monitoring systems. During this period people tend to spend more per transaction, and they also purchase more regularly, which need to be accounted for. To ensure that you keep your false positives to a minimum, it might be desirable to adjust transaction velocity thresholds.

Non-retail sectors and refunds
Some industries outside retail are more prone to be exposed to CNP fraud than others, e.g. the airline and accommodation sectors. These industries can facilitate other crimes, such as trafficking in human beings, drug trafficking and illegal immigration. Thereto, the CNP fraud can precede refund fraud. In such cases the fraudster makes multiple bookings of hotel rooms simultaneously, only to cancel the bookings shortly afterwards and demand a refund to another credit card.

"There are some very effective actions that can decrease the risk of falling victim to fraudsters who hunt for card details"

How to proactively protect your customers
There are some very effective actions that can decrease the risk of falling victim to fraudsters who hunt for card details.

1. Use geo-blocking to prevent the card from being used outside of a certain geographical area

2. Issue cards that as default are blocked from internet purchases and allow the customer to easily switch it on when making a purchase

3.Make sure to encourage shopping on secure websites that use data transmission encryption

4. If possible, allow invoice as payment option

Better safe than sorry
Black Friday signals the start of the seasonal Christmas gift shopping. We all want to enjoy a merry Christmas so if you and your customers plan to spend money on gifts, make sure it goes to those you hold dear and not end up in the pockets of criminals.

Even though CNP fraud has been on the rise in the last couple of years, substantial efforts have also been taken to delimit the illicit use of cards. Thereto, increased e-commerce trade and a steady rise in monetary transactions also provides more data to study in the fight against financial crime.

In other words, make sure you use the information you have to truly understand your CNP fraud risks, especially this time of year.

ACUMINOR

Terms of use

You are free to use this report for your own personal development, in internal training or in other risk management activities.

You are of course not allowed to resell this report, nor claim that you have made it yourself.

Please remember to state the source as follows: Acuminor. (2018). Black Friday - Fraud Bonanza. Report 2018:4. Stockholm: Acuminor.