Taiwan responds to increasingly sophisticated fraud models with Financial Education

David Stinson*

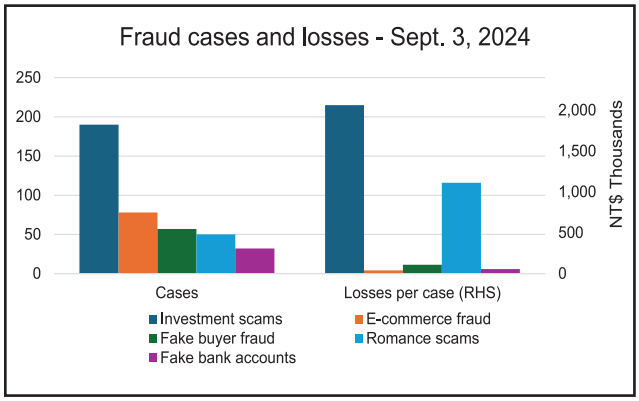
Since the pandemic, 'pig butchering' or *shazhupan* scams have entered our vocabulary. The name refers to the highly labor-intensive process of building the victim's confidence, frequently spanning months or even years. Due to this workload requirement, it often makes use of slave labor lured by fake job opportunities, particularly based in Southeast Asian countries like Myanmar and Cambodia, resulting in double victimization (Office of the UN High Commissioner for Human Rights, 2023). At its peak in 2022, this employment fraud became so common that Taiwan even started monitoring travel by Taiwanese citizens to Cambodia (Everington, 2022).

Outside of the social engineering aspect, the mechanics of pig butchering fraud are not entirely distinct from the much less sophisticated "Nigerian prince" category of confidence scams. Victims are introduced to investment opportunities and promised outsized, guaranteed returns. The scammers may even allow victims to withdraw a portion of their funds as part of this confidence-building process, before perhaps delaying withdrawals so that they will deposit more, requesting a fee to withdraw more and eventually blocking all communications. The payments may take place on fake trading apps or physically through mules. Although such schemes involve investment, it is important to distinguish them from broader investment fraud, such as Ponzi schemes, which involve a real entity or project, even if the money is eventually misappropriated. Instead, the misrepresentation occurs during the payment stage.

Pig butchering is typically associated with romance scams and its emergence has sparked international discussions about problems like social isolation and victim shame. The name and concept however imply nothing about romance. Especially in the wake of a semiconductor stock market boom, scammers in Taiwan have increasingly found it more advantageous to directly approach victims about investment opportunities, immediately selecting for victims with the ability and willingness to pay. On August 30, Taiwan's Ministry of the Interior started publishing a daily fraud dashboard. Typical daily numbers show that although scams with romantic pretexts are more common, monetary losses from investment fraud are significantly higher, indicating larger losses per incident (Figure 1).

*Research Fellow, Taiwan Academy of Banking and Finance, Taiwan.

Figure 1: Case count and loss amount by fraud type in a typical 24-hour period



Source: National Police Agency, Ministry of the Interior

Basic Business Model

A victim might see an investment-related advertiement on a search engine, social media or in a public discussion group, perhaps using the likeness of a well-known financial expert, celebrity, doctor or entrepreneur. They are eventually invited to a free private chat group, which in addition to the guru figure at the center of the marketing, will also typically include an assistant, customer service and perhaps dozens of other ordinary investors (Chen, 2024). Some members may also impersonate police officers, providing an additional element of legitimacy.

Unbeknownst to the victim, they may be the only naturally-interacting person in the group; almost every other account is controlled by the threat actor. During the discussion, the different accounts can proactively address any doubts the victim might have, without the victim even needing to voice them. The scammers can also train the victim on how to avoid banks' Anti-Money Laundering (AML) procedures. For instance, one justification for the use of payment rails outside of the banking system is insider trading, which (according to the pretext) does not necessarily harm the victim (Christian Daily, 2024). Later, they may learn that the same AML procedures which are there to protect them are the reason they cannot withdraw their funds.

Experts note that real investment advice is given, indicating more of a targeted model than romance fraud. Some fraud operations apparently cooperate with real financial advisors to deliver daily market updates, particularly for the early marketing stages of the fraud. At the same time, the fraud actors sometimes have also demonstrated unfamiliarity with Taiwanese geography and linguistics, indicating some degree of offshore operations. Many similarities exist between this model and the later stages of a romance scam and elements of recombination might be possible, but the economics appear to differ slightly from the classic version.

Regulatory mitigations

One important logistical challenge for the implementation of fraud is the coordination of dummy accounts, which happens to be the area under the most direct control of Taiwan's financial regulator, the Financial Supervisory Commission (FSC). A previous campaign by the FSC to crack down on personal dummy accounts, blocking or restricting accounts purchased for use by fraudulent operations for up to five years, has apparently proven successful. In response, many scammers have switched to the use of business accounts over the past year, which also have several advantages in the case of investment fraud. Such accounts may appear more legitimate in the context of the investment pretext in case the victim examines the account and they can also receive larger

amounts without triggering AML warnings – although accounts without registered capital or with shorter history, will still attract increased scrutiny (Yang, 2024a). Of course, opening a business account is significantly more difficult than for a personal account, but it is also substantially more valuable.

Most recently, in August, the FSC also issued a warning about the misuse of its own name (Yang 2024b), which also highlights the growing threat from investment fraud. It mentioned four types of documents which it said were most likely to be forged: securities investment advisory business licenses, margin contracts, statements on internal Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) controls and other announcements and correspondence.

When thinking about mitigation of this investment fraud model, many of the breakpoints are the same as for romance-based scams, with the main exception being that the initial promotion is more likely to take place on the open web, rather than on dating platforms or through private messages. Technical solutions can be applied at various points like app stores, telecom networks or dedicated apps which a user can download ahead of time to monitor activity on the phone. Legislations requires multinational digital platforms to appoint a legal representative in Taiwan to be responsible for issues related to fraud.

Public financial education

Regarding public messaging, meanwhile, the most important message is to never take investment advice from a celebrity; a real investment advisor would not have an attractive assistant who is available all hours of the day. Nevertheless, after the victim enters the confidence-building stage, there are perhaps fewer general psychological markers of fraud than in other models. There is little need for time pressure and there is also little pretext for secrecy when the 'sales funnel' started on the open web. Moreover, many social manipulation represents the next level of social engineering, altering not only one's emotions, but also one's perceptions of reality. It can be quite difficult to recognize in real time.

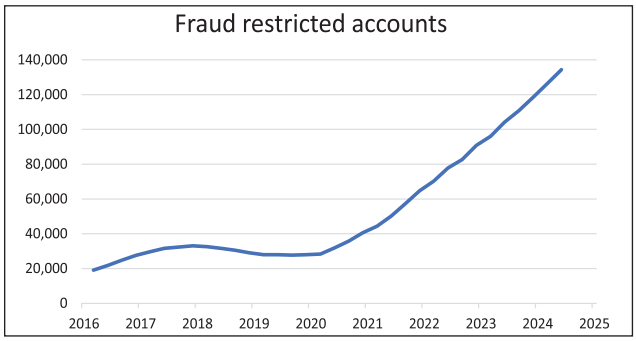
Even if overall psychological hardening may be less relevant for this method, however, because the victims had an original intention of accessing financial services, there may be a more direct opportunity for financial institutions to educate the public about their services. Many victims admit that they did not sufficiently understand how to properly invest. Asked why she thought a bank could not offer the carry trade the scammers could offer, with 12% returns at an interest rate of 2%, for instance, the YouTuber anna_getaway, who was scammed out of NT$ 6 million (US$ 190,000), replied "in fact, I thought about that at the time and asked them about it. But they said their channel required a certain volume…a bank's VIP customers would be offered that opportunity." The arbitrage pretext was not just between Taiwan dollars and foreign exchange, but between the bank itself and the middleman.

Greed is human nature, but financial bodies should do more to educate the public about the benefits of the formal financial system. Taiwanese consumers frequently take an aggressive attitude toward cost-cutting and are receptive to offers to cut fees. They also respond well to terminology like "no risk" and "guaranteed returns," which the financially savvy would understand to signify fraud. This can be another point of emphasis to the public, although it is also to keep in mind that it is a more superficial element of the business model. Scam artists sometimes also prefer to retain some of the more obvious language in

order to initially filter out more skeptical targets.

The other area for public intervention is the dummy accounts and mule operations, which together create large onshore expenses for fraud organizations. The number of suspicious accounts has increased sharply and continuously since the start of the pandemic (Figure 2). Although it has become rarer for people to knowingly sell their accounts, separate fraud models still exist with account takeover as an endpoint. In lending fraud, for instance, targets with no salary history who are unable to obtain lending other ways, often college students or recent graduates, turn to non-traditional methods. Scammers offer a service, whereby, they move money into and out of the account in order to build a history of freelance work on behalf of the client, who can then eventually apply for a bank loan, not realizing they may be held legally liable. Thus, as with offshore slave labor, a dual victimization aspect also exists for onshore operations.

Figure 2: Bank accounts restricted for potential fraud activity

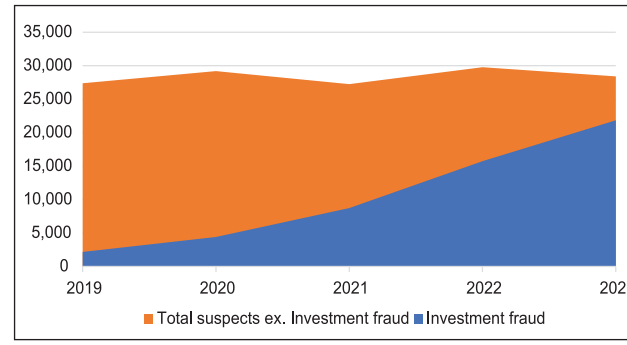


Source: FSC

Regarding dummy accounts, public education can probably focus more on cybersecurity than anything specific to finance. People should understand the dangers of giving out their personal account information, regardless of the degree to which they may trust the other party. Bank accounts are only one particularly sensitive account, out of many.

Mules are generally recruited using traditional employment fraud, meanwhile. Many high-profile arrests of mules have been made, which may explain the growing number of suspects related to investment fraud, which account for most of the growth in fraud suspects over the past several years (Figure 3). Nevertheless, the suspects typically know little or nothing about the core operations, so this is a less useful choke point.

Figure 3: Number of fraud suspects by method



Source: Criminal Investigation Bureau of the Ministry of Interior

List of fraud categories in order by number of arrests in 2023 (categories with >1% of total arrests)

- Investment fraud
- ATM installment payment fraud*
- E-commerce fraud
- Ordinary commercial fraud
- Impersonation of Government officials
- Romance scams
- Lending fraud
- Impersonation of personal contacts
- Gaming fraud
- Employment fraud
- Fraudulent borrowing

**Attackers use information on real e-commerce purchases to convince buyers they mistakenly signed up for installment*

Broader lessons

Investment fraud of this type is mostly an incremental value-added outgrowth of the original romance scam model and it retains some elements of its psychological manipulation. At the same time, it reminds us of the broader role of the financial sector in upholding social order. As the foremost institute in Taiwan responsible for financial training, the Taiwan Academy of Banking and Finance (TABF) has been working to address the trend of investment fraud by proactively teaching investment and saving behavior to the public. Through outreach to primary educational institutions, we have helped young people to enter the workforce with healthy financial habits. In a 2023 pilot project, we also partnered with the Jhe Hui Foundation to not only teach basic financial concepts to rural women, but also track their ongoing results and coach them for further improvement, helping introduce them to formal financial institutions in the process. Through this process, we aim to correct misunderstandings about investment from the source, preventing situations where people need to be rescued later.

Financial inclusion can be defined in terms of three dimensions: access, usage and quality. It is not enough for the proper services simply to exist, particularly when it comes to the higher-value investment services which play an essential role in building lifetime wealth. Ordinary people must feel comfortable using them and they must understand the consumer protection which justify the slightly lower margins. Otherwise, increasingly sophisticated attackers will devise methods which emulate real financial services with increasing precision, requiring genuine experts to tell the difference. When people plan their finances in a deliberate fashion, on the other hand, they are less likely to invest impulsively and more likely to go through the proper, regulated channels, ensuring consumer protection.

References

Office of the UN High Commissioner for Human Rights, 2023. Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response.

https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

Everington, Keoni. August 15, 2022. "9 Taiwanese rescued from Cambodian human trafficking ring." Taiwan News. https://www.taiwannews.com.tw/news/4626546

Chen, Rui-ting. April 10, 2024. "LINE conversation history revealed! She made the mistake of joining the '3.26 million' scam group and personally exposed their fraud methods [Chinese]." FTV News. https://www.ftvnews.com.tw/ news/detail/2024410W0125

Christian Daily. June 13, 2024. "Besides the victims, everyone else in an investment fraud chat is a scammer [Chinese]." https://cdn-news.org/News.aspx?EntityID=News&PK=000000006ac29786c99addee 6877934e 96b9c9 edb2fb256e

Yang, Xiao-jun. August 13, 2024. "To prevent fraud, businesses must undergo three levels of checks to open an account [Chinese]." United Daily News. https://money.udn.com/ money/story/5613/8157365

Yang, Xiao-jun. August 14, 2024. "The latest scam: fraudulent documents from the Financial Supervisory Commission. Urgent advice on two identification methods [Chinese]." United Daily News. https://udn.com/news/story/7239/8161954

anna_getaway. June 9, 2023. "I was defrauded out of NT$ 6 million in a scam like Ayers Alliance…The full recovery process [Chinese]." YouTube. https://www.youtube.com/ watch?v=oXsAzOOmnbc