Defining and Modelling the Online Fraud Process

J. Kävrestad and M. Nohlberg

School of Informatics, University of Skövde, Skövde, Sweden
e-mail: joakim@kavrestad@his.se; marcus.nohlberg@his.se

Abstract

As we have become more and more active online so has online criminals. Looking at one type of Internet crimes, online frauds, it is apparent that any-one can be targeted by a fraudster online. It has also been shown that online frauds keep increasing from year to year. It has even been estimated that one third of the adult population in America encounters online fraudsters, annually. In this paper we aimed to increase the knowledge about online frauds. We did this by producing a model that describes the process and aspects of an online fraud as well as a proposed definition of the term "online fraud". In this paper, we present the model and definition that we created and demonstrate their usefulness. The usefulness is demonstrated in our validation step, where we applied the definition to known online fraud schemes. We also conducted an interview in which the model was said to be useful in order to explain how an online fraud scheme was carried out, during a criminal prosecution. As such, that demonstrates that our model can be used to increase the understanding of online frauds.

Keywords

Online fraud, Definition, Model.

1 Introduction

With the technical development, most people has come to be present online in one way or another. You could even argue that a separate shadow-community has been established online. Looking at how the Internet has evolved it is now common to socialize, shop, pay bills and more on the Internet. However, as society have become more and more active online there has subsequently been a rise in criminal online activity that, in different ways, tries to exploit Internet users for malicious intents. One such activity that is constantly increasing is online frauds. During the last couple of years, several online fraud schemes received a lot of attention in media and they serve to show that lots of criminals are continuously trying to defraud as many Internet users as possible. Some of these fraudulent schemes includes the Microsoft phone scam (TechAdvisor, 2016), Internet romance frauds (Marimow & Hedgpeth, 2016) and Facebook frauds (ActionFraud, 2016).

Even if online fraudsters is not a new phenomenon, the number of online frauds continue to rise. In Sweden, The Swedish National Council for Crime Prevention (BRÅ) stated, in 2017, that frauds in general had doubled in the past ten years. BRÅ also shows that over 50% of the frauds are computer related (BRÅ, 2018). In 2013, IC3 (Internet Crime Compliant Center) reported that online frauds were increasing in America as well (IC3, 2013). Further, it is evident that a large number of internet users are targeted by online fraudsters, as one example, Pratt, Holtfreter and Reisig estimates that one third of the American adult population experience victimization – annually (Pratt, Holtfreter, & Reisig, 2010).

As of today, Swedish legislation does not have a comprehensive definition of what online fraud is. There are only two computer related crimes defined in Swedish law: computer intrusion and computer fraud. However, computer fraud in this context only covers crimes against databases and automatic data management (Polisen, 2018). Looking outside of Sweden there are several definitions available. In 2009 Alnajim discussed that Internet could be a method to carry out frauds (Alnajim, 2009). A more comprehensive definition was given by The Australian Federal Police in 2014 (AFP, 2018):

> *" The term 'online fraud' refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme."*

This definition lists the possible arenas were frauds can be committed. A potential drawback of that could be that it excludes frauds that are taking place in other arenas, such as social networks. A common denominator over in the discussed literature seems to be that online fraud is a fraud were the Internet is used. However, no one seems to discuss what "using the Internet" actually means. In this paper we propose a definition of online fraud and a descriptive model that explains the process and other aspects involved in an online fraud. To cover practical as well as legal aspects we make use of action based research where we include investigators from the Swedish police in the research process and validate our results with a representative from the Swedish court system.

With this approach we aim to reach conclusions that can provide a better understanding of online frauds in a global context as well as being practically applicable in the justice system, in Sweden as well as globally.

1.1 Research goals

This paper explores how the term "online fraud" can be defined and explains the aspects of an online fraud process. However, even if online fraud is a term used all over the world, as a crime it is to some extend defined in legislation. As such, the intent of this paper is to provide insight into what characterizes online frauds that can be implemented in any local jurisdiction rather than a fit-all legal definition. This paper aims to reach the following research goals:

Goal 1: Create a definition of online fraud.

Goal 2: Create a descriptive model that explains the process and aspects involved in an online fraud.

1.2 Outline

The rest of this paper is structured as follows. Section 2 describes the method used in this study. Section 3 presents the outcome of the study and Section 4 presents a discussion on the results presented and possible directions for future research.

2 Methodology

The research aim was addressed using an action based approach with qualitative interviews. As described by SBU, an action-based approach allows the participants to take an active part in the research (SBU, 2014). In this case investigators from the Swedish police was involved in the study as interview subjects and a series on semi-structured interviews was held with them. The interviews was transcribes and analysed using thematic coding as described by Robson (2011). The study began by constructing a definition and a model of online fraud based on the sources presented in the introduction. That was used as input for the first round of interviews. The model and definition was then updated and new interviews was held and the process was iterated until all participants were satisfied.

Lincoln and Guba (1985) describes four criteria's for quality in research; Credibility, Transferability, Dependability and Conformability. The main tasks conducted in this study to ensure credible results involved taking care to document the research process in order to make the study easy to replicate and understand. Also, Lincoln and Guba suggest using triangulation to increase the probability of producing reliable results. Triangulation was using in two ways in this study. First, separate interviews were held with different respondents, different investigators from different departments of the Swedish police. Second, after all interviews where completed, a final interview was held with a person from a different professional background than the other subjects. The respondent in the final interview was a judge from a Swedish court. Finally the definition was further validated by using lists of online fraud schemes presented by IC3 (2018) and ActionFraud (2018) to ensure that the definition covered all the listed fraud schemes The research process is visualized in Figure 1.

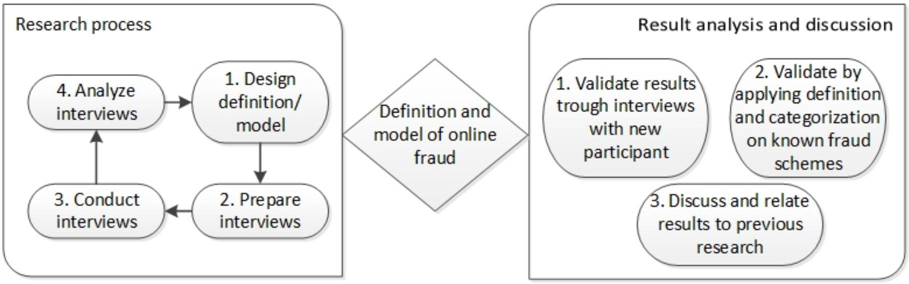
Research process
4. Analyze interviews
1. Design definition/ model
3. Conduct interviews
2. Prepare interviews
Definition and model of online fraud
Result analysis and discussion
1. Validate results trough interviews with new participant
2. Validate by applying definition and categorization on known fraud schemes
3. Discuss and relate results to previous research

Figure 1: Research process overview (Authors own)

3 Results

This section presents the results of the study. Since an iterative method was used, the results from each step in the research process will be presented. The final sub-section will present the final definition and model of online fraud.

3.1 Preparation

Using the background literature, presented in the introduction section, a proposed definition and model was created before the first round of interviews. First, Swedish law states that a fraud is when someone tricks someone else into doing something that person would not normally do. That implies that a fraud must have the following entities:

- A fraudster that commits the fraud
- A victim that is defrauded

In criminology means, opportunity and motive is often discussed as the aspects of a crime (Sarnecki, 2009). It seems reasonable to include those aspects in the definition of online fraud and in this step it is done as follows:

- Means: The tools needed/used to commit the fraud
- Opportunity: The ability of the fraudster to get access to an attack vector
- Motive: The reason why the fraudster commits the fraud

The previous discussion on current definitions of online fraud indicates that a common denominator in earlier definitions is the fact that online fraud is fraud that uses the Internet as the means for the crime. This would indicate that an online fraud is a fraud where some computerized tools are used in order to commit fraud. With this conclusion the following suggested definition was created:

"Online fraud is a fraud where computerized tools are used as the means needed to commit the crime."

Given that definition, the online fraud process was modelled as shown in Figure 2.

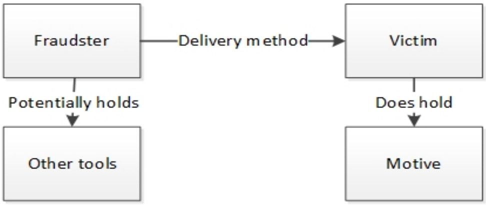

Figure 2: Prototype model that was presented to participants (Authors own)

The model reflects the fraudster and victim as entities. Further, the fraudster can hold tools used for the fraud and the victim must hold something that the fraudster wants to get. Finally the fraudster and victim must be connected through a delivery method.

3.2 Interview round 1

During the first interview round, interviews with two persons was held. One of the participants worked as an investigator of financial crimes with the Police department in Örebro and the other was a former investigator who now worked with coordinating online fraud investigations within the Swedish police. These and all other interviews in the study was conducted and transcribed in Swedish. Citations from the interviews are translated to English. Citations and summaries presented in this paper was reviewed by the participants to reduce the risk of any information being changed or misinterpreted in the translation. The participants were handed the model and definition from the previous step before the interviews, they served as a starting point for the interviews. The interviews in this step then served to provide answers to the following questions:

- What should decide if a crime is to be classified as online fraud or not?
- What characterizes online fraud?
- What should control how to classify online frauds?

The participants expressed that there is currently no common definition of online fraud but a main factor is that the frauds are carried out over the Internet in some way. A key point that was expressed is that just using digital tools in some way is not enough for a fraud to be classified as an online fraud. It should rather be classified depending on the how the fraud is delivered to the victim, or as one participant expressed it:

"…it is that Internet has been used in some way, either that the contact has been taken through the Internet or that the whole transaction has been carried out over the Internet."

A lot was said about fraud as a crime that clearly showed that a key factor is that for something to be classified as a fraud it must include that a fraudster persuades a victim into giving up something of value. Thus, a fraud brings monetary loss for the victim and equal monetary gain for the fraudster.

Based on the input from the interviews it is evident that a definition of online fraud must include that a fraud must be delivered over the Internet in order to be called an online fraud. However, it is also evident that there are several delivery methods that are used to commit online frauds. Consider the process of using an automated dialler to call peoples analogue phones and defraud them. That scheme begins in a digital manner but end up being analogue. On the other hand, Microsoft frauds as described by TechAdvisor (2016) begins with an analogue call and ends up being an online fraud when the user is persuaded into installing software on his computer. Considering the input from the interviews and the distinct differences in the different fraud schemes the definition was updated as follows:

Online fraud is a fraud where computerized tools are used for full or partial delivery of the fraud.

The word fraud was intentionally left undefined in this definition. This is to make the definition of online fraud depend on the legal definition of fraud, thus making it work in a global context and if the law is changed. Given the new definition, the model was redesigned to reflect that the delivery of an online fraud can be separated into several steps. The model produced in this step is presented in Figure 3.

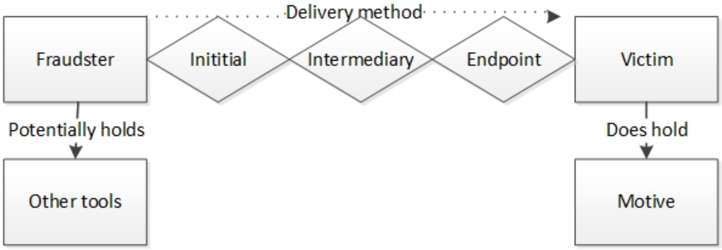

Figure 3: Model after first interview round (Authors own)

3.3 Interview round 2

This interview round used the model and definition from the previous round as input and served to answer the following questions:

- What are the strengths and weaknesses about the model and definition?
- What changes should be made to the model end definition?

Given the information from the second interview round the definition is fine and does not need further updates. It was pointed out that it is preferable to make the definition depend on the legal definition of fraud.

For the model it was pointed out that the model should reflect that a fraud is about a fraudster affecting the victim into giving something up. The victim giving something up rather than the perpetrator just taking it is what differs fraud from theft. Also, the keyword “motive” was not seen as clear and was suggested to be changed to a word that reflects that the motive is to get something of value. Based on the response the following changes was made to the model, resulting in the model shown in Figure 4.

- The word motive was changed to “Article of value/money”
- An arrow indicating that the fraudster wants the valuable was added
- Arrows showing that the Fraudster deceives the Victim into giving up the valuable was added.

In the resulting model (Shown in Figure 4) the boxes represent the entities that are present in any fraud; a fraudster, a victim and some article of value or money. The tilted boxes visualize the different steps in the delivery of a fraud. The dotted line shows relationships; in this case the presence of a delivery method and that the fraudster wants the article of value. Finally the dashed lines indicates the actions that needs to take place, namely that the fraudster is persuading the victim of giving him or her the article of value.

After this round the participants from the police was pleased with the definition and model. Thus, no more interviews were held. Instead, the model and definition was validated as presented in the next sub-section.

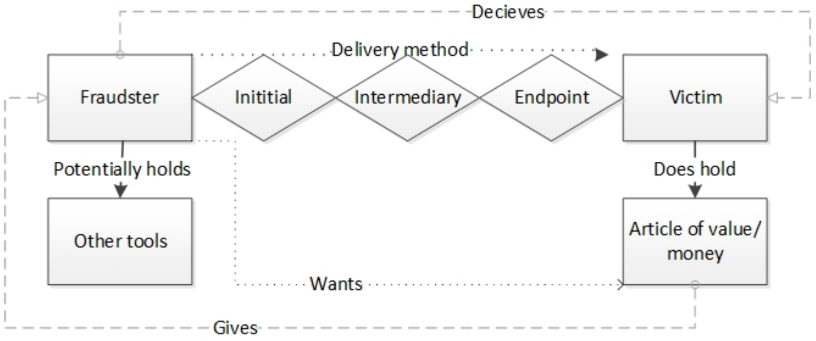

Figure 4: Final model of the process of online fraud (Authors own)

3.4 Validation

The results of this study was validated by conducting an interview with a judge from a Swedish court and by practical implementation of the definition by matching it to actions commonly referred to as online fraud schemes. The interview served to answer the following three questions:

- Q1: What is online fraud?
- Q2: What are your thought about the definition and its model?
- Q3: In what ways do you think that the definition and model can be used?

The information gathered from this interview provided the following answers to the three questions:

- Q1: The participant concluded that a fraud is a crime were a fraudster is deceiving a victim into giving him something of value.
- Q2: The interview showed that the participant thought that the model matched the definition and that the definition covered all aspects of online fraud.
- Q3: The participant said that she thought that the model could be used to explain to jurors how a specific online fraud crime was actually executed.

To summarize, this interview generated information about the model and definition that matches the information gathered in the previous steps and validated the statement that a fraud is a crime were the fraudster is deceiving a victim into giving him something of value. Further, this participant said that the model could be used as a tool to explain to jurors how a certain crime was committed – thus indicating a practical use of the model.

To further validate the correctness of the definition it was tested in real world scenarios by matching is against lists of online fraud schemes presented by IC3 (2018) and ActionFraud (2018).In total, the two sites listed 35 different schemes as online fraud schemes.

Most of the schemes used in this validation was concluded to be online frauds according to the definition. However some schemes was not considered online frauds according to the definition that we propose. This was due to the fact that they did not meet the legal criteria's to be considers fraud in Swedish legislation due to one of the following requirements for an act to be consider fraud under Swedish law (SFS1962:700, 2018):

- A fraud must involve monetary gain or include gaining something of monetary value for the fraudster and equal loss for the victim
- A fraud must involve that the victim is deceived into giving up something of value to the fraudster

This leads to that acts such as identity theft and computer intrusions cannot count as online frauds within Swedish legislation since they do not count as frauds. And given the definition that we propose, *Online fraud is a fraud where computerized tools are used for full or partial delivery of the fraud,* an act has to be a fraud to be an online fraud. However, the acts that was not considered online frauds because of this reason would have been matched by the definition of online fraud if they were considered frauds, legally.

Further, some acts were considered *possible* matches for the definition and because the description of the acts gave room for several different way of carrying them out. In these cases, the way that they was to be carried out would determine if they match the definition or not. The possible matches where the following:

- Credit card fraud: If the attacker steals the credit card it should not be considered fraud, however if the fraudster deceives the victim into giving up his credit card details it would count as online fraud.
- Nigerian letter: if sent over e-mail Nigerian letters are online frauds, however when sent over physical mail they are not.
- Phishing: phishing e-mail aimed at gaining personal information or injection malicious software into the victims computers are not online frauds. However, if phishing is used to obtain money it is considered online fraud.
- Account takeover: If an account is compromised by hacking, it is not a fraud. However if the victim is deceived into giving up the log in information to his bank account that is fraudulent.

This practical implementation of the definition shows that the definitions excludes actions that are not considered frauds by law and frauds that are not carried out online.

Also, it does include schemes that are defined as frauds and were a part of the delivery method is digital. This indicates that the definition does work in reality.

4 Conclusions

In this paper we use an action-based approach implemented by using iterative semi-structured interviews with investigators from the Swedish police to develop a definition of online fraud. We then used triangulation as suggested by Lincoln and Guba (1985) to validate our results. The validation process included an interview with a person with a different perspective and background, namely a judge from a local court. We also tested the practical use of the definition by matching it against known online frauds schemes. The outcome of this process was the following definition of online fraud:

"Online fraud is a fraud where computerized tools are used for full or partial delivery of the fraud"

This definition meets the key criteria's that for an act to count as an online fraud it has to, first and foremost, be considered a fraud. Second, what decides if the fraud is online or offline should be determined by the way that it is communicated with the victim. During the study it became evident that a fraud may be partially delivered in an online fashion and should then still be considered an online fraud, this is also covered by the definition that we propose. To further clarify the concept of online fraud we also developed a model of online fraud. The model is intended to provide an overview of the components and events that are present in an online fraud scheme. The final model is presented in Figure 4.

5 Discussion

The aim of this study was to increase the knowledge about online fraud by developing a definition and model that described the aspects of online fraud. As described in the background literature there are currently different understanding of what constitutes an online fraud and this can make it tedious to study the area. Further, as stated by the judge in the validation interview, our results can be used to explain to jurors what happened in a specific fraud case. It's easy to make the argument that it is crucial for a working justice system that jurors and laypersons understand how a crime was committed in full. Thus, as our work can contribute to a better understanding of online fraud, it also contributes to the justice system.

It should be mentioned that this study was conducted in the context of the Swedish legal system. We have taken great care to make the results generalizable in that context by implementing our results in the real world scenario and conducting interviews with a person from a different branch of the legal system than the interview participants. It is our strong belief that, since our definition is based on the legal definition of fraud, it is also applicable globally. There is, however, a need for further research in order to make that claim. As for the model, aspects of it does depend on the Swedish legal definition of frauds, namely that a fraud must include the fraudster getting something of monetary value. As such, it may be hard to use without modification in some other countries. However, the model still gives insight into the online fraud process that would be globally useful.

It should also be noted that while this study is focused at online frauds it does provide insight into online crime in a more general meaning. What is interesting, on that topic, is that several criminal activities online are not conducted by computer professionals. Rather, it appears as if traditional criminals are to a large extent making use of the Internet to commit traditional crimes in a more convenient, online manner.

6 References

ActionFraud. (2016). Alert: Watch out for Facebook Marketplace fraud. Retrieved from https://www.actionfraud.police.uk/news/alert-watch-out-for-facebook-marketplace-fraud-dec16

ActionFraud. (2018). Online Fraud. Retrieved from https://www.actionfraud.police.uk/node/298

AFP. (2018). Online fraud and scams Retrieved from https://www.afp.gov.au/what-we-do/crime-types/cyber-crime/online-fraud-and-scams

Alnajim, A. M. (2009). *Fighting Internet Fraud: Anti-Phishing Effectiveness for Phishing Websites Dectection.* Durham University,

BRÅ. (2018). Bedrägerier och ekobrott. Retrieved from https://www.bra.se/brott-och-statistik/statistik-utifran-brottstyper/bedragerier-och-ekobrott.html

IC3. (2013). *2012 Internet Crime Report*. Retrieved from Fairmont, WV

IC3. (2018). Internet Crime Schemes. Retrieved from https://www.ic3.gov/crimeschemes.aspx

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* (Vol. 75): Sage.

Marimow, A. E., & Hedgpeth, D. (2016). Md. man convicted of fraud in 'Internet romance scheme'. *The Washington Post*. Retrieved from https://www.washingtonpost.com/local/public-safety/he-wooed-them-and-fleeced-them-maryland-man-convicted-of-running-online-romance-fraud-scheme/2016/05/05/24112c5e-12be-11e6-93ae-50921721165d_story.html?utm_term=.bb6fb203a73a

Polisen. (2018). It-relaterade brott - utsatt Retrieved from https://polisen.se/utsatt-for-brott/olika-typer-av-brott/it-relaterade-brott/

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296. doi:10.1177/0022427810365903

Robson, C. (2011). Real world research: A resource for users of social research methods in applied settings 3rd edition. In: West Sussex: John Wiley & Sons.

Sarnecki, J. (2009). *Introduktion till kriminologi*: Studentlitteratur.

SBU. (2014). Utvärdering av metoder i hälso-och sjukvården: En handbok. *Stockholm: SBU–Statens beredning för medicinsk utvärdering.*

SFS1962:700. (2018). *Brottsbalk*: Sveriges Riksdag.

TechAdvisor. (2016). Microsoft phone call scam: don't be a victim. Retrieved from https://www.techadvisor.co.uk/how-to/security/microsoft-phone-scam-dont-be-victim-tech-support-call-3378798/