(2020) 26 JUUM 65 - 72
https://doi.org./10.17576/juum-2020-26-08

Online Scammers and Their Mules in Malaysia

Mohamad Rizal Abd Rahman

ABSTRACT

Scammers have adopted various scam techniques in defrauding their victims. One of the most common ways is by engaging mules to assist them. This article discusses relevant legal provisions in Malaysia which are enforced against these illegal activities. The objectives are to highlight the significance of section 415 and 420 in dealing with online scammers, and section 414 and 424 in dealing with mules who assist them. Relevant cases are also cited to enable readers to understand the real scenario behind these scammers and their mules. The article ends with a scenario to be pondered in between human conscience and government intervention in order to prevent, if not eradicate, these illegal activities.

Keywords: scam; mule; Malaysia; law

INTRODUCTION

Humans are prone to be susceptible to matters which benefit them financially and emotionally. Fake multilevel marketing or pyramid system, business opportunities, auctions, credit card offers, loans, job vacancies, etc are the most common fake "attractions" that scammers adopt in defrauding others. Either by way of phishing, pharming, grooming, etc, scammers usually highlight matters which are in demand to those in needs. And the way they target people, it is not simply executed by random choices. They have indeed studied the profiles of the victims before scheming to defraud them. The more skillful a scammer in social engineering, the more potential of success he will gain.

According to the last three years reported incidents based on general incident classification statistics issued by CyberSecurity Malaysia, online fraud has continued to be the highest reported incidents, totaling 7774 reports in 2019, 5123 reports in 2018, and 3821 reports in 2017. From January until March 2020, there have been 2330 reported incidents on online fraud. This is indeed a worrying trend.[1]

While prevention mechanisms are constantly updated, legal enforcement should also be in the best form. Hence the following discussion will entail the relevant legal provisions and cases on the matter.

DEFRAUDING A PERSON

Kevin Mitnick, the first hacker who was listed in the FBI's most wanted list, made the following testimony beforethe US Senate Governmental Affairs Committee on 2 March 2000:

> "The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the *weakest link* in the security chain, the people who use, administer, operate, and account for computer systems that contain protected information...
>
> In my experience, when I would try to get into these systems, the first line of attack would be what I call a social engineering attack, which really means trying to manipulate somebody over the phone through deception. I was so successful in that line of attack that I rarely had to go towards a technical attack. The human side of computer security is easily exploited and constantly overlooked."[2]

The phrase weakest link here refers to a human being. The moment a scammer manages to manipulate the victim's emotion and interest, it will be a walk in the park to the scammer who will not have to endure painstaking hacking and cracking scheme. Bypassing the technical stage, by social engineering the victim himself will allow access.

The word fraud does not appear anywhere in the Penal Code of Malaysia. Nevertheless, the statute adopts the word "cheating", which is equivalent to fraud.

The general provision of section 415 Penal Code states:

> "Whoever by deceiving any person, whether or not such deception was the sole or main inducement,-
>
> a. fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property; or
> b. intentionally induces the person so deceived to do or

omit to do anything which he would not do or omit to do if he were not so deceived and which act or omission causes or is likely to cause damage or harm to any person in body, mind, reputation, or property, is said to "cheat"."

Section 417 Penal Code states:

"Whoever cheats shall be punished with imprisonment for a term which may extend to five years or with fine or with both."

In addition to the general provisions, several specific provisions are also provided for in the Penal Code. For example, regarding cheating and dishonestly inducing delivery of property, section 420 Penal Code states:

"Whoever cheats and thereby dishonestly induces the person deceived, whether or not the deception practiced as the sole or main inducement, to deliver any property to any person, or to make, alter, or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment for a term which shall not be less than one year and not more than ten years and with whipping, and shall also be liable to fine."

Now, if we look closely at the wording of section 415, the pre requisite for the act of cheating is that a person must be deceived. If a computer is cheated, can the person who cheats be charged under this section?

The answer to this question can be seen in section 11 which states:

"The word "person" includes any company or association or body of persons, whether incorporated or not."

Is computer a "person"? Of course, legally not by virtue of the provision. Even factually, it is also not right to include "computer" under the category of "person". Despite the fact that computers are capable of doing things beyond our imagination, yet the intelligence in computers are merely artificial. This is due to the fact that computers lack empathy. That is why, in the United Kingdom, when the Fraud Act was passed in 2006, the "deceiving a person" element is intentionally left absent. Section 2(1) of the Act states that fraud by false representation occurs when someone expressly or impliedly does the following act:

"... dishonestly makes a false representation, and intends, by making the representation, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss."

Section 2(5) of the Act further states:

"For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)."

The Fraud Act clearly favours false pretence over deception, thus there is no more need to establish that a human being is deceived.[3] Unfortunately, the definition of "cheating" in the Penal Code remains unchanged, where "deceiving a person" element is still a requirement. That indeed explains why in the classic case of *PP v Aman Shah (1990)*[4], the accused was charged for criminal breach of trust by using computers and convicted under section 408 of the Penal Code. What happened in that case was that he engaged in *salami slicing* (a method where money is deducted from clients' accounts in nominal value in stages) while working as an officer at Hock Hua Bank. He reseted all nominal value in a client's account to zero, and transferred the value to another account owned by him in another bank. Although there was an element of cheating, he was not charged under section 415/420, because he cheated nobody but the computers of Hock Hua Bank.

However, for online cheating committed against a person, the person who commits it can be charged under section 415 or 420. For example, cheating people through websites or emails about fake get rich schemes or free/discounted products. The following cases illustrate this criminal practice.

In *PP v Mohamad Azmil Mohd Diah [2017]*[5], an unemployed was charged and convicted under section 420 of the Penal Code for cheating a fast-food outlet supervisor in relation to the sale of a smart phone (iPhone 6) which he advertised through WeChat in March 2016.

In *Rose Hanida bt Long v PP [2017]*[6], a secretary to the Head of Corporate Banking Department at OCBC Bank was was charged and convicted under section 4(1)(a) of the Computer Crimes Act and section 420 of the Penal Code for 13 series of unauthorised access using ID and password belonging to the Department Head. The acts were committed to cheat the OCBC Bank Finance Department by submitting false financial claims, causing the department to approve and deposit RM348,294.81 to her account in 160 transactions, between January 2010 to December

2013. Her appeal against sentences was dismissed, and instead the High Court ordered for her sentence to be increased due to the gravity of her action.

In *Basheer Ahmad Maula Sahul Hameed & Anor v PP [2016]*[7], a HSBC bank officer and her husband, a mechanic, were accused of transferring and withdrawing RM85,180 from 3 passengers and 1 crew who were the victims of MH370 tragedy. The act was committed by using the victims' debit cards at the ATM machine, transferring money using unauthorized internet access, stealing money via manual money transfer and submitting fake debit card application document as genuine. They were both charged under section 378, 417 and 471 of the Penal Code, and section 4(1)(a) of the Computer Crimes Act. They were convicted upon their plea of guilt. They filed an appeal to retract their plea but their appeal was dismissed by the High Court, and the High Court ordered for their sentence to be increased due to the gravity of their actions.

In *PP v Siti Latifah Mohd. Said [2016]*[8], a part-time computer application engineer was charged and convicted under Section 420 of the Penal Code for masquerading as Khalisya Najwa in social media and deceiving a 28-year-old doctor until the victim handed over RM75,750 between October 7 and November 3, 2014. The money was purportedly to cover for the cost of their "upcoming marriage".

In *PP v Mazrin Abd Aziz [2015]*[9], an unemployed was accused of cheating a teacher and his wife in relation to the sale of a house which was not his property at a price of RM280,000 at http://www.mudah.my in 2014.

In *PP v Peace Okotie [2009]*[10], a Nigerian Business Management student from a private college was was charged and convicted under Section 420 of the Penal Code for cheating a public administrative officer via email about a $ 1 million (RM3.6 million) winning prize in 2008. She was also accused of residing in Malaysia with expired student visa. She earlier informed the victim that she could manage the process of bringing in the Microsoft 2008 prize from the United Kingdom. The victim was deceived and transferred USD2750 (RM9969.85) to her account.

AIDING IN DEFRAUDING A PERSON

It would be risky for a scammer to direct his victim to transfer money directly to his own account. By doing so, he can easily be tracked down by the authority. That is why the scammer more than often will rely on a money mule to be his scapegoat. According to Jansen and Van Lenthe (2017), a money mule is "someone who offers his bank account on payment to criminals, who use the account to launder money."[11]

One of the ways of getting the mule to work for the scammer is by contacting the mule (usually after studying his profile on social media) and convey to him some good news about him being appointed as the agent of a fictious international company. The mule however needs to share the details about his bank accounts with the "company" since the company is not yet registered to operate in Malaysia. The scammer will advise the mule to open a bank account, and then some amount of money will appear in the new account, to which the scammer will tell the mule that the money is initial payment for the mule's role as the company's agent. Thinking that he will gain more benefits as an agent, the mule will surrender his bank card to the scammer for "validation". The scammer lends assurance to the mule that despite the fact that he does not have the card in his possession, he can still easily transfer any future amount received to his own other account which he already has prior to the opening of the new bank account.

However, what happens in the background of the above scenario is that the scammer will deceive another victim who will transfer money to the mule's account. Now, since the scammer has the mule's bank card in his possession, he can simply go to any ATM machine to withdraw the money. Even if the mule may notice that the amount is received and transfer it before the scammer is able to withdraw it, the scammer is never at loss, since the money has never been his own money. It is just a race of wits between the scammer and the mule, and the losing person is the victim.

Yet, if the victim realises that he has been cheated and files a report to the authority, who will the authority come after? The mule, of course, because the record of the transaction will reveal that the money was transferred to a bank account registered under his name. And the scammer will scout free.

What is then the position of the mule? Can the mule be legally regarded as aiding the scammer? What if the mule at all material time knows that whatever money that he receives is not legit, yet still allows his bank account to be used?

To answer the above questions, reference need to be made to section 411, 414 and 424 of the Penal Code. In relation to dishonest receipt of stolen property, section 414 states:

"Whoever dishonestly receives or retains any stolen property, knowing or having reason to believe the same to be stolen property, shall be punished with imprisonment for a term which may extend to five years or with fine or with both; and if the stolen property is a motor vehicle or any component part of a motor vehicle as defined in section 379A, shall be punished with imprisonment for a term of not less than six months and not more than five years, and shall also be liable to fine."

In relation to assistance in concealment of stolen property, section 414 states:

"Whoever voluntarily assists in concealing or disposing of or making away with property which he knows or has reason to believe to be stolen property, shall be punished with imprisonment for a term which may extend to seven years or with fine or with both; and if the stolen property is a motor vehicle or any component part of a motor vehicle as defined in section 379A, shall be punished with imprisonment for a term of not less than six months and not more than seven years, and shall also be liable to fine."

In relation to dishonest or fraudulent removal or concealment of consideration, section 424 states:

"Whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or claim to which he is entitled, shall be punished with imprisonment for a term which may extend to five years or with fine or with both."

The following cases on mules being charged and convicted are based on the types of scams engaged by the scammers.

LOVE / PARCEL SCAM

In *Sarimah binti Peri v Pendakwa Raya [2019]*[12], Sarimah was accused of receiving RM251,990 belonging to a scam victim in her CIMB account between 15 and 30 March 2016. The victim earlier befriended via Facebook a scammer who fraudulently represented himself as a director at Shell oil and gas company. The deposit payments were made to "assist" him in settling his debt so that he would be receive USD4.25 million after the expiry of his contract with Shell.

Sarimah was charged and convicted under section 424 Penal Code. However, she appealed against the decision, and Shah Alam High Court allowed her appeal on the ground that the magistrate had erred when she found that the prosecution had established a prima facie case.

In *PP v Tee Chiu Hang [2018]*[13], Tee, a tile shop worker was charged and convicted under section 411 of the Penal Code for receiving stolen money totalling RM148,490 from a scam victim into her bank account in multiple transactions between 21 April and 12 June 2017. Tee earlier befriended two Nigerian scammers on Facebook, and surrendered her ATM card to them.

The victim also befriended the scammers on Facebook. She was informed that they wanted to send her valuables, but she needed to pay a deposit to Tee's account to release the items.

In *PP v Gollneer Roshandin [2017]*[14], Gollneer was charged and convicted under section 411 of the Penal Code for receiving stolen money totalling RM37,800 belonging to a scam victim into her CIMB account in multiple transactions between 19 to 21 July 2017. The victim earlier befriended an Iranian scammer on Facebook. The scammer informed her that he wanted to give her a gift parcel containing a necklace, bracelet, ring and earring, plus a handbag and mobile phone, and a large sum of money in Iranian currency.

When she was later contacted by another scammer posing as a custom officer notifying her that she needed to pay a certain amount of money to collect the parcel, she immediately transferred the amount to Gollneer's bank account. However, she received no further news after the amount was paid.

In *PP v Charles Sugumar a/l M. Karunnanithi [2017]*[15], Charles, a tour driver, was accused of concealing RM36,300 belonging to a scam victim in his Maybank account in 3 occasions between 17 and 18 November 2015. The victim earlier befriended a scammer posing as a male from United Kingdom on Facebook. The scammer then informed the victim that he had received a job offer from Petronas in Kota Kinabalu and would bring his US$3 million cheque. Due to the large amount, he would not be able to convert it to cash without the victim's assistance. After receiving a phone call from another scammer posing as an officer from Standard Chartered Bank concerning the matter, the victim then transferred money to Charles's bank account so that the cheque could be cleared.

Charles was earlier requested by his customer (the scammer) to receive money on his behalf, since the customer's friend needed to transfer the money to him so that he could continue his tour in Malaysia.

Charles was charged under Section 424 Penal Code. However, he was discharged and acquitted since the prosecution failed to prove the case

beyond reasonable doubt. The prosecution appealed against the decision of the court, but Kota Bharu High Court dismissed the appeal of the prosecution and retained the decision of the Magistrate Court.

In *PP v Rose Suraya Ideris [2017]*[16], Rose, an unemployed was charged and convicted under section 424 of the Penal Code for concealing RM14,000 belonging to a scam victim in her bank account in multiple transactions on 8 September 2017. The victim earlier befriended a scammer who fraudulently represented himself as a male person from United Kingdom and promised to give her a parcel gift from his country.

When the victim received a phone call on 8 September 2016 notifying her that a parcel was to be delivered to her, she agreed to pay RM14,000 "government tax" in advance so that the parcel could be couriered to her address. The money was transferred to the "courier's account" (Rose's account) in four transactions. However, the courier company asked for another transfer of RM70,000.

In *PP v Minah Anak Nyangat [2017]*[17], Minah was charged and convicted under section 424 of the Penal Code for removing RM6500 belonging to a scam victim to her Maybank account on 14 November 2016. The victim earlier befriended a scammer who posed as an American by the name of Harding Scott on Facebook. The scammer told her that he would like to visit Malaysia and give her gifts and money. She later received a text message from him, informing her that she had to make some payment to Minah's bank account to release the gifts that he sent to her. However, after transferring RM6500 to the account, the gifts were still not delivered to her.

In *PP v Erick Andrew Mbwambo [2014]*[18], Erick, a Tanzanian student from a private college was charged and convicted under section 424 of the Penal Code for concealing RM12,500 belonging to a scam victim in his Public bank, Hong Leong Bank and Affin bank accounts in multiple transactions between 27 and 30 June 2014. The money was acquired through parcel scam. Erick was promised a reward of RM50 to RM100 for every transaction.

LOAN SCAM

In *PP v Lim Chau Ching [2019]*[19], Lim, a house builder was charged and convicted under section 411 of the Penal Code for receiving stolen money belonging to a scam victim totalling RM5640 into his CIMB bank account between 21 and 22 December 2018. The money was acquired after deceiving the victim about a housing loan. The victim earlier received a loan advertisement via a text message, and was asked to make a deposit payment.

In *PP v Karundendran Poopalan [2019]*[20], Karundendran was charged and convicted under section 424 of the Penal Code for removing RM3500 belonging to a scam victim to his bank account between 10 and 14 March 2017. The victim earlier received a WhatsApp message from a scammer posing as a moneylender. Attracted by the loan package, the victim was then instructed to contact another scammer for the loan application of RM20,000. He then made a deposit payment of RM3,500 to Karundendran's bank account for processing and legal fees. However, he did not receive further news about the matter, and his phone calls on the matter were also not picked up by the two scammers.

In *PP v R. Muniandy [2018]*[21], Muniandy, a factory worker was charged and convicted under section 424 of the Penal Code for removing RM5500 belonging to a scam victim to his CIMB bank account on 5 June 2017. Muniandy earlier surrendered his ATM card to a scammer for loan application, but the scammer later contacted the victim by posing as a moneylender. The victim was instructed to make insurance payments to secure the loan in multiple transactions to Muniandy's bank account.

In *PP v Nurliyana Mohd Sahari [2017]*[22], Nurliyana was charged and convicted under section 424 of the Penal Code for concealing RM1000 belonging to a scam victim in her bank account on 29 August 2017. The victim earlier deposited the amount to Nurliyana's bank account as GST payment after being instructed by a scammer to enable the victim to make a loan of RM25,000.

In *PP v Syed Ahmad Nashrul Sayed Othman [2017]*[23], Nashrul, a chauffeur was charged and convicted under section 424 of the Penal Code for concealing RM500 belonging to a scam victim in his Hong Leong bank account scam on 9 August 2017. The victim earlier agreed to make a personal loan of RM30,000 upon seeing a fraudulent advertisement by a scammer on Facebook. He then made a deposit payment of RM500 Nashrul's bank account as instructed to secure the loan.

FBI/POLICE SCAM

In *PP v Rafidah Che Mat Zain @ Zainuddin [2018]*[24], Rafidah, a bank officer was charged and convicted under section 424 of the Penal Code for removing RM22,500 belonging to a scam victim to her bank account in multiple transactions between June and July 2017. Rafidah earlier surrendered her ATM card and pin number to a Nigerian scammer who later contacted the victim by posing as an FBI agent. The scammer informed the victim that her nude photo was about to be circulated on social media. To prevent that from happening, the victim was instructed to deposit RM12,500 to Rafidah's bank account. However, after she deposited the amount in multiple transactions, she was instructed to deposit another RM10,000 to the same account.

In *PP v Muhamad Sahrizal Ismail [2018]*[25], Sahrizal, a broadband installation contractor was charged and convicted under section 424 of the Penal Code for concealing RM20,000 belonging to a scam victim in his CIMB bank account on 27 March 2017. The victim earlier received a phone call from a scammer posing as an officer from Affin Bank, notifying him that a new bank account was recently opened using his name in Penang. The "officer" also informed the victim that RM12,000 had been transferred from the account to another account owned by one "Lim Seng Siang" who was a dangerous drugs dealer and money launderer.

The victim then transferred RM20,000 to another bank account allegedly owned by an "auditor" in Putrajaya (Sahrizal's account) after receiving another phone call from a person posing as a police officer, warning him that the amount was needed for police investigation.

In *PP v Tay Siao Leng [2017]*[26], Tay, an unemployed was charged and convicted under section 424 of the Penal Code for concealing RM15,000 belonging to a scam victim in his bank account on 19 August 2016. The victim earlier received a phone call from a scammer posing as a police Inspector who notified him that his son was detained with three other individuals for drug trafficking, punishable with death if convicted. He was instructed to make a payment of RM100,000 to release his son from police custody. The scammer agreed to reduce the amount to RM50,000 after being informed about the victim's financial constraints.

However, after depositing RM15,000 to Tay's bank account and the remaining RM10,000 and RM25,000 to other bank accounts under the name of other individuals, he discovered that his son had never been detained by the police.

CREDIT CARD USAGE ALERT SCAM

In *PP v Muhammad Lukmanhakiem Soekanto Pura [2019]*[27], Lukmanhakiem was was charged and convicted under section 424 of the Penal Code for concealing RM4000 belonging to a scam victim in his bank account in May 2018. The victim earlier received a phone call from a scammer who informed him that his credit card was used in Genting Highlands and had total arrears of RM8,513.23. The scammer offered to assist the victim to update his personal information with the authorities, but the victim had to transfer all his money into Lukmanhakiem's bank account first. Although the victim was told the money would be refunded once the personal information had been updated, yet he heard no further news after the transfer.

In *PP v Mohd Nadzrin Zaidel [2018]*[28], Nadzrin, an unemployed was charged and convicted under section 424 of the Penal Code for concealing RM10,479.48 belonging to a scam victim in his Maybank account in multiple transactions on 17 January 2017. The victim earlier received a text message from Nadzrin who warned him that his credit card had been used at Kuala Lumpur International Airport and Genting Highlands. The victim was advised to call the Central Bank using the phone number given in the message. When he made the call, another scammer posing as an officer from the Central Bank informed him that his personal information had been misused, unless he transferred his money to Nadzrin's bank account. However, after transferring RM10,479.48 to the account, the victim realised that he had been cheated.

In *PP v Lai Fook Fatt [2017]*[29], Lai, a company production manager was charged and convicted under section 424 of the Penal Code for illegally assisting in transferring RM49,000 belonging to another company manager to his own account on 14 December 2016. The victim earlier received a phone call from Lai who accused him of using Lai's credit card in a premise in the Kuala Lumpur International Airport. The victim then transferred the above amount to Lai's bank account after

receiving another phone call from a scammer posing as an officer from the Central Bank, warning him regarding the matter.

ONLINE SALE SCAM

In *PP v Ng Chee Wei [2019]*[30], Ng, a Grab driver was charged and convicted under section 424 of the Penal Code for concealing RM9000 belonging to a scam victim in his Maybank account via online transfer of RM900 and cash deposit of RM8100 in May 2019. The amount was transferred by the victim to Ng's bank account for the initial payment of a non-existent car fraudulently advertised by two scammers on http://www.mudah.my. Ng was paid RM700 by the scammers.

In *PP v Nur Nirmal Manoj Kumar [2018]*[31], Nirmal, a housewife was charged and convicted under section 424 of the Penal Code for concealing RM900 belonging to a scam victim in her Bank Simpanan Nasional account on 20 March 2016. The victim earlier agreed to purchase an iPhone 6 Plus which was advertised online for the price of RM1800. She was then instructed by Nirmal to make a deposit payment of RM900, and the balance to be paid after the delivery of the phone to her address. However, she later received a message asking for the balance payment to be paid before delivery, yet she was notified that she could cancel the purchase and her deposit money would be refunded. Although she decided to cancel the purchase, the deposit money was still not returned to her.

In *PP v Shaarani Mohd Abas [2018]*[32], Shaarani, a retired assistant nurse was charged and convicted under section 411 of the Penal Code for receiving stolen money totalling RM3500 from a scam victim into her bank account in multiple transactions between 2 and 4 September 2018. Shaarani earlier befriended a scammer on Facebook, and surrendered her ATM card to him.

The victim was earlier contacted by the two Nigerian scammers (one of them was the one befriended by Shaarani) who informed her that they wanted to purchase her motorcycle which was advertised online.

In *PP v Jamalulhisham Jusoh [2017]*[33], Jamalulhisham, a security guard was charged and convicted under section 424 of the Penal Code for removing RM1300 belonging to a scam victim to his bank account on 16 May 2014. The victim earlier transferred the above amount to Jamalulhisham's account for the purchase of iPhone 5s fraudulently advertised on http://www.mudah.my.

In *PP v Khairunnisa Ab Rahim [2017]*[34]. Khairunnisa, a housewife was charged and convicted under section 424 of the Penal Code for concealing RM1700 belonging to a scam victim in her CIMB bank account in multiple transactions on 21 and 23 March 2017. The victim earlier agreed to purchase a baby stroller fraudulently advertised online by a scammer. However, the stroller was not delivered to her after she made the purchase payment as instructed to Khairunnisa's bank account.

In *PP v Jazrina Jaapar [2016]*[35], Jazrina, a freelance clerk was charged and convicted under section 424 of the Penal Code for concealing RM4150 belonging to a scam victim in her CIMB bank account in multiple transactions between 25 June and 11 July 2012. The victim earlier agreed to purchase a Nikon camera advertised on http://www.mudah.my for RM4150, but after the amount was paid by installment to Jazrina's account in six transactions, the camera was still not delivered to him.

CONCLUSION

It is clear from the above discussion that online scam is a twisted scheme designed to manipulate the weak traits in a person. And the way the scammers manipulate both the mules and the victims reveal that this problem will continue to subsist since it depends heavily on one's own conscience. It is indeed quite difficult for legislation to be put forward to control a person's monetary and emotional needs, as this is human nature which goes beyond the legal provisions.

Too much control on people, though done for the betterment of the society is always equated with dictatorship and violation of privacy. However, one has to understand that it is not possible for security and privacy to co-exist in their 100 percent form. Full security can only be reached at the expense of privacy, and vice versa. This notion however is not a preferred option in Malaysia as it would cause the government its popularity. It needs a very strong political will if this strict measure is to be imposed. Thus the cliché recommendation for solution which is mostly focused on awareness campaigns and education is the only viable mechanism at the moment.

NOTES

1 Reported Incidents based on General Incident Classification Statistics. http://www.mycert.org.my/
2 Committee on Governmental Affairs, Cyber Attack: Is the Government Safe? : Hearing Before the Committee on Governmental Affairs United States Senate One Hundred Sixth Congress, 2nd Session, 2000, p8-9, 47.
3 Rizal Rahman, Malware and The Law of Deception in Malaysia, 2018, 3 MLJ lxxxvi, p 12.
4 Sessions Court, Kuala Lumpur (1990).
5 Magistrate Court, Gua Musang (02/02/2017).
6 MLJU 1212.
7 6 CLJ 422.
8 Magistrate Court, Ayer Keroh (20/09/2016).
9 Sessions Court, Kuala Lumpur
10 Magistrate Court, Kuala Lumpur (24/03/2009).
11 Floor Jansen and Jarmo Van Lenthe, "Adaptation Strategies of Cybercriminals to Interventions From Public and Private Sectors" in Thomas J. Holt (ed.), Cybercrime Through an Interdisciplinary Lens, 2017, Routledge, 210 at 219.
12 MLJU 230.
13 Magistrate Court, Kuantan (09/11/2018).
14 Magistrate Court, Sungai Petani (26/12/2017).
15 High Court, Kota Bharu (07/09/2017).
16 Magistrate Court, Kuala Lumpur (25/10/2017).
17 Sessions Court, Kuala Lumpur (25/07/2017).
18 Magistrate Court, Kuala Lumpur (21/07/2014).
19 Magistrate Court, Kuala Terengganu (18/02/2019).,
20 Magistrate Court, Sibu (19/06/2019).
21 Sessions Court, Kuala Lumpur (28/02/2018).
22 Magistrate Court, Seremban (15/09/2017).
23 Magistrate Court, Seremban (15/08/2017).
24 Magistrate Court, Kuala Lumpur (14/02/2018).
25 Magistrate Court, Ayer Keroh (14/03/2018).
26 Magistrate Court, Miri (04/03/2017).
27 Magistrate Court, Sibu (10/01/2019).
28 Magistrate Court, Sibu (06/10/2018).
29 Magistrate Court, Petaling Jaya (22/02/2017).
30 Magistrate Court, Shah Alam (06/08/2019).
31 Magistrate Court, Seremban (05/02/2018).
32 Magistrate Court, Kuantan (09/11/2018).
33 Magistrate Court, Kuala Lumpur (24/06/2017).
34 Magistrate Court, Petaling Jaya (10/08/2017).
35 Magistrate Court, Ampang (29/11/2016).

REFERENCES

Reported Incidents based on General Incident Classification Statistics. http://www.mycert.org.my/

Committee on Governmental Affairs, 2000. Cyber Attack: Is the Government Safe? : Hearing Before the Committee on Governmental Affairs United States Senate One Hundred Sixth Congress, 2nd Session, p8-9, 47.

Rizal Rahman. 2018. Malware and The Law of Deception in Malaysia, 3 MLJ lxxxvi, p 12.

Jensen, F. and Van Lenthe, J. 2017. Adaptation strategies of cybercriminals to interventions from public and private sectors. In Cybercrime Through an Interdisciplinary Lens, edited by Thomas J. Holt. Routledge.

Mohamad Rizal Abd Rahman
Faculty of Law
Universiti Kebangsaan Malaysia
43600 Bangi, Selangor
Email: noryn@ukm.edu.my