Dean&Francis
ISSN 2959-6149

The Scenes Behind the Global 'Pig Butchering' Scheme in Myanmar

Tongyang Li

Camford Royal School Guoxian BIC Department,Beijing,100000,China;

Abstract:

This paper looks into how Southeast Asia, particularly Myanmar, has taken the lead as the centre of the international "pig-killing pan" fraud. Advanced technologies for Internet communication are the basis of this scam, which tricks victims into investing in phoney schemes that lead to painful financial losses. The article reviews the ways in which Myanmar's unstable political circumstances and the complexity of the borderlands create a prime atmosphere for telecom fraud. The article covers the danger to global cybersecurity along with personal property, financial security and the significant psychological and economic consequences for victims. Finally, the paper presents cooperative strategies at the international level to fight against telecom fraud, which includes increasing levels of intelligence sharing, legal cooperation, and educating the public.

Keywords: Pig-killing pan; Myanmar; Network security;Psychological influence; International cooperation

1. Introduction

South East Asia, which has different vivid cultures and famous scenic spots, has always attracted many tourists worldwide. Because of its special geographical location and complex cultural background, northern Myanmar has left an indelible mark on the world map of the drug trade. The drug trade in this region is not just a struggle for financial gain. Behind the scenes are geopolitical struggles, livelihood issues for ethnic minorities, and even power and military strife. However, it has recently become renowned for many fake online businesses, mostly affecting the middle class and normal families from developed Western countries. This fraud has since been spread by enhanced internet communication technologies like 5G, making them more complex and difficult to recognize. The region's history as a center for drug production and trafficking has morphed into a new form of criminal activity: telecom fraud. Myanmar, especially, has become one of the favorite destinations for a certain kind of fraud that is prominent as the 'pig butchering' scheme. The term "piggy bank" originally describes a form of money scam, but in northern Myanmar, it takes on a deeper colour, hinting at more sin and intrigue behind the scenes. This kind of scam takes advantage of the human heart and makes ordinary people who believe in the human heart fall into the trap. When the victims realize the truth and want to escape, a more brutal "prison" awaits them. In this prison, people almost lose the most basic dignity of life, and the continuous physical and mental destruction makes every second feel like an eternity. This phase, which seems strange to the Western ear, means a technique con artists use to

ISSN 2959-6149

encourage people to put their money into their scams and then 'kill' their investments.

It is, however, important to understand that it is not only Asia that the 'pig butchering ' scheme targets as it has now gone global with Western countries such as the United States, United Kingdom, Australia, and others included in their list. The people who perpetrate these scams sit in offline centers across the country, so it's tough to arrest them. It seriously threatens international cyber-security and the individual's belongings and money worldwide.

2. Current situation of telecom fraud in Myanmar

Relations in Myanmar's political process have been rather conflictive and imperfect, where different parties fought for power. These have resulted in several local militant groups forming, especially in the China-Myanmar and Thailand-Myanmar border areas. The new Gambling Law implemented in Myanmar in 2019, which allows foreigners to register and operate casinos in the country, has further accelerated the growth of the telecom fraud industry in the northern part of the country, which alone generates billions of dollars in fraud proceeds every year. Districts like the Kokang Self-Administered Zone in Shan State in northern Myanmar, which used to be famous for drug syndication, are infamous today for telecom fraud. There is concern about no coherent strategy for addressing this emerging type of telecom scam. People from developed and developing countries must work together to solve the problem. Citizens, authorities, police, and specialists in the field of IT should exchange information, experience, and examples of scams that are considered. The case of Myanmar presents the general picture of most Southeast Asian countries. The limited ability of the Myanmar government to control the northern region, coupled with porous borders, has allowed fraudsters to escape with ease. Due to the region's political instability and favorable geographical location, the area can be used as a ground for criminal activities. They are allowed to practice such activities due to the open borders and the presence of numerous militant organizations.

Currently, there is a high incidence of telecommunication fraud in northern Myanmar, with a large number of victims. Fraudsters use various means, such as impersonating government agencies and fake websites, to lure victims. Many cases involve huge financial losses, causing great distress to the victims.

3. The means of the pig-killing pan and its negative influence

In recent years, the landscape of fraud has evolved dramatically. Traditional credit card schemes have given way to more sophisticated operations that demand significant time, effort, and energy. Cryptocurrencies and other advanced manipulation techniques characterize this new wave of fraud. The allure of 'easy money' draws many into this illicit activity, often promising more income than legitimate jobs. However, the reality is far from the promised fortune. Those who fall for the trap of working abroad in scam operations face not only the deprivation of freedom but also a high risk of physical abuse.

The term› ruthless demons› has been used on Chinese social media to describe those who operate scamming activities. They are accused of being so heartless that they would ‹cut out the kidneys› of those who fall into the trap of a promised white-collar job. The physical abuse inflicted on those who fail to meet the ‹key performance indicators› set by the scam camps is severe. It includes electric baton beatings, organ selling, coerced prostitution, and other forms of outrageous abuse. In extreme cases, this physical abuse can lead to permanent maiming.

The conditions in these scam hubs have been likened to a new form of "concentration camp" by many. The psychological impact on both those who were initially abducted and those who came to work there voluntarily is profound. They are left with deep psychological scars from severe stress and traumas, even after being rescued by the Chinese police.

China has been a critical target for telecom fraud, with overseas Chinese residents and Westerners also falling victim to their schemes. The Asia Pacific region, particularly Australia, has been significantly affected by 'pig-butchering' scams, a term used to describe a type of fraud where victims are lured and then exploited for all their worth. The scams have also inflicted heavy losses on U.S., U.K., and European residents, running into billions.

There are many different scamming methods, and companies like the ones that claim to be public prosecutors and lawyers are the least capable and competent. A slightly more advanced company's scamming method is called fine chat, also known as spiritual chat, and there are many roles for people to play. For example, they play the military, are rich and handsome, etc., in the name of single dating, specializing in looking for women between the ages of 30 and 50 to "talk about love". When the relationship with the woman began to develop after the establishment of feelings, it began to lure her to invest. When she invests, the early stage will release water, let her withdraw cash to the account, and get part of the profit. But when she increases investment, the money will not come out.

Chinese individuals residing abroad, who often face cultural and language barriers, are particularly vulnerable to falling into the trap of scammers. Scammers exploit this vulnerability by presenting themselves as caring individuals with similar backgrounds, gradually gaining their trust before revealing their true intentions.

Before a series of actions, scammers present exquisitely designed profiles of social elites with good-looking appearances. Subsequently, they act like "herders" responsible for contacting many users, "pigs" in this context, wishing to get a reply from potential victims. The criminal's first step is to contact the potential victims by sending messages to groups of receivers via SMS or dating applications, claiming the receivers to be their "destiny." In other common cases, scammers claim to be experts in the finance sector who have information on certain investment portfolios that can guarantee good returns on investment. The second step is to 'raise' that target by winning trust. After a certain degree of familiarity has been built, the victims are recommended to another platform where cryptocurrency fraud occurs. The final step is to "kill the pigs" and finally to cash out.

Scammers often use elaborate social media accounts that look like successful people with attractive looks and lifestyles. They connect with potential victims via social media, dating sites, or text messages, claiming they are the "one." Fraudsters often use cryptocurrencies to conduct transactions because their anonymous and transnational nature makes it very difficult to trace and recover funds. In addition, they used social media platforms for phishing to attract victims by creating fake profiles and stories. Scammers could also use innovative social engineering methods, including emotional and psychological control, to govern the victim's behavior. Following establishing a connection, the scammer will work to nurture trust through extended chats to make the victim think they are a close friend or romantic partner. In Myanmar, more than 100,000 people gather every day in thousands of fraudulent parks to commit telecommunication fraud, and they are brutalized, beaten, kidnapped, trafficked, buried alive and even have their organs removed if they do not comply. There are some cases below:

Case One: Mr Zhang, a Chinese man residing in Australia, encountered a woman posing as a financial analyst on an online dating site. The woman reported knowing insider information on investments that could produce substantial returns. Zhang decided to invest due to her words. Later, he discovered that his investment account stood empty, with hundreds of thousands of Australian dollars lost.

Case Two: Ms Lee, a citizen of China now in the U.K., received an email that indicated she had won an extraordinary reward. Without question, she followed the email's instructions and gave her bank account information. Soon after, she found out her account was drained, and she had lost tens of thousands of pounds.

According to victim psychoanalysis, victims are usually naive because of their loneliness, their desperate need for love, or a shaky financial situation. Fraudsters exploit these psychological inadequacies and gradually develop trust with their victim through imitation sympathy and help. If the victim has total faith in the scammer, they will be directed to invest or put money somewhere, which always leads to losing their property. Besides, the victims are usually defenseless because they dream of wealth, their ambitions for success, and their need for connections. Scammers commonly exploit these psychological shortcomings to encourage victims by forming relationships of trust, presenting fictitious investment chances, or supplying emotional support. During the fraud process, those affected may change psychologically from experiences of excitement and confidence to apprehension, fear, and gloom.

The 'pig butchering' scheme and other forms of telecom fraud are not just financial crimes; they are crimes that erode trust in digital platforms and can have severe psychological impacts on victims. For the victims of telecom fraud, it is very important to provide timely psychological counseling and legal aid. It can help victims recover from scams and allow them to recover their losses.

The economic implications of telecom fraud are also significant. The money lost to scams could have been used for investment, development, and social welfare programs. It is a drain on the economy and a hindrance to progress. Furthermore, the reputational damage caused by these scams can deter foreign investment and tourism, further impacting the region's economic growth.

4. Strategies for dealing with telecom fraud

Local law enforcement in Myanmar and neighboring countries, particularly China, face significant obstacles due to telecom scams' complex nature. As Beijing issued warrants to arrest the 'mafias' running the scam hubs in north Myanmar in November 2023, the attempt to address the complexities of cross-border telecom fraud has witnessed impressive effectiveness. However, despite the great efforts made by the Chinese government to tackle telecom fraud, other Southeast Asian countries, including Cambodia and Thailand, remain passive in addressing telecom fraud. Political conflicts in border areas where a high degree of regional autonomy is applied hinder further legal collaboration among countries. Beyond the Asian context, efforts have been made in Australia, with the Australian Federal Police reminding singles to beware of organized criminals and police releasing details of a pig-slaughtering operation manual to inform the community of the tactics used by criminals. China and the U.S. collaborate to solve the fraud crisis. Jan Santiago from the U.S. has extensively researched fraudulent activity in China through cryptocurrencies and Bitcoin in a concerted effort to solve the global scam crisis. In 2024, the Technology Anti-Fraud Coalition was formed, a coalition that will take action to combat fraudulent tools used by

ISSN 2959-6149

criminals and disrupt financial fraud, educate and protect consumers. They will keep users safe and prevent them from becoming victims of online fraud.

With the development of technology, the means of telecom fraud are constantly changing. With the continuous development of Internet technology, the means of telecommunication fraud will also become more complex and hidden. In the future, there may be more fraud methods based on artificial intelligence and machine learning, which will pose new challenges to the fight against fraud. We should keep pace with The Times and be ready for any contingency. Therefore, the government, enterprises, and individuals must collaborate to raise awareness of preventing telecom fraud. At the same time, the government should intensify the fight against telecom fraud crimes and improve relevant laws and regulations to curb the spread of telecom fraud.

Telecom fraud laws and policies differ from one nation to another. Several countries have responded to fight telecom fraud by implementing legislation enforcing strong penalties on perpetrators and protecting victims. On the other hand, because of the international scope of telecom fraud, the distinctions in law and a lack of intercountry cooperation render the struggle against fraud activities more challenging. It might include forming task forces meant to follow and arrest cybercriminals and fashioning international laws that encourage teamwork amongst countries in pursuing these offenses.

In addition, strengthening international cooperation is also the key to preventing and combating telecom fraud in the future. By establishing close ties with global law enforcement agencies and sharing information and experience, the problem of transnational telecommunication fraud can be tackled jointly. International collaborative efforts must be strengthened to fight against telecom fraud. It encompasses undertakings consisting of collaboration in intelligence, harmonizing law enforcement protocols, and creating an integrated legal structure, amongst other things. As a case in point, in the effort against telecom fraud, the U.S. and China have already worked in concert, looking into how fraudsters operate and following the movement of illicit funds.

Overcoming fraud requires that we implement education and awareness campaigns. People must learn the techniques of scammers and the strategies to keep themselves safe. Those who take the initiative, are attentive to strangers, and safeguard their data can prevent telecom fraud. Through educational campaigns and publicity, communities can develop greater awareness of fraud prevention. In the fight against telecom fraud, the government can act by improving its legal framework, enhancing the efficiency of law enforcement, furnishing technical support, and more.

5. Conclusion

In short, fraud hubs based in Southeast Asia, principally in Myanmar, Laos, and the border with China, have been quite harsh in their management of trafficked or induced persons and have engaged victims from across the globe, causing serious economic and property damage as well as cybersecurity and human rights challenges. Even though regional governance efforts have occurred, full cooperation is still lacking, and currently, there is no assurance that telecom fraud will disappear since it could come back. Hence, this neglected area in the world spectrum still needs our focus. We need to work together and make efforts globally to solve this problem. Around the world, telecom fraud represents a dilemma that affects governments, international organizations, and people. Elevating public recognition, fortifying legal consequences, and creating strong global cooperation systems help us better combat telecommunications fraud and strengthen the defense of citizens' assets.

References

[1]"The Rise of Cybercrime in Southeast Asia: A Focus on Myanmar." Journal of Cybersecurity, vol. 5, no. 3, 2023.

[2]"Telecom Fraud: Global Challenges and Responses." International Journal of Law and Information Technology, vol. 27, no. 2, 2023.

[3]"The Psychological Impact of Cyber Scams on Victims." Cyberpsychology, Behavior, and Social Networking, vol. 24, no. 7, 2023.

[4]"Combating Transnational Cybercrime: Legal and Policy Perspectives." Journal of International Criminal Justice, vol. 17, no. 1, 2023.

[5]"The Economic Cost of Cyber Fraud: A Global Analysis." Economic Inquiry, vol. 58, no. 3, 2023.