FEBRUARY 2023

Control Risks
化险集团

Risk assessment

SIM farms and business SMS

In 2021-2022, Control Risks undertook work to research information in the public domain, including searches of the deep and dark web, and reached out to more than 40 well-placed sources with first-hand experience of SIM farms from the perspective of law enforcement, government regulators, legal advisors, commercial partners and perpetrators. The investigation included consulting experts based in Belarus, Cambodia, mainland China, France, India, Kazakhstan, Latvia, Russia, Ukraine and the UK.[1]

Key findings

- The global SIM farm industry is unregulated and fragmented, and publicly associated with cybercrime, corruption, and multiple forms of online and telecoms fraud.
- SIM farms make it easier for spammers and fraudsters to deliver SMS since SIM farms circumvent many mobile operator safeguards. SIM farms also handle large volumes of SMS for legitimate businesses that are likely unaware that their traffic is being processed in this way. This exposes those businesses and their customers to data protection and consumer protection risks and liabilities.
- The main appeal of SIM farms is that they offer below market prices, and this is how they enter the supply chains of even legitimate businesses with insufficient control over their SMS delivery chains.
- SIM farms have been known to often breach data protection legislation by harvesting and reselling consumer personal data or misusing the data themselves. Even SIM farms that do not seek to monetise consumer data are illegitimate as they do not have the required safeguards in place to secure the consumer personal data that they are processing nor are they always registered legal entities, another data protection requirement.
- SIM farms are difficult to stop because they largely conduct business outside the control of mobile operators, outside regulated banking systems, in opaque cross-border environments, and are often operated by experienced organised crime groups or individuals looking to make quick profits operating on a small, hard to detect, scale.
- The risks related to SIM farms for a business can be mitigated by applying appropriate supply chain due diligence on a strictly controlled, preferably short SMS delivery supply chain in combination with the use of reputable messaging aggregators that mainly use their own direct connectivity to mobile operators to send the SMS traffic entrusted with them.

[1] Enquiries in the Commonwealth of Independent States were conducted at the end of 2021.

Control Risks Group (Shanghai) Limited | Suite 701, Henderson 688 | No. 688 Nanjing Road West Shanghai 200041 | China
+86 21 6010 9700 shanghai@controlrisks.com

Ecosystem

The overlapping business of SMS and SIM farms ecosystems form a complex system with many different stakeholders.

SIM farms

Media references to SIM farms – where SIM cards are put into modems connected to a mobile network to send various types of telecommunications traffic like voice calls or SMS – often suggest that they are run by sophisticated underworld figures such as cybercriminals and fraudsters. Control Risks' findings indicate that SIM farm operators are commonly the least technically skilled players in a complex communications ecosystem. Unbeknownst to their end clients, they handle large volumes of legitimate SMS business communications while also servicing criminal enterprises.

> "*If you have an image in your mind of a SIM farm as a dirty basement with rows of SIM banks, then you are right; you might also see the operators of this equipment drinking vodka and fighting each other.*"
>
> *Former operator of a SIM farm in Russia*

SIM farms in the CIS

A data protection expert based in one of the Baltic countries summarised the SIM farm business model: "*The SIM controllers in the market…can be compared to* [an illicit] *ride-hailing service, and SIM farm operators can be compared to taxi drivers, with the difference that they are taxi drivers who do not face any government regulation in their work*."

This description was echoed by an executive of a microelectronics company who said, "*you buy compatible hardware, and a SIM controller… provides you with traffic to handle.*"

It is important to note that SIM farms are typically low-tech operations run by individuals who do not have a registered company, technical skills, or independent access to SMS traffic. In the SMS ecosystem, these operations and individuals are the SIM farm operators. An analyst who has previously advised the Russian government said: "*I don't think that SIM farm operators are representatives of criminal or hacker communities, rather these are the idiots who give out their bank card details in order to accept and process fraudulent payments or withdraw money for fraudsters. Basically, not rich and not very smart people.*"

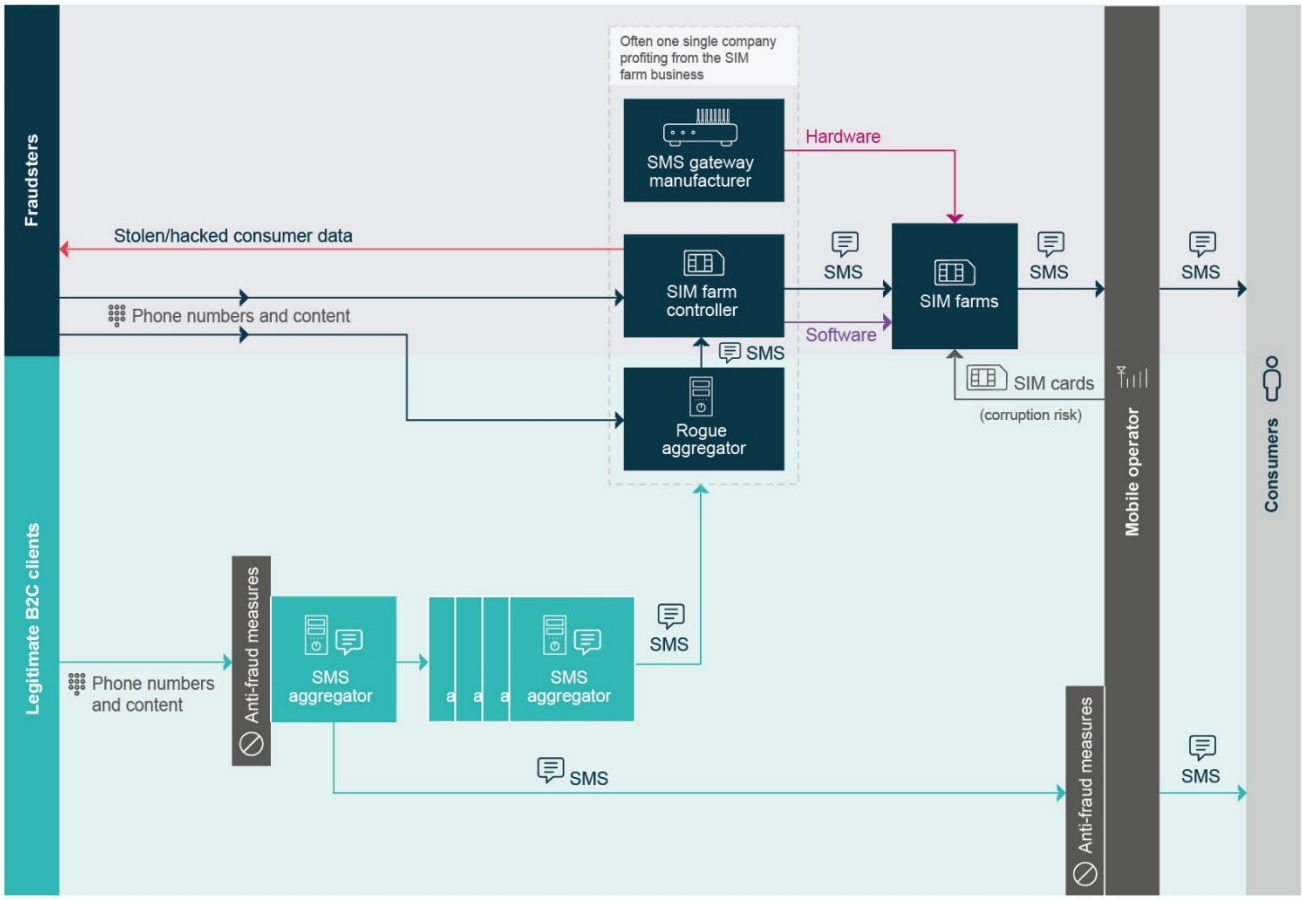
SIM controllers

SIM farm operators are only able to plug into the ecosystem through SIM controllers. SIM controllers provide the SMS traffic that a SIM farm processes. They commonly present themselves as seemingly reputable aggregators who receive SMS traffic from businesses through upstream intermediaries or they might be an arm of a company manufacturing the hardware used in SIM farms. SIM controllers depend on attracting legitimate SMS traffic while simultaneously maintaining links with SIM farms and fraudsters. As such, they are the most clandestine and hard to identify actors in this space.

Besides making money from sending legitimate business SMS, SIM controllers also send SMS on behalf of fraudsters who intend to deceive consumers in various ways. SMS phishing – where the fraudster impersonates a known brand, like a bank or a courier to trick consumers into providing details or to act in a way that allows fraudsters to steal their money – is one common fraud scheme perpetrated via SIM farms. The reason fraudsters often use SIM farms is that SIM farms circumvent many mobile operator safeguards, making it more likely the SMS will be delivered. On top of that, SIM farms are cheaper than sending SMS via proper channels.

Spam – traffic that a consumer has not agreed or accepted to receive – is another type of fraudulent traffic passing through SIM farms.

Figure 1: SMS communication ecosystem



SIM farm infiltration of the business SMS ecosystem

SIM controllers can infiltrate the SMS supply chains of legitimate businesses through competitive pricing. Discreet enquiries conducted in the Commonwealth of Independent States (CIS) indicated that rogue aggregators use SIM controllers and, by extension, SIM farms to lower their overall pricing to upstream aggregators in order to attract traffic and ultimately make money.

A senior security manager of a Russia mobile network operator (MNO) and an employee of an IT centre in a Baltic country described the practice among aggregators of splitting SMS traffic between direct connections to MNOs and SIM farms for different clients, or even within a single SMS marketing campaign, to lower the overall average price. The IT centre source said that if the market rate of SMS sent via mobile operators was ten cents, SMS sent via SIM farms might cost only two cents. Therefore, if the aggregator processes some via MNOs and sends others to SIM farms via a SIM controller, the average cost per message would be six cents per message and the aggregator could offer services to its clients with prices based on this, enabling it to beat the market rate. The source said that aggregators reduce costs by splitting their traffic in this way to attract prestigious clients, such as banks, through

cheap pricing. According to the source, a rogue aggregator that subcontracts to a SIM controller typically offers the same average price to both prestigious and less prestigious clients.

SIM farms are able to operate and prevent being shut down permanently thanks to the cross-border nature of these operations. For example, a US bank that wishes to use SMS for two-factor authentication might send data to a tier one aggregator registered in the US, which passes the data to another aggregator registered in Mexico, which in turn passes the data to a SIM controller in Russia, which finally passes the data to a SIM farm operator working from their basement. The SIM farm operator might use equipment manufactured in mainland China and SIM cards from the UK to send the US bank's SMS.

In practice, the business contracts a seemingly reputable aggregator that subcontracts work to other seemingly reputable aggregators. A SIM farm only becomes involved when a conscious decision is made by an aggregator to subcontract to a SIM controller that will direct traffic through a network of SIM farms to reduce costs in order to be able to offer a cheap price. However, the two sources cited above cautioned against attempting to divide aggregators, at least in the CIS, too strictly into "good" aggregators that work officially and legitimately with MNOs and "bad" aggregators that use SIM farms.[2] The sources said that, in practice, there is considerable overlap. The senior security manager of a Russia-based MNO said: *"There are no companies that work only with mobile operators or only with SIM farms. It is easier and more stable to use both and distribute the flow of SMS between them."*

> "*It is important to understand that the market for SIM farms is a shadow industry. Payments are carried out using cash, or informal transfers of funds to personal bank accounts, or even through digital payments. This is a market that is, by definition, poorly regulated by the state, if at all.*"
>
> *Former law enforcement officer in Ukraine*

The fragmented and global nature of the SMS industry hampers national industry regulators and law enforcement agencies in taking action against the facilitation of crime. A former analyst at the Latvian government summarised the situation in the CIS, saying: "*To be honest, this industry is totally unregulated, and I don't see any sign of it changing in the near future.*"

Containing SIM farms – case study from China

Where there have been prolonged and concerted efforts by a national government to contain illicit SMS traffic to reduce online fraud, such as in mainland China, fraudsters have moved deeper underground and into offshore jurisdictions.

Market sources in mainland China recounted that during the crackdown on online and telecoms crime, which began to focus on the SMS sector in 2020, key stakeholders of SIM hardware manufacturers were detained and questioned by the police about telecoms fraud in mainland China. In one case, the stakeholder was released only after he signed a letter of guarantee that from that day the company would not sell a single SIM bank in mainland China. An industry source who is familiar with the company said that organised crime groups in Shenzhen had previously conducted telecoms fraud using SIM banks manufactured by the company.

Our public-record research, as well as discreet enquiries in India, Thailand, and Cambodia, indicated that since the crackdown, criminal activities related to SIM farms associated with PRC nationals have dispersed across Asia, particularly to Cambodia, which since 2016 has been associated with criminal activities conducted by Chinese nationals. Sihanoukville, where there is a large expatriate population of Chinese nationals, is reputed to be a centre for illegal online gambling, human trafficking, kidnap and ransom, violence and fraud, especially online and SIM-

[2] The sources are the senior security manager of a Russia MNO and the employee of an IT centre in Latvia.

enabled scams.[3] A Cambodia-based industry analyst said that SIM farms that send a blend of legitimate and fraudulent SMS commonly also engage in "*more illegal and therefore more profitable*" activities such as online gambling scams and romance fraud. Criminal SIM farm operations such as these in South-East Asia often recruit and later unlawfully detain workers in what the media commonly describes as slave conditions.

The scale of a SIM farm operation moved from mainland China to offshore is apparent from a 2017 case in which police officers in Thailand arrested three Chinese nationals for working without permits and smuggling SIM cards.[4] They were conducting small-scale fraud through a SIM farm and were found to have smuggled almost 350,000 SIM cards into Thailand, using them to register fake online accounts. Their set up was comprised of a rig of 21 SIM banks fitted with 500 smartphones, which were linked to computers. The aim of the fraud was to artificially increase the perceived popularity of websites, social media posts or advertising revenue by automatically clicking on links or liking online content (a click farm). Subsequent investigations found that the operation had been funded by a company in mainland China.

Hardware

SIM gateways (also known as banks, modems or boxes) are the devices that house SIM cards and through which the traffic is sent. Despite criminal SIM farm activities appearing to have largely moved away from China, manufacturing devices with the ability to circumvent MNO anti-fraud detection systems continues in China. The product features of SIM banks manufactured in mainland China potentially violate requirements imposed by both overseas and domestic regulators, such as enabling users to change IMEI (International Mobile Equipment Identity) numbers to make detection more difficult.[5,6] We identified products manufactured in mainland China highlighted on dark web criminal forums for their human behaviour simulation features to support SMS and Unstructured Supplementary Service Data (USSD) services,[7] which are used in sophisticated scams. We also found several open-source tutorials on Russian-language IT and tech blogs detailing how to configure SIM banks for mass messaging. Criminal actors demonstrate the intent and capability to use SIM devices for malicious purposes, such as for call flooding attacks (a denial of service (DoS) attack that involves directing large numbers of calls at a specific target to disrupt the normal telephone operations of businesses), in addition to making money from sending legitimate business SMS and SMS spam and fraud traffic.

SIM Cards

SIM cards are necessary in order to operate a SIM farm. These need to be procured from a mobile operator and in many countries the MNOs and/or regulators have set up safeguards to prevent SIM cards from being obtained by fraudsters. As such, SIM cards are often procured in bulk through fraud and the process is also generally associated with bribery.

SIM cards procured by bribery was a common theme in our enquiries and several sources mentioned SIM farms working with someone inside an MNO to obtain SIM cards. A risk analyst working at a Ukrainian MNO said: "*SIM farms, as a rule, spring up around MNOs.*" As some telecoms companies are state-owned, this adds an additional

3 https://www.scmp.com/news/asia/southeast-asia/article/2107452/we-call-them-criminal-nomads-chinese-scam-suspects-took; https://asia.nikkei.com/Spotlight/The-Big-Story/Cyber-slavery-inside-Cambodia-s-online-scam-gangs; https://www.voacambodia.com/a/chinese-scammers-enslave-jobless-teachers-and-tourists-in-cambodia/6231075.html; https://www.phnompenhpost.com/national/chinese-nationals-detained-voip-scams

4 https://www.vice.com/en/article/43yqdd/look-at-this-massive-click-fraud-farm-that-was-just-busted-in-thailand

5 For example: https://www.dinstar.com/WEB/files/47154/2019-04-30/; http://www.hybertone.com/uploadfile/download/20140304125509964.pdf

6 An IMEI number is a unique identification or serial number that all mobile phones and smartphones have.

7 USSD is a messaging protocol used in cellular networks based on the Global System for Mobile Communications (GSM) and is used to send small data packages without data connection or incurring SMS costs.

regulatory risk for businesses with SIM farms in their delivery chain, as there is potential exposure to anti-corruption regulations where bribery has been used. The analyst who has advised the Russian government described operating a SIM farm in Russia as "*not really a business at all, more like a way for those with friends in MNOs who have access to SIM cards to earn a bit of money on the side*".

> "*Our biggest concern is that SIM farms gain access to SIM cards from telecoms operators through corruption. They pay bribes for access to corporate SIM cards.*"
>
> *Former law enforcement officer in Ukraine*

A Cambodian analyst noted that a common practice to procure SIM cards in Cambodia is to falsely pose as a reseller or to "*register a SIM to a scan of a dead guy's passport that the police have posted on their official Facebook page*".

Risks

Our investigation built up an image of SIM farm operators as being motivated by money and of poor integrity. Some of the key risks associated with SIM farms are summarised below.

Risk to consumer data

Businesses that allow SIM farms access to their customers' personal data expose themselves and their customers to significant risks.

Data theft exposes a company to direct data protection legal liabilities and its customers to fraud, which in turn entails legal liabilities as well as reputational risks for the company. The 2022 Identity Fraud Study published by Javelin Strategy & Research estimated that data breaches lead to losses of USD 52bn for consumers in the US in 2021.[8] Cybercriminals that carry out SMS phishing use SIM farms to bypass MNO safeguards.

The link to cybercriminals creates a loop as SIM farm operators have a motive to harvest personal data from legitimate businesses to sell on the deep and dark web to fraudsters and other cybercriminals. This data could be used in spam campaigns as well as in more sophisticated attacks that combine personalised phishing emails and SMS with malware. A former security advisor based in India described their experience investigating SMS funnelled through a SIM farm, which was intended to illegally influence the electorate using personal data obtained by bribery.

While SIM farm operators may not typically have high-tech skills, our research indicated that SIM farm equipment from the brands most mentioned on criminal forums is susceptible to security issues, implying that a SIM farm operator with modest technical skills could access poorly encrypted data, giving them access to consumers' personal data.

> "*The routing procedure of these products is vulnerable to hackers, who are able to harvest the traffic and transmitted content…industry peers used to say that the products were mainly supplied to criminals running telecoms fraud.*"
>
> *Sales manager of a SIM bank manufacturer in mainland China*

An international projects manager for a global search engine said that they were familiar with a large SIM controller operating in the CIS. The source said: *"Its data protection mechanisms are – to put it mildly – outdated*". Sources in mainland China unanimously described the technology in products from a brand, which we found mentioned

[8] 2022 Identity Fraud Study: The Virtual Battleground | Javelin (javelinstrategy.com)

frequently on dark web forums, also as "*outdated*". According to a former marketing manager of a distributor, the products referred to on these forums have not been updated since 2017 or 2018.

Several sources in the CIS recounted an incident whereby data was stolen from an internet and telecoms operator within a well-known and large construction group. The company was using a network of SIM farms in Latin America but in 2017 had a data protection failure of "*systemic proportions*", according to a former SIM farm operator. The company intended to outsource regional SMS communications to a disparate group of small SMS farms in Latin America. To save time and costs, the SIM farms were identified through a consultant. What the company had not realised was that the group of SIM farms were all controlled by the consultant, who had opportunistically adopted the role of a SIM controller. The consultant had his own equipment installed in the SIM farms, which were used to control and mine data from the entire network. As a result, the consultant was able to consolidate all the personal data processed by the company, which he subsequently tried to sell.

Even without actively mining data with malicious intent, a SIM controller posing as a reputable aggregator to its clients typically does not live up to requirements regarding handling personal data. The international projects manager said that SIM controllers' internal storage processes are usually poor. The source said: "*I am told* [by a colleague in Ukraine] *that…data is simply stored in an Excel spreadsheet on a local computer.…Who knows which employees are authorised to access that computer or who could use it without authorisation?*" As such, even if a SIM controller does not have bad intentions, the safeguards required by data protection legislation to keep consumer data safe are typically not in place.

Risk of legal data protection breaches

As explained, SIM farms and SIM controllers process traffic for legitimate businesses. Data protection legislation makes the business sending SMS responsible for data compliance throughout the delivery chain. When a SIM farm breaches data protection legislation, the sending company is legally liable. Such businesses are unwittingly in contravention of laws such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the US, the Protection of Personal Information Act (POPI Act) in South Africa and the General Data Protection Law (LPGD) in Brazil. A former SIM farm operator cheerfully admitted to having been in breach of the GDPR, as well as local regulations.

On the most fundamental level, most SIM farms and SIM controllers do not even operate under a registered corporation and are therefore ineligible to legally handle data, according to major data protection regulations. A data protection lawyer said, "*Even leasing a piece of equipment to transfer personal data through is a delegation of personal data processing and requires documents. But SIM farms are not companies and, accordingly, they cannot provide workflow documents adequate for the requirements of the GDPR.*"

Where the original source of leaked data can be identified, businesses that are liable for data leaks can face regulatory fines and class action lawsuits running into millions of USD.[9]

Furthermore, the sending company indirectly breaches the terms and conditions of the majority of MNOs globally, as they typically specify that SIM cards cannot be used in SIM farms for the mass sending of business SMS. Although the SIM farms are in direct breach of the MNO's terms and conditions and there is no liability for the business, the

[9] For example, in terms of regulatory fines related to SMS, in July 2020 an Italy-based telecoms operator was fined USD 18.8m for data breaches by a subcontractor and in November 2020 a multinational telecoms company was fined USD 14.5m by the Italian data protection supervisory authority.

Class action lawsuits for data breaches have been faced by a credit bureau agency which in 2019 agreed to pay USD 575m (which may have increased); a bank holding company which in 2021 settled for USD 190m having faced a similar unrelated suit in 2019 that settled for USD 80m; and a global financial services firm in 2022, which settled for USD 60m (after a regulatory fine of a further USD 60m).

businesses unknowingly become part of defrauding the mobile operators, as if the traffic had been sent properly, the MNO would have made money from it.

Unless aggregators and all their subcontractors are selected with appropriate due diligence, content is at risk of passing through SIM farms. SIM controllers and SIM farm operators are not usually properly registered businesses in good standing with regulators and therefore cannot meet the criteria of most data protection legislation or anti-money laundering requirements. They are covert operators that seek to conceal the identities of their ultimate beneficiaries and maintain a level of secrecy around their business, which is often associated with facilitating crime. A business that sees its SMS pass through SIM controllers and SIM farms is in breach of data protection legislation.

Risks for parties using SIM farms and SIM controllers themselves

The criminal nature of many SIM farm operators puts parties that leverage SIM farms at risk.

A source based in Russia said that SIM farm operators often attempt to extort SIM controllers by threatening to harvest the consumer personal data that they process.

> "*Another favourite of SIM farm owners is extortion. Almost half of all the temporary contractors that we used tried to threaten us at one point. They would try to work out who our clients were, to go to them themselves, or threaten to sell the data on.*"
>
> *Former owner of a SIM controller in Russia*

Sources said that there was no legal recourse to address the opportunistic and unscrupulous business practices of SIM controllers and SIM farm operators. For example, a manager of a call centre in Russia commented on personal data theft by a vendor in Ukraine that was retrospectively identified as a likely SIM controller. The source said:

> *I am sure that* [the vendor] *sold our clients' data. Our clients were three small advertising studios entering the Ukrainian market. A month after starting to work with us, all three studios began to receive offers from our competitors. I'm sure* [the vendor] *sold our customer data, but we did not have a contract and could not make a claim.*

Conclusion

SIM farms are primarily used to send SMS by both seemingly reputable, but ultimately rogue, aggregators and for nefarious purposes, such as fraud, by bad actors. Businesses – legally liable for data protection and compliance throughout their communications supply chains – might be unknowingly delivering consumer personal data to SIM controllers and SIM farm operators, who might concurrently be facilitating or engaging in fraud that could end up targeting their customers.

Our assessment is therefore that even when directly contracting a large and seemingly reputable aggregator, a business should know its suppliers' delivery chain, possibly through an audit, understand its own data protection risk, and examine any low-cost pricing properly as it may be indicative of a bad actor.