ACUMINOR

Merry Fraudsmas!

If it's too good to be true, it probably is

relations@acuminor.com
www.acuminor.com

Acuminor
REPORTS

Report 2018:5

Jingle bells, jingle bells
Jingle all the way,
Oh how fun to look at ads
And not fall for foul play,
Jingle bells, jingle bells
Jingle all the way,
Oh how fun to shop online
And keep all your details safe.

As the season of joy is falling upon us, we ourselves might fall onto fraudsters. Even though Christmas is the time for sharing, it should not include your banking details. Over the last couple of years there has been an increasing trend to give second-hand goods as Christmas gifts. The trend is growing stronger each year, and Swedes are big enthusiasts of both giving and receiving second hand goods, which is friendly both to the environment and the wallet.

Ho-ho-hold up, do not fall for Christmas scams

Christmas is a particularly lucrative season for shopping and much of the trading takes place online at various second-hand sites. Naturally, this is something criminals have not been late to exploit. Online market places exist in various forms, they can either be organised (e.g. Ebay) or less organised (e.g. social media platforms).

The former often rely on some sort of verification of the users and provide more reliable payment options. However, the latter often leave it up to the potential buyer/seller to confirm the identity or reliability of the other user. Both types of online markets are abused by fraudsters. Some general advice might come in handy in times of festive stress:

- Be cautious if the seller operates from abroad
- Do not pay in advance
- Do not migrate to less traditional payment options suggested by the offender
- Do not hesitate to abort the trade if you have a feeling that something is off

Online Shopping and Auction fraud

These types of fraud can occur in various ways, e.g. the fraudster can use a legitimate website for second-hand trading or auction to redirect the victim to a fraudulent site, or create fake accounts on legitimate websites. The peculiar thing with fraud on online trading platforms is that the victim can be both the buyer and the seller. In the former, the victim does not receive an item after having paid, or it arrives in worse condition than stated. In the latter, the victim sends an item which will never be paid for. Money transfers are commonly used in this fraud, but on an international level there have also been cases where fraudsters have paid with cheques, that not necessarily bounce. However, in such cases they might be forged or stolen and victims have reported receiving cheques with a higher value than agreed, and the victim refunds the difference. Thereto, victims are sometimes asked by the perpetrator to state their banking details, which are used to defraud the victim and could further lead to identity theft.

"An indicator of fraud is an alarmingly low starting bid for an expensive item"

In auction fraud, the accounts on auction sites are typically recently created and lack reviews. However, it can also occur that reviews exist, but are in fact fake.

An indicator of fraud is an alarmingly low starting bid for an expensive item. The perpetrator can also contact the victim via a private message/email and offer the victim to buy below a current bid.

"Fraud and transaction monitoring can only tell us once something has actually happened, and then it can be too late to save your customer's money"

False advertisements
Fraudsters also post false ads on second-hand sites in order to trick people into buying goods that either do not exist or they will never receive. False ads concerns all types of goods such as cars, clothing and accessories. However, among the most frequently reported false ads are ads related to mobile phones and other electronics. The victim is advised to transfer money in advance either directly into to fraudsters account, or to an account held by a goalkeeper or transfer money via an online payment service provider. When the victim has transferred the payment, the fraudster typically vanishes. The fraudster usually receives multiple incoming transfers with references to purchase of a product, and the money is often quickly withdrawn. The cost for the victim seldom exceeds EUR 1000, however the fraudster that scams numerous victims can obtain illicit profits of hundreds of thousands of Euros.

Being proactive is always best
Fraud and transaction monitoring can only tell us once something has actually happened, and then it can be too late to save your customer's money. Since your customers probably are your most valuable assets, it could be a good idea to inform about the potential dangers that lurk around in the darkness, in this so otherwise happy time of year. That way we can all help out to raise awareness and prevent the criminals from succeeding.

In conclusion: If a deal is too good to be true, it probably is. Let's make sure everybody knows that. ■

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). Happy Fraudsmas! - If it's too good to be true, it probably is. Report 2018:5. Stockholm: Acuminor.