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.

Money Laundering

Source: Judy Robinson-Cox, Flickr.com

Moving Bricks: Money-Laundering Practices in the Online Scam Industry

CHEN Yanyu

This essay sheds light on the work of some of the key actors who provide money-laundering services to the online scam industry. It shows how, while these businesses frame their involvement as simply 'matchmaking', their brokerage helps shape the rules and practices of the sector, regulating the distribution of both profits and risks. It also highlights how these money-laundering businesses occupy a liminal space between legality and illegality and between national and transnational financial systems, contributing to an expanding underground financial network that spans the globe.

Jingjing invited me to her office and asked me to wait for her to finish work before we headed out to dinner together. At the time, she was working in a third-party payment company—what, in the jargon of the money-laundering industry, is known as a 'gateway' (通道, *tongdao*). Like another similar enterprise I had previously visited, their premises was in a dozen hotel rooms above a casino in Sihanoukville that were rented monthly. The managers had replaced the beds with desks and now the business was up and running. As I sat on the couch waiting for Jingjing*, the office was filled with the rapid and frequent tapping of keyboards and the constant notification alerts of new Telegram messages. It felt like I had entered the trading hall of a traditional stock exchange, but the work being performed here was very different. The job of Jingjing and her colleagues was to match the right buyers ('clients', 客户) and sellers ('account providers', 账户供应商) and facilitate transactions in exchange for a commission.

Money-launderers call this type of 'matchmaking transaction' (撮合交易) process 'moving bricks' (搬砖, *banzhuan*), in which money is the commodity being moved from one place to another, sometimes through direct transfers between accounts and sometimes by withdrawing cash and then depositing it in other bank accounts. Jingjing told me that if a client entrusts them to receive a sum of money on their behalf, the company will contact an outside team that operates bank accounts, which they refer to as 'motorcades' (车队), to prepare to receive the sum. In the words of one of her colleagues with whom I had a chance to speak: 'We are just natural carriers, acting as middlemen to earn a commission.' But what is it that they broker?

*Jingjing is a pseudonym, as are the names of other informants cited in this essay.

The term *banzhuan* has an interesting history. Originally, it literally referred to moving bricks at a construction site; then, by extension, it came to represent any sort of repetitive physical work. Later, Chinese netizens mockingly used the phrase to refer to hard and poorly paid work. At the same time, *banzhuan* also refers to the commercial practice of buying and selling at a profit or 'arbitrage'—that is, taking advantage of the difference in the price of goods between different platforms to earn a profit. It is in this last meaning that the term has entered official discourse in law enforcement circles. For instance, in 2022, the Supreme People's Procuratorate of the People's Republic of China issued a press release about its investigation of cyber-scam money-laundering channels. It documented a money-laundering case in which a Chinese man frequently bought and sold Tether (a type of cryptocurrency commonly known by the acronym USDT) on different online trading platforms (Jian and Cai 2022). The man claimed he was just 'moving bricks' with friends to earn commissions, but in fact he was laundering money for cyber-scam operations.

Indeed, the 'clients' to whom Jingjing was referring were cyber-scam companies, which she and her colleagues call *pankou* (盘口). In the context of the cyber-scam industry, 'moving bricks' refers to the activity of assisting or brokering these money-laundering transactions. This is an aspect of the sector that is widely known but so difficult to penetrate that the existing literature often gloss over it, except for a few studies and reports based mostly on blockchain analysis (Reiter and Bitrace Team 2024; Griffin and Mei 2024; UNODC 2024; for valuable journalistic takes, see Keeton-Olsen 2023; Faux 2023). Its existence serves as a reminder of how the cyber-scam industry is a complex industrial chain or ecosystem that includes not only the teams or companies that perpetrate scams, but also those who conduct ancillary activities of money-laundering, personal information buying and selling, software development outsourcing, and so on.

To fill this gap in the literature, I interviewed four employees of three Cambodia-based money-laundering firms, which I call Company P, Company W, and Company G. Some of them shared internal documents with me and showed me the private Telegram groups managed by their companies. I also participated in some of their after-work chats, conducted informal interviews with nearly a dozen stakeholders in the money-laundering industry, and observed related public Telegram groups and websites over several years to understand the ecology of the sector. In particular, the essay presents money-laundering brokerage in Cambodia as occupying a liminal space between the legal and illegal, between risk and trust, and between different financial systems. By outlining the ambiguities and personal reflections on values, ethics, and legitimacy of the actors involved in these illegal activities, I argue that these practices are consistent with neoliberal beliefs in economic rationality and free markets and are intertwined with the institutional environment of Cambodia's free circulation of US dollars and a thriving underground financial sector that provides a critical infrastructure for the global operations of cyber-scam groups.

The Gateway as Information Broker: Framing the Information Network

In the public Telegram groups run by Company P, every day many people post all sorts of supply and demand information related to cyber-scams. You can see bank account providers (the 'motorcades') actively promoting their services, claiming that their 'advantages' are 'fast pick-up, large amounts, speed' or 'guaranteed time, guaranteed quantity'. There are also companies introducing their scam techniques and seeking to recruit motorcades for long-term cooperation. They require their prospective partners to be 'safe, smooth, [and] not likely to be caught by the police'. One adds sentimentally: 'Partners once, friends for a lifetime.' There are also service providers specialising in finding out why bank accounts are frozen, buyers and sellers of personal information, and scam software outsourcing services. If the actors in this illicit market could work openly in a free market, this would look like a huge cyber-bazaar.

Telegram's encryption and anonymity provide a readymade technological platform for illicit activity, helping people to overcome information barriers and gaps in the circulation of information. Whereas previously one had to know someone who could provide these types of services, now everything is online for those who know where to look. Company P alone has thousands of groups on Telegram that are used to facilitate transactions and provide a channel for the circulation of information. Most of these groups are publicly accessible (they are called 'public groups', 公群), and in them various players in the cyber-scam industry can find business information and establish private relationships with service providers and other actors. Company P draws revenue from advertisements that appear in these groups and from commissions for every transaction conducted through them, for which it also acts as a guarantor.

In addition, 'gateway' businesses like Company P often have private groups for specific trades, which they call 'trading groups' (交易群). Hezi, an employee of Company W, spends his days in the trading groups matching trades between scam groups, or *pankou,* and motorcades, then keeping track of the volume of daily trades generated by each transaction for the company's finance officers to reconcile the bills and settle the commissions. All transactions take place in the Telegram trading groups opened by the gateway company, and the traders work every day to forward the orders and bank account information, and to follow up on the progress of the processing of the scam funds. Hezi describes his job, which follows a repetitive pattern, as 'copy and paste'. This process and the flow of funds between the scammers in the *pankou*, the middlemen in the gateway, and the money-laundering motorcade are illustrated in Diagram 1.

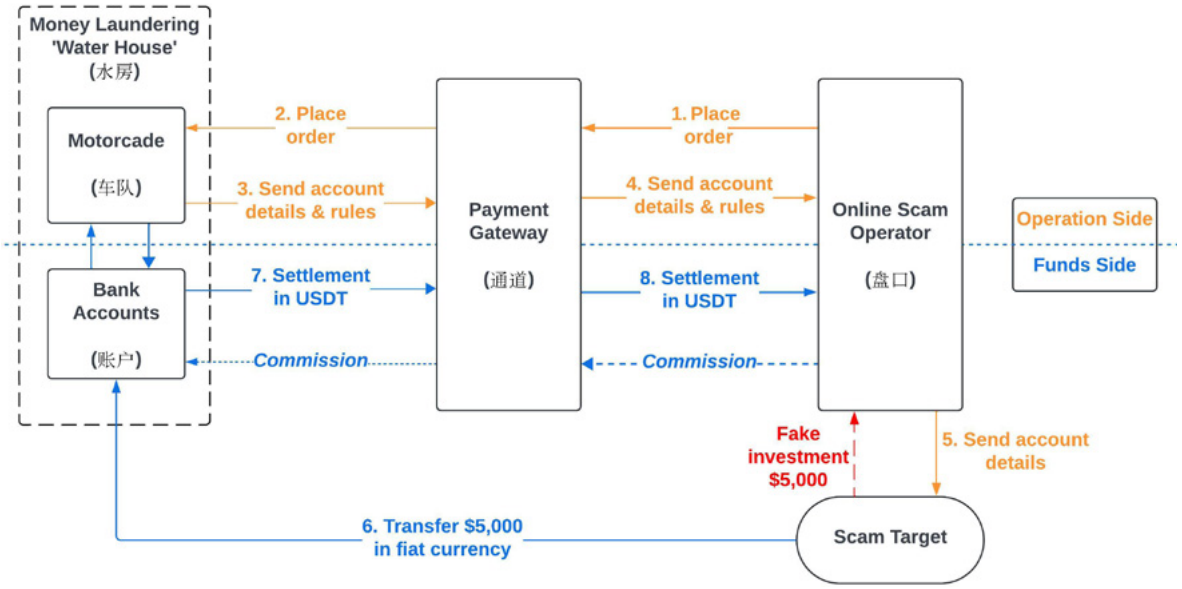

Diagram 1

Visual depiction of the process and flow of funds between the scammers in the *pankou*, the middlemen in the gateway, and the money-laundering motorcade. The motorcades who operate money-laundering and the tools they use such as bank accounts together make up what they call the 'water house' (水房).

Through Hezi's simple 'copy and paste', the *pankou* will be matched to a suitable bank account. The scam target then wires the money directly to the bank account provided by the motorcade and the funds, after fees and exchange rate differences are deducted, are settled to the *pankou* in USDT through the financial settlement of the gateway company—a process also known in Chinese as 卡接回U. 'It's like an intermediary platform,' says Yaya, who works for Company P. Semantically, the Chinese word *tongdao*, which we chose to translate as 'gateway', parallels the English word 'channel'—a linguistic coincidence that shows the intermediary nature of these businesses, which act as a channel for the circulation of both information and money.

The Gateway as Money Broker: Framing the Transaction Network

Using terms such as 'copy and paste' and 'natural carrier', money-laundering brokers distinguish their role from the scams that generate these funds, emphasising that they function only as a supposedly neutral 'channel of information'. However, they clearly play a critical role, facilitating the matchmaking of scammers and launderers. In so doing, they inform the rules of the game, with some gateways such as Company P becoming more influential than others as they establish themselves as authoritative actors in the sector.

This resonates with much anthropological literature on brokerage. In the past, anthropologists focused on the role of the broker in integrating cultural and social structures (Wolf 1956; Geertz 1960), such as integrating villages and communities into the nation-state, but this paradigm declined with the collapse of the colonial system. In the 1980s, the neoliberal turn brought about what has been described as 'the return of the broker' (Lindquist 2015). Scholars have since increasingly focused on how brokerage generates particular forms and frameworks in this new stage of global transformation. Brokers are no longer seen just as mediators (conveying meaning without transformation), but also as intermediaries, 'transforming, translating, distorting and modifying the meaning or the elements they are supposed to carry' (Latour 2007: 39).

Taking investment scams as an example, what happens after someone takes the bait and invests in the fake financial product? First, scam operators will coach them to invest money at certain times, claiming they have privileged information that enables them to predict trends, but also warning that the investment will be profitable only if it is made within minutes. Once the target agrees to proceed, the scam operator will send a message to the Telegram group run by the gateway explaining the currency and amount of money about to be remitted by the scam target. Brokers at the gateway will then send the details to the motorcade group to match bank accounts. After the motorcade group provides the information, the gateway will send the appropriate details and trading rules back to the scam operator.

The 'trading rules' provided by Hezi's gateway company impose a clear limit on the remittance period: within 30 minutes of when the account information is sent. If it takes more than 30 minutes to get the scam target to agree to the transfer, the *pankou* must 'place an order' again. Scam operators endeavour to get their targets to send money to the designated account within the specified time as behind the seemingly simple rule lies a complex act of balance and risk distribution. If the money is not sent within the time limit, the *pankou* may receive a different bank account when placing another order. This can easily raise the target's suspicion, which risks them realising that something is amiss. Furthermore, if something goes awry, all risks and costs are borne by the *pankou*, including compensation for higher bank account fees, frozen funds, and so on.

As for the motorcade, they usually operate many bank accounts at the same time. To avoid banks' anti–money-laundering (AML) scrutiny, they must strictly control the time interval in which each bank account receives different remittances, as well as the amount of each remittance. To do this and reduce the risk of their accounts being frozen or closed, they work with people with professional AML knowledge and experience. Moreover, when the money in a bank account reaches a certain amount, they must dispose of it in a timely manner in ways that suit the banking system of the country in which the account is located. For instance, motorcades located in China might choose to withdraw the funds, deposit them into another, unrelated bank account, and then convert them into US dollars or USDT, which usually takes less than two hours.

Motorcades also adapt their money-laundering strategies to the AML policies of the country in which the bank account is opened. In recent years many people in China have sold their bank accounts to scam gangs and other illicit actors for often paltry sums of money. In response, the Chinese authorities have taken harsh measures, beginning with a 'Card-Breaking Operation' (断卡行动) launched in 2020 (Ministry of Public Security 2020). This crackdown has been successful in tracing and freezing large amounts of funds and bank accounts involved in money-laundering. As a result, Chinese motorcades gradually moved away from the 'old way' of dispersing funds to different accounts through online transfers and began to go directly to bank counters to withdraw cash and then deposit it into different accounts. This method is more expensive, as motorcades must sometimes fly people to different locations to physically withdraw funds, but it is also much harder for authorities to track.

Gateway businesses must coordinate the work of *pankou* and motorcades and, in so doing, must keep up to speed with the AML policies of each country to avoid conflicts or disputes as much as possible. Thus, money-laundering brokers serve as a channel to circulate information and facilitate cross-border transactions, but also reconcile the different scales of market rules and conflicts, which include not only patterns of interactions between scam operators and scam targets, but also specialised knowledge in operating accounts in accordance with the financial systems of different countries. As well as requiring specific expertise, this helps shape the market for international illicit transactions.

The Gateway as Arbitrator: Risk Redistribution

As intermediaries and platforms for matching scam operators and motorcades dispersed all over the world, gateway businesses also act as an arbitrator and guarantor. As mentioned, the target of the scam does not send money directly to the *pankou*; rather, the money first passes through the motorcade and gateway, which makes the process fraught with uncertainty and potential risk.

Stories of people 'running away with the money' (卷钱跑路) often circulate on Chinese-language social media in Cambodia. For instance, one Chinese broker whom I met three years ago in Sihanoukville was wanted by the owner of a cyber-scam operation, who had put out a reward notice to try to get 'his' money back and possibly exact revenge. This man, who was working on his own, had not settled the money with the *pankou* after receiving it from the motorcade, and had instead absconded with it. To prevent such occurrences, *pankou* and motorcades usually seek a guarantor or arbitrator to guarantee the transaction, and in most cases this role falls to a gateway that has a 'good reputation' in the industry, such as Company P. The mechanism is like that of a guarantor bank in international trade, which holds the money during the period between the shipment and the delivery of goods.

Xin, an employee of Company G, mentioned to me that her company owned its own money-laundering motorcade. To prevent foul play, *pankou* would usually ask them to pay a deposit (上押) to Company P before the transaction begins:

> It is the one who receives the money [on behalf of others] that has to pay the deposit ... First, you talk about the rules and regulations—that is, rules like, if the money is dead [死钱, meaning that the bank account has been frozen], who is responsible for that ... Then there are practical situations, [such as] which party is responsible to pay—if it is the demand side [the *pankou*] or the supply side [the motorcade]. Then it is up to the two sides to provide evidence and, if there is a dispute, to see which evidence is more convincing and then pay to the other party accordingly.

More specifically, during the transaction, Company P's staff will act as an arbitrator and create a private group on Telegram (one of the 'trading groups' mentioned above) where the motorcade and *pankou* share their own trading rules. After both parties agree, the staff of Company P will collect a deposit from the motorcade. Once the transaction amount exceeds the deposited amount, the motorcade must settle the balance of the payment before any further transactions can occur. Should the scam continue and bring in more funds, the motorcade can repeat the process and transfer funds against its original deposit, provided it settles the earlier transaction. The gateway arbitrator keeps track of the amount of each transaction through a bookkeeping bot inserted in the Telegram group and takes a commission.

When a transaction dispute occurs, the gateway will ask both parties to provide evidence. Acting as an arbitrator, the broker will not directly decide which party is liable for the loss but wait for both parties to reach a consensus. If the dispute remains unresolved, Company P will continue to withhold the deposit. The arbitration regulates the allocation of risk in an illicit transaction and ensures that the motorcade will not run away with the money, while at the same time forming a flexible arbitration system.

Transaction disputes are often triggered by the freezing of bank accounts, which Simon, an employee at Company P, calls 'risk-control risk' (风控风险). It is an ironic term that refers to a risk caused by state and bank AML regulations, which Simon also calls the 'friction cost' for a company. Since there are risks, there are risk controls, and Simon's work is to 'control the risk-control risk' by developing standard operating procedures for employees to avoid exposing the company to losses due to operational errors by their staff. By means of 'internal risk control', gateway businesses attempt to transfer the risks resulting from state regulation outside the company.

When Hezi first joined Company W, he participated in internal training. The manager familiarised staff with the trading rules, after which they had to pass an exam arranged by the company. The purpose of these rules is to provide grounds to argue with clients in case of disputes.

> For example, 100,000 dollars come and then the account is frozen, but the money is in the account. But the account was frozen before the maintenance period [that is, a period during which the *pankou* is bound by the gateway to keep up the pretence of a legitimate investment with the scam target] was up, so … this is a [scam target] who transferred it in, and then reported the account [to the police]. It is because of the client that the money was frozen, but the *pankou* denies this … So, we have to show the rules and tell them: 'Your payment wasn't frozen because of us' … That's why we have to know the rules, so we can clear it with the client; otherwise, sometimes the client … will play dumb, he pretends that he doesn't know the rules.

Safe Harbour Off the Land

US dollars circulate freely in Cambodia today. After Pol Pot destroyed the country's monetary system during the Khmer Rouge era (1975–79), the United Nations temporarily took over national administration in 1991–93 and the Cambodian economy was rehabilitated through multilateral and bilateral international aid (Xiao et al. 2020). A large volume of US dollars flowed into Cambodia, creating a dual monetary system in which both US dollars and Khmer riel circulate. Although the government has been actively encouraging the increased use of the riel in recent years, this system remains today and has spawned a variety of underground financial networks. The free flow of US dollars constitutes an important infrastructure for the development of the money-laundering industry, as brokers like the gateway businesses discussed in this essay usually trade in US dollars and the US dollar-pegged Tether (or USDT). Both the large Company P and the smaller Company G provide their services to *pankou* based not only in Cambodia, but also in Myanmar, the Philippines, and other countries. Their transnational business model is well expounded by a corporate slogan for Company P that was related to me by its CEO: '*Rooted in Cambodia, looking to Southeast Asia, going global*' (扎根柬埔寨, 放眼东南亚, 走向全世界).

After decades of growth, the cyber-scam industry has developed into a behemoth that targets people all over the world. The actors providing money-laundering services for scam operators have expanded accordingly, and some have public-facing businesses and are well-known for their seemingly legitimate parallel business endeavours. Of the three brokerage companies I observed, Company P legally holds a Cambodian Payment Service Institution licence. In addition to its gateway business, this company has developed a money farm (钱庄, a traditional type of banking service with a long history in China), fiat currency exchange, cryptocurrency exchange, and a diverse range of other businesses. It also has a bank that legally holds a banking licence.

Announcements in Company P's official Telegram group (which is public) show that their gateway business already covers more than 20 countries and regions, making it one of the largest such businesses in Cambodia.

The 'actual global', as Ong and Collier (2005) put it, is loaded with heterogeneity and instability, while at the same time it has a distinctive capacity for de-contextualisation and re-contextualisation, with various technologies and values constantly reassembling. In a world of globalised flows of commodities, interactions between the legal and the illegal constitute the context in which we live (Nordstrom 2007). At the same time, interactions between the licit and the illicit reshape perspectives on the political legitimacy of those engaged in illegal activities (Roitman 2007). Brokers, as intermediaries connecting two or more worlds, not only graft local and global markets, but also connect the legal and illegal worlds. My interviewee Simon says that people like him and his colleagues 'are not creating a new market, they're solving a very old problem of getting into the banking system people who have long been shut out of it'. Such market needs have always existed. He used an analogy to describe the service they provide:

> Let's put it this way ... It's like a merchant ship, a cargo ship, a ship that can legally dock at the pier, as opposed to a pirate ship, which has no licence or a black flag. Well, there is no way for a pirate ship to dock, they will not let you dock. This kind of ship will always be floating in the sea. Then we are kind of floating on the sea, kind of like a small centre, kind of like a harbour off the land, especially for all pirate ships to come here to spend and unload. This is the kind of feeling. It's not a country; it's not a port; it's just a place where you don't know how many ships are coming tomorrow and you don't know how many are going to leave ... But we're just another channel for ships that don't have a way to dock. Yes, another solution.

In conversations with various global outlaws, Nordstrom has found that they do not understand the world in terms of legal versus illegal, but rather in terms of 'what works best', which coincides with Simon's view. For Simon, their work is like 'playing with the rules' (玩规则), playing with different market actors, playing with different countries' financial systems, and exploring how to do things without going through 'due process'. Situated in Cambodia, these brokers are protected by powerful partners and the local government and participate in the country's legal economy, but their activities are also connected to a massive international money-laundering network. Embedded in the discourse of the 'market', the ambiguous border between legality and illegality continues to challenge our thinking about politics, economics, and ethics.

The scale of the cyber-scam industry continues to grow. With policy changes in Southeast Asian countries, cyber-scam operators are gradually migrating from places like Cambodia, Myanmar, and Laos to West Africa, Georgia, and the United Arab

Emirates. Maizi, an employee of an online gaming company who I have known for a long time, has spent the past three years moving from Cambodia to Dubai, then back to the company's earliest home base in Manila. No matter where these businesses move, gateway brokers can handle their money transfer needs remotely while sitting in their offices in Cambodia.

This essay has sketched the network of the illicit money market in terms of an intermediary practice. From the practices of the actors I discussed, we can see that this underground market is still forming and transforming. This illicit market network is full of uncertainty and resilience, just like the neoliberal world we experience every day. Through these brokers' interactions with financial markets and online scams in different regions and the process of reconciliation at different scales, a large, complex, and multifaceted underground financial market is penetrating all corners of the world.

The CEO of Company P shared with me his view on cyber-scams. For him, the distinction between legal and illegal is an issue of power rather than law and behind it lies the question of 'who has the power to define what is illegal?'. Power, in turn, depends on access to social resources. In international money-laundering transactions, the actors involved are often at war with the financial systems of different countries and know how to play with their rules. In Cambodia, they can get the payment service provider and banking licences they need to enter the Cambodian financial system and build apparently legitimate fronts, but it would be a mistake to blame this exclusively on the shortcomings of the Cambodian political and financial systems: some companies have also obtained cryptocurrency exchange licences in a compliant manner in European countries. They hold the romantic view of themselves as bandits who 'rob the rich to give to the poor' in a cruel capitalist world, but ironically, at best, they only 'rob from the rich' (and even that claim is highly questionable), never giving anything to the poor. The truth is more prosaic: they are just the last representatives in a long line of 'entrepreneurs who use private, formally unlicensed violence as a means of social control and economic accumulation' (Sidel 1999: 71–72). ●