global china pulse.

01 24

SCAMMED: DISSECTING CYBER SLAVERY IN SOUTH EAST ASIA

This text is taken from *Global China Pulse*: Volume 3, Issue 1, 2024.

A Prosecutor in Taiwan

Harris Chen is a prosecutor with 17 years of experience at the Chiayi District Prosecutor's Office in Taiwan.

Prosecuting Cybercrime in Taiwan: A Conversation with Harris Chen

Yanyu CHEN,
Harris CHEN

Harris Chen is a prosecutor with 17 years of experience at the Chiayi District Prosecutor's Office in Taiwan. While specialising in fraud cases, Harris is also active in fields as diverse as human trafficking, corruption, drugs, and environmental crimes. Most recently, he has been focusing on cybercrime, with a particular interest in the new role of artificial intelligence (AI) in this sector. He also assists the High Prosecutor's Office, which has a cybercrime unit, and is a member of several organisations such as the Institute for Cyber Security, the Association of Digital Forensics, and the Artificial Intelligence Legal Research Foundation. We sat down with him to discuss the challenges he faces in prosecuting online scam cases in Taiwan.

Chen Yanyu: Taiwan played a special role in the rise of the online scam industry, with most accounts tracing the origins of the current boom in cybercrime to operations that began there in the mid-1990s. Do you think that still applies today and, if so, why is that the case?

Harris Chen: Taiwan is still very important for the online scam industry. The reason for Taiwan's current 'success' in this sector has a lot to do with our geographic location, foreign affairs, and technology. As you know, the places where criminal organisations today are conducting large-scale, sophisticated cyber-fraud are probably Taiwan, Mainland China, and Southeast Asia. Of course, there are many other countries, in Eastern Europe, such as Romania, Ukraine, Poland, and Bulgaria, where cyber-fraud operations are widespread. Russia is also a base, and India is now a big player. However, operations in Taiwan, China, and Southeast Asia work closely together and have combined in a way that allows them to dominate the industry.

There are several reasons for this. First, there is the issue of money flow. I don't think Taiwan is doing enough to combat money-laundering. The situation has become even more challenging because of the use of cryptocurrencies. To stop money-laundering, we need transnational cooperation, but due to Taiwan's complicated foreign relations, becoming a member of Interpol is a goal yet to be achieved. For example, diplomatically, Cambodia has been quite hostile to us, which makes this country a haven for Taiwanese criminals. Second, Taiwan has a very strong technology industry, which means there is a lot of IT talent who can be used to set up websites or money-laundering platforms

well and fast. Another thing is that our foreign exchange control is a little bit looser than in many countries in the region, including China and Southeast Asia, and the level of economic freedom here is higher, which means that we may not be able to regulate economic activities so strictly, even when it comes to fighting crime. Also, Chinese and Taiwanese people share common traits—we like to save money, to invest, to make money—and these characteristics make us a good target for fraudsters. The wealth accumulated in the Chinese and Taiwanese communities is quite large, so it has become a very coveted target for fraudsters. If you know the Chinese language, that will allow you to reach a very large market.

CY: Are there many prosecutors in Taiwan working on online scams today?

HC: Many of us have been focusing on that. We have been doing many seminars and there's been a lot of training on cryptocurrency and how to track these money flows. We have been doing presentations on cybercrime and information-sharing. But we have also encountered a major difficulty. People think that prosecutors are powerful, but, especially for cybercrime, we are extremely weak and not always efficient in obtaining information. For example, if we know of a person suspected of committing a crime, we can find them through the police or the relevant judicial authorities and try to stop them from running away—that's what criminal proceedings give us the power to do. However, we have no weapons when it comes to getting information on cybercrime. Due to the nature of this type of crime, most of the information is located in foreign countries. We prosecutors are very powerless; we need a lot of cooperation with other administrative organs to gather information, to cut access to the internet, and to cut off the flow of money.

I will take a typical case of cyber-fraud as an example to explain the difficulties we face. In a case that involves bank accounts, we would first ask the bank to provide us with the details of the transactions and the account information, which is usually made available to us. However, this process might not be very convenient or fast due to the issues in our financial sector that I mentioned above. Alternatively, we could use AI analysis to flag suspects. In this case, what is also challenging for us is how to identify IP [internet protocol] addresses that could reveal the location of the criminals. We need a warrant to get this information from internet service providers. One case can involve so many accounts: gaming accounts, Facebook accounts, Line accounts, etcetera. This is slow and, more importantly, we can only retrieve some information about the account, not its content.

Considering these challenges, prevention is key in this sector.

CY: Can you share a bit about the online scam cases you have handled? What are the common patterns in Taiwan?

HC: Taiwanese people like to borrow money from their acquaintances; it is quite normal here. For this reason, many online scams in Taiwan happen with people posing as relatives or friends. We see so often scammers posing as nephews or nieces and asking aunties for money. Scam operators really know how to manipulate. If the aunty says she can only give 50,000 TWD now, a normal person's first thought would be that this amount is good enough or to say that there is no urgency and ask again later when there is more. But the scammers are skilled manipulators.
They will insult her, blaming her for not helping the younger generation of her family. They will say something like: 'If you don't give me money, you are pushing me to borrow from an underground bank and, if something happens to me, you will have to look for me in hospital or jail.' They will first make her feel guilty, then say: 'Sorry Aunty, I should not talk to you like that, I am in trouble and really out of means. But I understand your difficulty, I will resort to private lending.' It is a very Asian thing; it is about making the aunt lose face and pushing her to offer money.

CY: What penalties do scammers such as these face in Taiwan?

HC: Taiwan's sentencing has always been lenient. There are several reasons for that. The first is that Taiwanese judges are afraid of appeals. This is because once an appeal is filed, their work is going to be examined and criticised, not to mention the fact that, if the case is dismissed and sent back, it will have an impact on their performance assessment. If the sentence is light, the chance of an appeal by the prosecutor is much lower than if there is a not-guilty verdict; as for the defendant, they will appeal only when the sentence is too heavy. So, the judge often prefers lighter punishments to avoid trouble, and sometimes we have seen judges go so far as to give the criminal a suspended sentence.

Then comes the issue of determining the penalty. Most internet fraud cases are treated as aggravated fraud, which carries prison sentences ranging from one to seven years. In other countries, sentences start from an average of four years and are reduced or years added according to the seriousness of the crime or whether the perpetrator shows a good attitude—for instance, by paying back the money or being cooperative. This is not how it works in Taiwan. The most common practice is to give a sentence of one year or slightly more. The criteria for imposing penalties are too vague, and judges in Taiwan always start from the lowest level. This is very different from, say, the UK system, where

sentencing usually starts from the middle of the range and they have clear guidelines about the standards and procedures for reducing it. For instance, the earlier you plead guilty, the shorter is the sentence. This is not the case in Taiwan: even if you plead guilty at the last minute, you still receive a light sentence. And no Taiwanese judge has ever explained why they decided to apply the minimum sentence.

This mindset also exists in the execution of the sentence. Let's say a person is convicted of four counts of online fraud. Normally, one count of online fraud receives a prison term of about 18 months, so you would think that the sentence given here will be a total of 7.2 years. But in Taiwan, no judge will ever give a sentence of more than six years, with most sentences about two years. It almost looks like the more offences you commit, the more discounts you receive: 60 per cent off your sentence for your second criminal case and 40 per cent for the third.

In addition, many judges in Taiwan may introduce religious thinking into their judgements. Many are afraid of making mistakes, locking up the wrong person or punishing them too heavily. The possible impact on their 'karma' has formed many judges' mindset, but they dare not speak of it. Again, to avoid trouble, they prefer lighter sentences or at least follow the 'market'. If most cases are sentenced to one year, they follow the general trend.

That being said, the Taiwan Judicial Yuan recently held seminars on sentencing in online fraud cases. On that occasion, they stated that they intend to put forward amendments to criminal laws to target certain situations, including imposing heavier penalties on criminals who resort to kidnapping or repeat offenders.

CY: What are the mechanisms to recover money and compensate victims in cases of cyber scamming? What are the challenges?

HC: In addition to the issues related to lenient sentencing, this aspect also remains quite problematic in Taiwan. In a typical case, after the court has ruled on the criminal aspects of the scam, there is usually a supplementary civil action in which the victim can claim damages in a civil court. This is the most common approach we see. The second way is to attempt a mediation independent of a criminal procedure. This gives both parties a chance to talk to see whether there is a way for the scam victim to receive proper compensation. Still, it is most common in Taiwan to start with the criminal process, which I don't think is a good strategy since most victims first want their money back and sometimes don't even care too much about putting the criminal in jail.

Alternatively, the government could deal with these cases as though they were consumer disputes—cases where a product is not of the promised quality, the place of origin is inaccurate, etcetera. Many victims are cognisant of the fact that they are consumers, as most scams start with an investment or with the acts of buying and selling. We can make cases like these a consumer protection dispute and the government can

coordinate with the consumer protection authority, instead of going to the judiciary. In that case, the most important thing is to make sure that the defendant has money that can be used to pay back the scam victim, and during the investigation we can seize their property to make sure the money is there. So, my suggestion is for the government to establish an intermediary organisation like the Consumer Protection Bureau.

If you're being defrauded of a million dollars and we are certain that is what happened, how do we proceed? How do we ensure that the sum is returned? This may be a problem that countries all over the world will face. The money restitution component should be independent of the judiciary; it can be dealt with at an early stage, while prosecutors work to arrest the criminals. Let's say that we arrest 10 defendants working as a syndicate. This new bureau can ask the syndicate to return the money before the trial. If they do not, this will be considered as one indicator in their sentencing. This third-party organisation should also have the authority to access information and even issue orders to seize assets. After confirming the facts of the victimisation, this agency can then coordinate the request for compensation without having to wait for the outcome of criminal proceedings, which is generally very time-consuming.

CY: Personally, what do you feel are the main challenges you face when prosecuting online scam cases?

HC: Cryptocurrency and all the money-laundering activities it enables. China did the right thing in prohibiting the trading of cryptocurrencies, unlike Taiwan, where it is still permitted. This means that cryptocurrencies in Taiwan can be used as money but are not regulated as such, which makes them perfect for money-laundering. If you're using cash to trade in US dollars, the banks will keep a record, but this does not always apply to Tether and other cryptocurrencies. On top of that, the transfer or exchange of cryptocurrencies can be so fast, it just takes a click on your smartphone. Now, fraudsters just need a mobile phone to commit a scam, transfer the proceeds, and launder them. With applications like Telegram, they can do all these steps and erase their tracks in one second. Another challenge is the spread of third-party payment applications. For example, Apple Points or game points can be used as a method of money-laundering and, if police need the information, it is in the hands of other countries or big foreign corporations. You just cannot gain access to it efficiently.

CY: I believe Taiwan has done something about blocking the flow of funds in the past few years. From the Cambodian side, it looks like there are some money-laundering groups that have abandoned the Taiwan market. Is that the case?

HC: As a result of the efforts of our prosecutors and the police, as well as the pressure exerted by other departments, we managed to block some cash withdrawals. But you can see very clearly that we can't do much about the financial part of the problem. Why?

Because it's all regulated by the financial institutions, and the regulation of financial institutions involves the banks and the so-called Financial Supervisory Commission. In the past few years, we have been pushing them to do something bigger, but it has not been easy.

Let me give you a simple example. If a foreign bank card is frequently used to withdraw money from a 7-Eleven in Taiwan, the bank should know about it beforehand and you could take some preventative measures, such as stopping or slowing the transaction. That's something that could be done quite easily. So, why don't they do it? It is because of the costs they would incur and the fees they lose. That's a big problem and that's part of the reason we don't touch this aspect as much as we would like to. A bank charges 5 TWD to 10 TWD per transfer, sometimes even 15 TWD or more. That is a small sum for scam companies, but if you consider the huge number of transactions these operations make, it can become a lot of money for the bank. That means that the fraudsters are contributing a lot of money to our financial institutions in fees and charges.

The state should think about how we can encourage banking institutions to recognise this as an issue of compliance. Take, for instance, what happened at CTBC Bank, which is an exaggerated example of the problems in our financial institutions. In more than one branch in Taiwan, the bank had moles who helped fraud groups open accounts, covered up for them, and helped them to launder money. That's a very serious crime and if this had happened in the United States, the bank would probably have been shut down. Just consider that a branch of the Mega International Commercial Bank in Panama was fined more than 5 billion TWD [roughly 180 million USD] by the United States because it didn't fulfill its reporting obligations. CTBC Bank committed so many crimes, but so far it has been fined only 20 million TWD by the Financial Supervisory Commission. My idea is that our government should slowly correct this. The state should say which banks are doing well and reward them, while penalising the others, letting the public know whom they are dealing with to ensure that the industry gets better.

Technology can also help. It's not that difficult to use AI to track the flow of money, but here again it's just a matter of whether the banks want to handle it or not, and whether they want to share the information. Many countries, including Taiwan, urgently need to adopt rules to ensure that banks promptly share financial information when required by law enforcement. We must be able to act quickly because the flow of money is global and instantaneous, and we must keep up.

CY: Just one final question. At the beginning of our conversation, you mentioned that Taiwan's foreign affairs are a significant complication when it comes to tackling the online scam industry. How is Taiwan working with regional and global law enforcement to share information and pursue the perpetrators of these crimes?

HC: Taiwan's situation is very special. We can't join Interpol, and we have a hard time engaging with countries that refuse to have any diplomatic relations with us, either formal or informal, like Cambodia. If we could have better diplomatic relations with Cambodia, we could access a lot of information that we could use to deal with Taiwan-related cases. The online scam industry is so rampant in Taiwan because we have almost zero intelligence-sharing with many countries. This is a huge problem in investigating cybercrime.