ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse105922020.pdf
https://doi.org/10.30534/ijatcse/2020/105922020

The Current State of Social Commerce Fraud in Malaysia and the Mitigation Strategies

Yurita Yakimin Abdul Talib[1], FarizaHanim Rusly[2]
[1]Tunku PuteriIntanSafinaz School of Accountancy, Universiti Utara Malaysia, Malaysia, yurita@uum.edu.my
[2]Tunku PuteriIntanSafinaz School of Accountancy, Universiti Utara Malaysia, Malaysia, hanim@uum.edu.my

ABSTRACT

Previous research has acknowledged the widespread adoption of social networking (SNS) platforms for online shopping among social media users, known as social commerce. While the positive effects of shopping on social network platforms have received much attention in the literature, the negative outcomes of this type of commerce remain under-explored. Notably, the prevalence of cybercrime, specifically related to online purchasing fraud, has increased rapidly. To address this gap, this paper explores the online purchasing fraud cases related to shopping on the social network platforms, the demographic characteristics of the victims and the financial impact of the fraud to the victims. In addition, this paper also explores the strategies to mitigate the fraud cases. The data was gathered from social network users via an online survey. The findings show that almost seventy percent of the respondents were currently using social network platforms to shop, with Facebook being the most popular platform. For those who use social commerce, as many as twenty-four percent (24%) admitted to having been victims of purchasing fraud. The overwhelming majority of the victims were highly-educated middle-income earning married women, aged between 26–35. In terms of financial impact, the majority of the victims had lost nearly RM400. Few mitigation strategies were identified, including word of mouth, background check of sellers, reliable and transparent transaction process, and avoidance.

Key words: Social commerce, social network, online purchasing, fraud, online fraud, victimization, mitigation strategies

1. INTRODUCTION

Cybercrime encompasses criminal activities conducted through the use of computers and the Internet and its related technologies. Identity theft, malicious attacks, and online fraud are typical of cybercrime. Cybercrime has received considerable attention recently from the government of Malaysia due to the growing number of reported cases. In 2018, Malaysia experienced over 10,000 reported cybercrime cases, the majority of which involved online fraud[1].One of the most common fraud cases is e-commerce or online purchasing fraud. Online purchasing fraud occurs when a fraudulent seller deceives a potential buyer into giving money with a promise of goods or services via the Internet that do not exist and there is no intent to provide them. The National Consumer Compliance Centre (NCCC) of Malaysia[2]reported that online purchasing fraud generated the highest number of reported complaints in 2017, amounting to 10,160. This marked an increase of 3,000 complaints compared to the previous year. Normally, these complaints are associated with online purchasing via social networking sites (SNS) platforms. Malaysia is not alone. The Australian Competition and Consumer Commission (ACCC)[3]found that 19.9% of online shopping scams reported in August 2019 were conducted via SNS. It is clear that the evolution of SNS as an online business platform has created new opportunities for fraudsters to conduct social interactions with their potential victims. Fraudsters, either anonymously or posing as trustworthy businesspeople, pretend to be genuine sellers and initiate social relationships to build trust with the intention of defrauding their victims.

Surprisingly, many shoppers believe what they see and read advertised on SNS. For instance, a media news site in Malaysia reported that RM700,000 was fraudulently obtained from hundreds of individuals by one online seller via his Instagram shop [4]. This data illustrates how the revolution in the way goods and services are bought has created more risk of victimization for many, as well as more opportunities for fraudsters. Put simply, SNS have become the favoured method for scammers to get in touch with their potential victims. A review of current social commerce fraud data is much needed to help clarify the current state of affairs in Malaysia and stimulate new research ideas.

This study focuses on a very specific fraud: online purchasing fraud conducted via social networking platforms, coined as *social commerce fraud*. The objectives of this study are to investigate the current usage of SNS for commercial activities (i.e. social commerce), to examine social commerce fraud cases, to investigate the characteristics of the fraud victims, to examine the financial impact of the fraud cases, and finally, to examine the mitigating strategies. It is hoped that the findings of this study might serve as a reference for government and enforcement bodies to design a strategy to mitigate this type of cybercrime. It is particularly recommended that the findings be used by online shoppers as guidance before committing to purchases on SNS platforms.

2. LITERATURE REVIEW

2.1 Social Commerce

As a major development, social commerce is expected to evolve as a widely accepted practice, rather than remain a temporary business trend, although the specifics of the practice are still at an emerging stage [5].Social media refers to Internet-based applications that allow people to create, share, or exchange information, video/pictures, interests and ideas. Some prominent examples of social media are Facebook, LinkedIn, Pinterest, Instagram, and Twitter. There were 3.5 billion users of social media in 2019 [6]. In 2018, social networking via Facebook, Instagram, Twitter and other platforms was the second most popular activity among Malaysian Internet users after interactions via communication applications such as WhatsApp, Telegram and WeChat [7]. The evolution of social network not only as marketing platform [8], but also completely new methods of purchasing goods and services have grown exponentially worldwide and are becoming norms.

In this study, social commerce refers to the use of social networking sites such as Facebook and Instagram as a sales or business transaction platform. This category matched the first classification of social commerce as suggested by [9],[10]. Presently, many online sellers use social networks beyond marketing platforms, as a tool to interact with and conduct direct business transactions with their potential customers. Naturally, it is attractive for online sellers to use social networks as their sales platform because a huge investment is not required compared to creating a business website or paying for the use of online marketplaces. On Facebook, sellers can create a business page to advertise their products and perform actual sales transactions. On Instagram, online sellers can create an 'Instashop' for their business activities. Using these social media platforms, sellers do not need to pay any hosting fee, maintenance fee or other expenses related to business website development. Indeed, it can be said that almost anyone can become a social media seller. Stephen and Toubia [11]made the point that social commerce sellers should, therefore, be thought of as individuals instead of firms.

Bringing much easier ways of collecting data, the social media revolution has brought with it a variety of new studies. A review of the literature indicates that most studies of social commerce have been on the positive impact of such commerce and its advantages for consumers. Wang and Zhang [5] investigated this impact from 2005 to 2011, identifying four dimensions: people, management, technology, and information. Prior studies of purchases on social media tended to investigate the ways in which social support and the nature of such relationships impacted on the intention to make purchases on social media [12]. Hajli[13] argued that the perceived usefulness of social media, coupled with trust, had the largest effect on decisions to make online purchases on such platforms. Although now widely used, Hajli [14] suggested social commerce checks such as recommendations and referrals, forums and communities, and the ratings and reviews. While such studies emphasised the positive aspects of social commerce development, the literature, to date, offers little empirical investigation into social commerce fraud. The advent of the Internet, new methods of communication and related technology has provided new opportunities for online crimes and frauds [15],[16].

2.2 Online Fraud

Put simply, fraud occurs when someone is cheated out of money by another party (individual or business on the basis of a seller's promise to provide services or goods which do not exist, are not intended to be provided or were misrepresented [17]. Fraudsters offer products or services and demand a certain amount of money. Victims proceed with payment, even though the products or services have not yet been received. Victims only realise that they had been defrauded later when the seller is unresponsive to their communications [17]. Online fraud, now a global issue, uses various Internet technologies such as e-mails, chatrooms, websites, and most recently social networking sites to conduct fraudulent transactions. Such tools are relatively cheap or free and are easily accessible by fraudsters [18].

There are numerous different types of fraud activities carried out online. Button et al. [16] identified that the most common types of online fraud in the UK and Wales are job scams, investment scams, relationship scams, and purchasing of goods scams. Cross et al. [19] also confirmed that there are various different ways in which online fraud can be perpetrated such as advanced fee fraud, employment opportunities, phishing emails, and romance fraud. In Malaysia, statistics provided by MyCERT highlighted that five of the most common online fraud incidents reported in Malaysia from 2011 to 2013 were job scams, 419 scams, online scams, phishing, and purchasing fraud [18]. Amore recent statistic showed that as many as 2252 cases of online fraud were reported between January 2019 to August 2019 [20]. Online fraud is expected to increase in tandem with the evolution of online technologies [21] and it should be assumed, as with other countries, that many more Malaysians have been subjected to online fraud but did not report the incidents [1]. Typical reasons for not reporting such incidents are embarrassment, self-blame, the small scale of the fraud, and the victim not knowing what to do [17].

2.3 Social Commerce Fraud

While there are various types of online fraud, this research specifically focuses on purchase fraud committed online via social networking sites, also known as social commerce fraud. Purchase fraud occurs when a fraudulent seller deceives a buyer. When this happens, the legitimate buyer will lose money for goods or services that did not exist/arrive or will purchase goods found to be fake or faulty. The explosive growth of online purchasing on social networking sites has certainly increased the risk of fraud for the general public.

CyberSecurity Malaysia reported that as many as half of the online purchasing fraud cases in Malaysia occurred on social media sites [18]. More recently, the NCCC Malaysia reported that complaints related to online shopping scams were mainly associated with social networks [2]. Similarly, in Australia, the ACCC reported that there were 9,692 reports on online shopping scams, amounted to a total loss of $3,278,796. Of these reports, 19.4% of the online purchasing scams were conducted through social networking sites, coming third after the Internet and Email [3].

There are a few unique features of the use of social networking sites for business transactions which may have contributed to social commerce fraud cases. Firstly, any individual can begin to engage in online selling on social networking platforms because they do not have to invest much on website development nor pay for access to online marketplaces. Anyone can become an online merchant without any filters. To repeat a point made above, by Stephen and Toubia [11], traders via social commerce are individuals rather than companies. The anonymity afforded by social media sites is an attractive feature of non-genuine sellers or scammers in defrauding innocent shoppers. The non-transparency and invisibility of sellers in social networks increases the risk of victimisation for social media shoppers. Anyone is vulnerable to social media shopping scams in which the perpetrators, anonymously or even posing as people one trusts, cheat people through purchasing activities. When shoppers engage in online purchases, they do not know the sellers well enough and it is very difficult to prove that an act of fraud had occurred. To put it another way, when money is involved there is always someone trying to take advantage and at any time the seller's account on social networking sites can be closed.

Secondly, social networks connect online shoppers directly with others to form a social community. The immediacy provided by social networks allows online shoppers to obtain and share product-related and seller-related information within their social community. The current literature suggests that active online shoppers and active participants on online forums are exposed to a higher risk of victimisation by online fraud [22]. A market surveyreported that while 92% of respondents worldwide trusted recommendations by friends and families, as many as 70% of them ranked online consumer reviews as the second most trusted source of information [23]. The trust developed among an online social community certainly has an impact on purchasing decisions. Researchers discovered that social media characteristics such as social support which facilitate the social interactions of consumers inevitably leads to increased trust and intention to buy [12],[13]. While interactions and exchanges of information help online shoppers to make informed and smarter buying decisions, online scammers also utilise such features to lure their victims. Prior studies have found that victims responded to scams because of appeals to trust [17],[24].

The third feature of purchasing via social networking sites pertinent to this study concerns payment method. Normally, buyers are required to make up-front payments through bank transfers directly to a seller's bank account [25]. Using this method, it is difficult to recover the money sent if sellers fail to deliver the ordered products because there is no third party to govern the transactions. This is unlike online shopping via marketplaces such as Amazon, Shopee and Alibaba which implement an escrow method of financial arrangement. The escrow method uses a third party to hold and regulate payments between two parties, meaning that payments will only be released to sellers after buyers receive their products with no complaint.

3. METHODOLOGY

The population of this study was selected from social media site users. Naturally, the sample was collected through an online survey via social media platforms such as Facebook and Instagram and communication applications such as WhatsApp, WeChat and Telegram for a two-month period, using a structured questionnaire. Respondents were asked to provide data on shopping and fraud experiences on social networking sites as well as demographic characteristics. Characteristics of the social media users and their purchases were assessed to establish diversity in terms of their age, gender, education level, employment, social media platform usage and type of product purchased. And the end of the questionnaire, respondents were asked to provide their opinion and recommendation on how to avoid from being scammed when conducting an online purchase via social networks. Overall, a total of 721 social media users in Malaysia responded to the questionnaire. After removal of cases of non-users of social networking sites, outliers and missing values, there were 707 remaining usable cases.

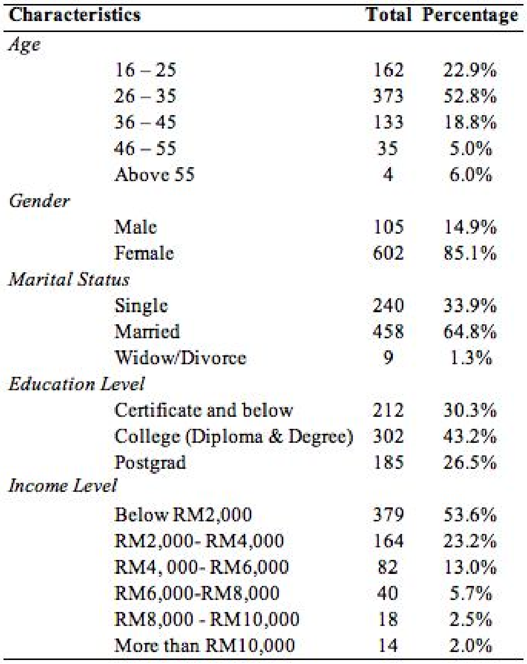
4. FINDINGS

4.1 Respondents' Profile

The basic demographic information of the respondents is presented in Table 1. It can be seen that social network users are mainly women with 52.8 percent of them being between the ages of 26 – 35 and 22.9 percent of them being between the ages of 16 - 25. Clearly, the usage trend is more popular among millennium generations. Majority of them attained at least a Diploma with various income levels.

Social media networking was the second most popular activity (after information search) among Malaysian internet users (Malaysian Communications and Multimedia Commission, 2014). As shown in Figure 1, this study found that the most used social networking platforms among Malaysians are Facebook (61%), Instagram (23%) and Twitter (12%).

Table 1: Respondents' Characteristics (n=707)



Characteristics	Total	Percentage
Age		
16 – 25	162	22.9%
26 – 35	373	52.8%
36 – 45	133	18.8%
46 – 55	35	5.0%
Above 55	4	6.0%
Gender		
Male	105	14.9%
Female	602	85.1%
Marital Status		
Single	240	33.9%
Married	458	64.8%
Widow/Divorce	9	1.3%
Education Level		
Certificate and below	212	30.3%
College (Diploma & Degree)	302	43.2%
Postgrad	185	26.5%
Income Level		
Below RM2,000	379	53.6%
RM2,000- RM4,000	164	23.2%
RM4, 000- RM6,000	82	13.0%
RM6,000-RM8,000	40	5.7%
RM8,000 - RM10,000	18	2.5%
More than RM10,000	14	2.0%

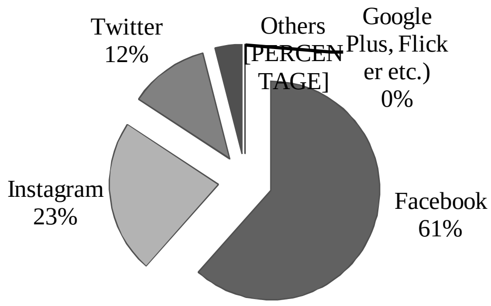
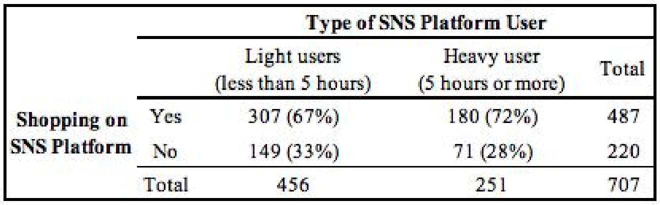


Figure 1: Social Networking Sites Usage

4.2 Level of Usage and Shopping Pattern

Generally, most of the social network users spent up to five hours per day on their social network accounts (65%) and the remaining 35 percent of the respondents spent more than five hours per day on social networking sites. This indicates that Malaysians, generally, love to spend time on social network.

Table 2: Type of SNS Shoppers

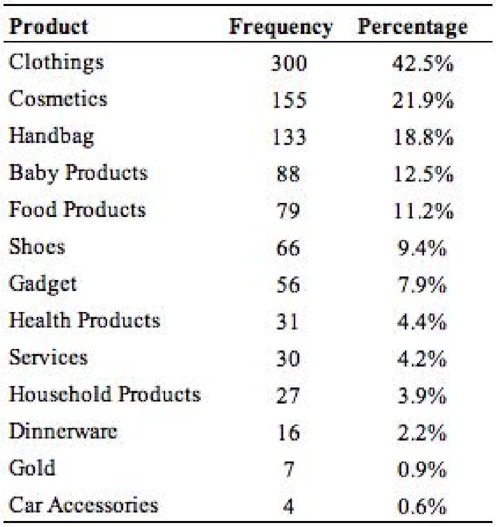


		Type of SNS Platform User		
		Light users (less than 5 hours)	Heavy user (5 hours or more)	Total
Shopping on SNS Platform	Yes	307 (67%)	180 (72%)	487
	No	149 (33%)	71 (28%)	220
	Total	456	251	707

In line with the popularity of social network, the trend of online shopping via social networking platforms among Malaysians is also rising, with 69 percent of respondents (i.e. 487) saying that they had bought from social networking platforms at least once for the last 12 months (Table 2). When comparing between types of social network users and their shopping behavior, heavy users tend to become shopper on the social networking platforms (72%) as compared to light users (67%). This indicates that the more time spend time on the social networking platforms, they more tendency to shop on the platforms. With these results, it can be affirmed that the level of awareness among Malaysians regarding social commerce is considerable and will continue to grow. The increase in mobile device usage and improvements in Wi-Fi technologies, bandwidth, etc. could also be large contributing factors for the rise of social commerce. Naturally, entrepreneurs, online or offline should see this as an opportunity to take advantage of the popularity of social media, especially Facebook, as platforms for legitimate commerce.

In terms of buying patterns, typical products bought on social networks include clothing, baby products, food products, gadgets, books, health products, gold and many more items. The highest purchase categories were clothing, cosmetics and handbags (Table 3). This data is consistent with the respondents' gender, dominated by females (85.1%).

Table 3: Frequency of product/service purchased on SNS platforms



Product	Frequency	Percentage
Clothings	300	42.5%
Cosmetics	155	21.9%
Handbag	133	18.8%
Baby Products	88	12.5%
Food Products	79	11.2%
Shoes	66	9.4%
Gadget	56	7.9%
Health Products	31	4.4%
Services	30	4.2%
Household Products	27	3.9%
Dinnerware	16	2.2%
Gold	7	0.9%
Car Accessories	4	0.6%

In terms of spending, most buyers had spent between RM100 and RM399 over the last 12 months. Surprisingly, five respondents had made purchases over RM10,000 (Figure 2) of items such as gold and car accessories.

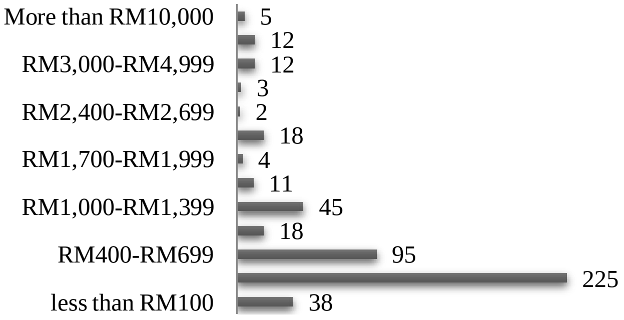
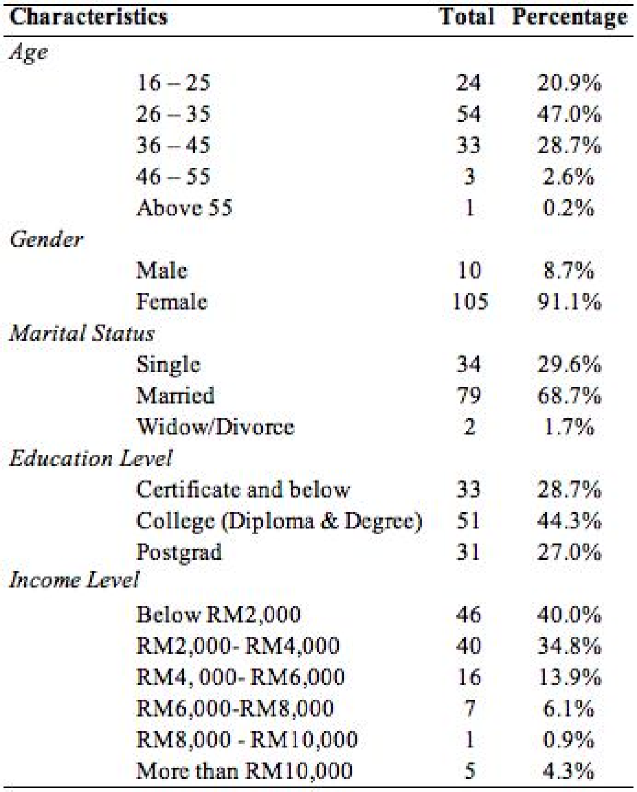


Figure 2: Amount of Spending on SNS Platforms (in 12 months)

4.3 Social Commerce Fraud Victim

As social commerce continues to evolve, so do opportunities for fraudsters to find victims. In this study, we identified 105 victims of social commerce fraud. Looking at the demographic profile of the victims (Table 4), the majority were married women aged between 26 – 35 who were highly educated with an income level of RM2,000 – RM4,000. It can be summarized that the victims of social commerce fraud are often young educated female with a good income.

Table 4: Social commerce fraud victims' profile (n=105)



Characteristics	Total	Percentage
Age		
16 – 25	24	20.9%
26 – 35	54	47.0%
36 – 45	33	28.7%
46 – 55	3	2.6%
Above 55	1	0.2%
Gender		
Male	10	8.7%
Female	105	91.1%
Marital Status		
Single	34	29.6%
Married	79	68.7%
Widow/Divorce	2	1.7%
Education Level		
Certificate and below	33	28.7%
College (Diploma & Degree)	51	44.3%
Postgrad	31	27.0%
Income Level		
Below RM2,000	46	40.0%
RM2,000- RM4,000	40	34.8%
RM4, 000- RM6,000	16	13.9%
RM6,000-RM8,000	7	6.1%
RM8,000 - RM10,000	1	0.9%
More than RM10,000	5	4.3%

Two types of purchasing fraud victims on social network were identified. The type 1 victim is someone who bought on social network but never received the goods. The type 2 victim is someone who bought on social network, received the goods but the goods were not as described /promised. Out of 488 respondents who bought on social network, 4.7% (23 shoppers) indicated that they were victims of purchasing fraud type 1, 14.3% (70 shoppers) were victims of type 2 and twenty-one respondents were victims of both types of fraud.

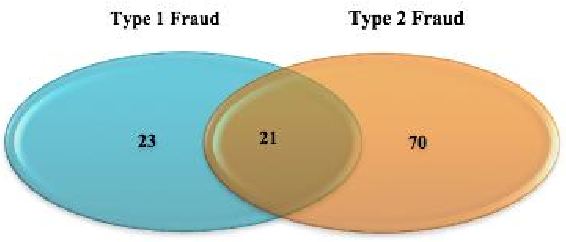
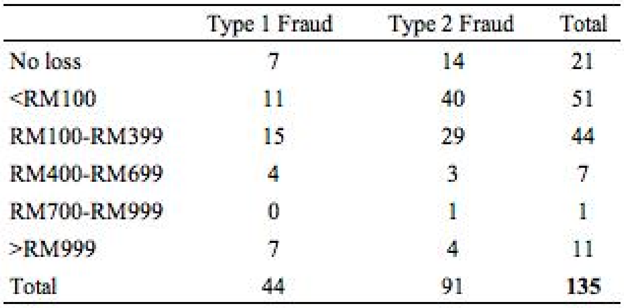


Figure 3: Social commerce fraud victims by fraud type

With respect to the amount of loss incurred, majority of the victims for both categories had lost some amount of money (*see* Table 4). For type 1 fraud, most of the victims had lost between RM100 to RM399. For type 2 fraud victims, a great majority (69 victims) had lost below RM399 and several victims (8.1 percent) had lost a huge amount of money (i.e., RM1000 and above) to the scammers. However, twenty one respondents who said they had been scammed had not actually lost any money as they asked for refund or replacement from the scammers. In other words, a great majority of the victims did not take further action (i.e. ask for refund or replacement) even they realized they have been scammed.

Table 5: Victims of social commerce fraud segmented by loss amount



	Type 1 Fraud	Type 2 Fraud	Total
No loss	7	14	21
<RM100	11	40	51
RM100-RM399	15	29	44
RM400-RM699	4	3	7
RM700-RM999	0	1	1
>RM999	7	4	11
Total	44	91	**135**

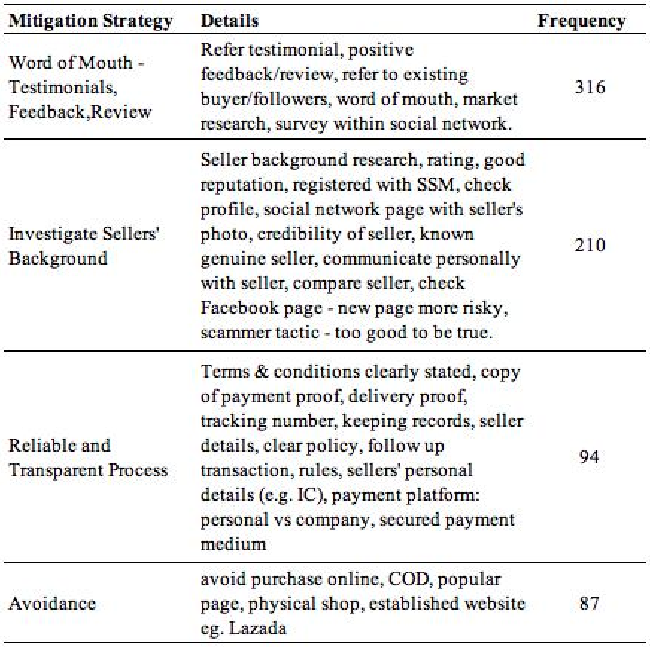
Note: Scam Type 1 = not receive product/service; Scam Type 2 = received but fake or not similar as described.

4.4 Users' Perception on Mitigation Strategies

Finally, this study investigated the strategies to reduce or mitigate the social commerce fraud from the social network users' perspective. Users' perspective is important because users have knowledge about their tasks that will provide sound information about their future decision [26].Based on the respondents' answer to an open-ended question regarding their perception on how to mitigate social commerce fraud, we come out with four major ways or strategies, as shown in Table 6.

Many respondents suggested that potential buyers need to do some research or investigation before buying on social networks. Almost half of the respondents agreed that referring to testimonials, reviews and feedbacks from previous buyers (i.e. word of mouth) is the most important strategy to ensure that the sellers are genuine. Once the potential buyers satisfy with the word of mouth, they can proceed by investigating the sellers' background such as checking their profile, photos, business page date, registration with SSM, and also, they can communicate with the sellers. The third mitigation strategy is to check for the reliability and transparency of the purchasing process through a clearly stated terms and conditions. This terms and conditions should include product details, seller details, payment method details, delivery process, proof of payment, tracking number and follow up process. And finally, almost 10% of the respondents suggested to avoid buying from social networks. Alternatively, they can buy from a more secured platform such as Lazada, or physical store.

Table 6: Mitigation strategies



Mitigation Strategy	Details	Frequency
Word of Mouth - Testimonials, Feedback,Review	Refer testimonial, positive feedback/review, refer to existing buyer/followers, word of mouth, market research, survey within social network.	316
Investigate Sellers' Background	Seller background research, rating, good reputation, registered with SSM, check profile, social network page with seller's photo, credibility of seller, known genuine seller, communicate personally with seller, compare seller, check Facebook page - new page more risky, scammer tactic - too good to be true.	210
Reliable and Transparent Process	Terms & conditions clearly stated, copy of payment proof, delivery proof, tracking number, keeping records, seller details, clear policy, follow up transaction, rules, sellers' personal details (e.g. IC), payment platform: personal vs company, secured payment medium	94
Avoidance	avoid purchase online, COD, popular page, physical shop, established website eg. Lazada	87

5. DISCUSSION AND CONCLUSION

This study explored the social network usage and fraud cases experienced by social network users in Malaysia. As the present results demonstrate, Facebook is very popular among Malaysians and is the most used platform for online purchasing. The most bought items are fashion-related and beauty products, consistent with the majority of the social commerce purchasers consisting of women who work in the public and private sectors. Most of these purchasers have acquired a stable income and have already settled down. With a tertiary educational background, they could be also be considered technologically savvy and have a tendency to spend money on social commerce platforms.

However, as mentioned above, while there is great potential for social commerce activities to grow on this platform, there is also an increasing number of incidents of dishonest acts committed by online sellers. The predominant types of fraud experienced by Malaysian social commerce buyers are products received with compromised quality, followed by goods not delivered. Although the amount of loss amounts to below RM500 on average, the results highlight that the majority of victims are young and educated women. It can certainly be said that the unique features of anonymity, non-transparency, invisibility and payment method features of social commerce mean that individuals are exposed to a high risk of falling prey to fraud, regardless of their educational background.

Considering the results of the study, there are theoretical as well as practical implications. Theoretically, these results may provide a good basis for further work on social commerce fraud victim profiles and their purchasing decisions. In addition, this study points to the need for continued research on the correlations between demographic background, human characteristics and the potential for becoming victims of social commerce. Practically, the findings also serve to inform buyers interested in engaging in social commerce by suggesting some mitigating strategies. Firstly, buyers must be aware that scammers on social networks may be selling products at a very low price but buyers are advised not to naively buy a product if the offered price is “too good to be true”. Secondly, buyers need to research information about sellers (i.e. check their seller profile), delivery, payments and other terms and conditions. If possible, it is clear that purchasing from registered companies is preferable to purchasing from individual sellers. Buyers are in a better position if something goes wrong and there is a need to make a complaint or dispute the transactions to the authorities. Finally, buyers need “to think twice” before making advance payments to anyone they don’t know. One possible solution is to buy from sellers that offer cash on delivery (COD) to avoid being scammed. The results of this study might also be useful to policymakers by providing current demographic data for social commerce policy development in the interest of promoting and allowing social commerce to flourish in the near future.

There was a significant limitation of this study related to the diversity of the respondents. The respondents were limited to friends, families, friends of friends and friends of families of the researchers. Although a snow-balling technique was used to distribute the questionnaire, it was still within the researchers’ personal circle. For example, all of the researchers were Malays and the great majority (92.6%) of the respondents were Malays. They might have similarities in personality (or culture, religion) and some similar traits will be more obvious. As a result, it does not provide a good foundation for generalization. In the future, the research sample can be expended to a wider and more diverse audience in terms of gender and ethnicity that would allow for better research results.

ACKNOWLEDGEMENT

This research project is funded by Ministry of Higher Education (MOHE) of Malaysia under Fundamental Research Grant Scheme (FRGS).

REFERENCES

1. CyberSecurity. **MyCERT Incident Statistics**, Retrieved from https://www.mycert.org.my/assets/graph/pdf/2015-1.pdf, 2015.
2. K. Khalidi, **AduanPenipuan Online Tertinggi**. *Kosmo!* pp. 6, October 6, 2015.
3. ACCC(n.d). **Online Shopping Scams**. Accessed from https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams
4. A. Rusman, and W. Aziz. **UmpanSelebriti**. *Harian Metro*, pp.4, October 1, 2015.
5. C. Wang, and P. Zhang, P. **The evolution of social commerce: The people, management, technology, and**

information dimensions. *Communications of the Association for Information Systems*, *31*(5), 1-23, 2012. https://doi.org/10.17705/1CAIS.03105

6. **Global Digital Report 2019**. Retrieved from: https://wearesocial.com/global-digital-report-2019.
7. Malaysia Communications and Multimedia Commission, **Internet Users Survey 2018.** Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018-(Infographic).pdf
8. I. K. Sumerta, G. P. A. Widyagoca, and I. W. Meryawan. **Online Consumer Behavior on Using Social Media on E-Commerce, based on the AISAS Model Approach. Case Study; Bukalapak, Tokopedia and Blili.com**,*International Journal of Advanced Trends in Computer Science and Engineering*, 8(1.5), pp. 234 - 242, 2019. https://doi.org/10.30534/ijatcse/2019/4281.52019
9. Z. Huang, M. Benyoucef, **User preferences of social features on social commerce websites: An empirical study**. *Technological Forecasting and Social Change*. 95, 57–72, 2015. https://doi.org/10.1016/j.techfore.2014.03.005
10. Indvik, L.**The 7 Species of Social Commerce**. Mashable.Com, 5–10. Retrieved from http://mashable.com/2013/05/10/social-commerce-definition/. 2013.
11. A. T. Stephen, and O. Toubia.**Deriving value from social commerce networks.** *Journal of marketing research*, *47*(2), 215-228, 2010. https://doi.org/10.1509/jmkr.47.2.215
12. T. P. Liang, Y. Ho, Y. W. Li, and E. Turban. **What drives social commerce: The role of social support and relationship quality**. *International Journal of Electronic Commerce*, *16*(2), 69-90, 2011. https://doi.org/10.2753/JEC1086-4415160204
13. M. Hajli. **A research framework for social commerce adoption.***Information Management & Computer Security*, *21*(3), 144-154, 2013. https://doi.org/10.1108/IMCS-04-2012-0024
14. M. Hajli.**Social commerce adoption model**. In Proceedings of the UK Academy of Information Systems Conference, 2012.
15. R. Z. Abdulgaziev, M. R. Alsultanov, V. N. Mamichev, A. R. Sarukhanyan, D. I. Sostin, and A. N. Sukhorukova. **Social Causation of Criminalization of Cyber Crime Committed with the Use of Information Technology**, *International Journal of Advanced Trends in Computer Science and Engineering*, 8(5), pp. 2459-2463, September - October 2019. https://doi.org/10.30534/ijatcse/2019/90852019
16. N. S. Jamil, S. S. Kamaruddin, and F.K. Ahmad. **Social Tension and Crime Related Events Detection on Twitter**, *International Journal of Advanced Trends in Computer Science and Engineering*, 8(6), pp. 2821-2824, November–December 2019. https://doi.org/10.30534/ijatcse/2019/23862019
17. M. Button, C. Nicholls, J. Kerr, and R. Owen. **Online frauds: Learning from victims why they fall**. *Australian & New Zealand Journal of Criminology*, 2014. https://doi.org/10.1177/0004865814521224
18. eSecurity, **Online Fraud: A review on Current Trend and Mitigation to Reduce the Threat**, Retrieved from: https://www.cybersecurity.my/data/content_files/12/1526.pdf, 2015.
19. C. Cross, R. G. Smith, and K. Richards. **Challenges of responding to online fraud victimisation in Australia**. *Trends & Issues in Crime and Criminal Justice*, 474, 2014.
20. e-Security. **Malaysia Threat Landscape 2018 – Based On Incidents Reported To CyberSecurity Malaysia**. Retrieved from: https://www.cybersecurity.my/data/content_files/12/1971.pdf, 2019.
21. B. Xiao, and I. Benbasat.**Product-related deception in e-commerce: a theoretical perspective**. *MIS Quarterly*, 35(1), 169-196, 2011. https://doi.org/10.2307/23043494
22. J. Van Wilsem. **'Bought it, but Never Got it': Assessing Risk Factors for Online Consumer Fraud Victimization.***European sociological review*, 2011. https://doi.org/10.1093/esr/jcr053
23. Nielsen.**Word of mouth still most trusted resource**: **implications for social commerce**. Retrieved From http://digitalintelligencetoday.com/word-of-mouth-still-most-trusted-resource-says-nielsen-implications-for-social-commerce/, 2014.
24. T. Buchanan, and M. T. Whitty. **The Online Dating Romance Scam: Causes and Consequences of Victimhood**. *Psychology, Crime & Law, 20*(3), 261-283, 2014. https://doi.org/10.1080/1068316X.2013.772180
25. A. Leeraphong, and B. Papasratorn. **S-Commerce Transactions and Business Models in Southeast Asia: A Case Study in Thailand**. *KnE Social Sciences*, 2018. https://doi.org/10.18502/kss.v3i1.1397
26. R. H. Raja Mohd Ali, R. Mohamad, Y. Y. Abdul Talib, A. Abdullah, **The roles of top management and users in strategic IS planning: A perspective of SMEs.***International Journal of Information Systems and Project Management.* 6, 61–80, 2018.