International Fraud in Current Russian Realities

Globalisation and digitalisation make business processes easier and a provide level playing field for everyone, especially for emerging nations. At the same time, these trends create new opportunities for criminals, who employ technological developments in their favour. Russia is one of the countries to have faced the growth of international fraud and crimes using new technologies which have created a number of problems for the Russian authorities.

In recent years, cross-border crime has increased worldwide. The contributing factors are well known and include development of digital technologies and the convenience of cross-border communication. Thus, in many cases, cross-border fraud means cyberfraud or fraud committed by means of digital communications.

This tendency is well demonstrated by the exponential increase in spending on cyber security, which is expected to comprise up to US$10.5 billion in 2025. Russian authorities registered an upsurge of cybercrime up to 80 per cent in 2022 as compared to 2021. The majority of these crimes were committed from abroad.

A substantial part of cross-border crimes is accounted for by fraud offences. In the Russian legal system, 'fraud' is defined as the stealing of other people's property or acquisition of the right to other people's property by deception or breach of trust.

This tendency is relevant both for actions committed on Russian soil against foreigners and for crimes committed from abroad. However, modern technologies (for instance, VPN connections) often make it impossible to pinpoint the exact location of a fraudster. Therefore, some crimes that appear to be cross-border may actually be committed by local citizens adept at using modern technologies.

For instance, a substantial number of frauds were committed by making calls from fake phone numbers (so called 'substitutive phone numbers'). A caller may cause any phone number to appear on a victim's phone screen (for example, a phone number of a bank or any other organisation). The purpose of this is to persuade a victim that the call is being made by a representative of their bank or even a police officer who is trying to prevent the stealing of the victim's assets. The aim of the fraudster is to receive personal information of the victim, including the CVV code of their credit card.

The number of such incidents motivated some Russian banks to create an antifraud system that operates in several CIS countries. Banks often encounter malicious and phishing mailings directed not only to depositors, but also to bank employees. It was reported that the system has helped to save billions of rubles from being stolen.

Such attacks and calls may be performed by individuals regardless of their location. In 2021 in Russia, more than

500,000 crimes were registered and committed with the use of information and telecommunication technologies or in the field of computer information.[1]

The employment of modern technologies in cross-border crimes makes it necessary for a lawyer to engage digital specialists for facilitating the process of gathering evidence of the deed. It becomes a general rule for law firms to carry out internal investigations of incidents jointly with IT specialists. This practice demonstrates high efficiency. For instance, in a series of internal investigations conducted regarding an alleged fraud, our team were able to obtain electronic correspondence with foreign entities that became a crucial piece of evidence.

Another important aspect of work that may be subcontracted to IT specialists is searching for digital traces of an offender. The personality of a cross-border culprit is intentionally hidden. Therefore, open sources of intelligence may discover a variety of vicarious evidence sufficient to establish the identity of the criminal. For instance, methods of intelligence helped our team to determine the name and location of a person involved in the theft of cryptocurrency from a foreign company. This information was necessary for preparing a criminal complaint.

The important role of digital evidence is recognised also by the state authorities which actively employ such specialists in investigations starting from the initial stages. For example, getting copies of all digital devices became a standard for every economic criminal case. They yield an abundance of information, even that which was deleted by the user.

Also frequent in Russia are cases where the assets of Russian companies are alienated on the basis of falsified evidence provided to Russian courts. This can be done by way of a corporate takeover of the company or establishment of a debt in the Russian courts. Despite the fact that the official court databases are mostly open to the public, in many cases the fraudsters exploit the efficiency of the Russian court procedure and the huge workload of Russian judges, obtaining judgments in the Russian courts in the absence of the defendant in two to three months and subsequently foreclosing on the assets of the company. The Russian courts are trying to fight such types of fraud. Recently the Supreme Court of the Russian Federation requested the lower courts to bring the state authorities (customs authorities, tax authorities, prosecutor's office) into suspicious cases. However, the number of such crimes didn't reduce. What is even more problematic is that such crimes are now conducted in many cases by big cross-border groups which use the falsified documents from other countries which are quite difficult to check in Russian courts.

The criminal law in Russia doesn't distinguish cross-border crime as a separate legal construction. It authorises investigative bodies to initiate a criminal case against foreign nationals and stateless persons who do not reside permanently in the Russian Federation and who have committed crimes outside the boundaries of the Russian Federation, where the crimes infringe upon the interests of the Russian Federation or a citizen of the Russian Federation. The Russian authorities should also investigate cases provided for by international agreements of the Russian Federation or other documents of an international nature containing obligations which are recognised by the Russian Federation in the sphere of the relations regulated by the Criminal Code and unless the foreign citizens and stateless persons not residing permanently in the Russian Federation have been convicted in a foreign state and are brought to criminal liability in the territory of the Russian Federation.

However, lawyers must take into account the specific features of cross-border crimes. With regard to fraud and other white-collar crimes, it is the duty of the lawyer to gather a pool of evidence sufficient for initiation of a criminal case.

The active role of consultants in searching for evidence derives from the features of the Russian criminal procedure. It consists of several separate stages, including a pre-investigative check, preliminary investigation and trial (that is, examining the merits of the case).

Each of the stages may be terminated without bringing the alleged offender to criminal liability. For instance, the criminal complaint by itself doesn't automatically lead to initiation of a criminal case in Russia as the pre-investigative check may be terminated with the investigator's decree to refuse to initiate the criminal case, which is a quite frequent outcome. The available statistics of the Ministry of Internal Affairs demonstrate that several years ago it was considering more than 11

million criminal applications per year, but only 1.7 million criminal cases were initiated.

The vast majority of criminal applications in Russia related to economic crimes do not result in prosecution. A lot of decisions not to initiate a criminal case were based on the grounds of there being a lack of the elements of the offence. However, the real ground for such refusals was absence of evidence presented in a form recognisable by state authorities. For instance, the investigator often isn't able to distinguish whether the disputable matter is of a civil or criminal nature. This problem is common for cross-border crimes in which the alienation of assets may be related to violation of a foreign law. In one such case, the offender provided his client (a foreign corporation) with false information, stating that the Russian legislation contained a provision that prohibited foreigners from owning immovable property. To circumvent this prohibition, the lawyer offered to register all the property rights in his name. According to his words, his status as a 'registered agent' deprived him of the right to alienate the assets. After receiving all the property rights, he swiftly sold the property. However, from the point of view of an outside observer, his actions could look like being of a civil nature. The attorney made all the misleading statements orally, during private conversations with his client. Therefore, there is no material evidence that could convince an investigator that a deception was committed.

It is even more relevant to cross-border crimes where the lack of easily obtainable evidence is a common obstacle for urgent initiation of a criminal case in Russia. Fraudsters are well informed about such difficulties and employ foreign accomplices as a self-protection measure. For example, illegal appropriation of title to assets is often done under a power of attorney by a person not aware of the illegal nature of their actions. The instigator of the crime issues such fake power of attorney abroad. Staying abroad prevents them from being caught and complicates the process of verification of the power of attorney.

Another factor that hinders efficient prosecution is the formalistic approach to the provided evidence adopted by investigative authorities. The law defines a list of admissible evidence which includes the evidence given by a suspect and an accused; the evidence of a victim and a witness; the conclusions and testimony of an expert; the conclusion and testimony of a specialist; demonstrative proof; records of the investigative and judicial actions; and other documents.

However, in practice an affidavit of a victim (witness) is not considered as evidence. It can be attached to the case file; however, the alleged victim (witness) is required to visit an investigator to be interrogated in person. The Russian authorities are not eager to accept interrogation using online technologies. In many cases it is quite difficult to organise such a personal visit of the victim or their representatives to Russia. This problem was especially crucial during COVID-19 restrictions on travelling in Russia and abroad.

A similar approach is usually taken in respect of digital evidence gathered and presented to the investigator by a third party or in respect of the copies of criminal case materials received from foreign jurisdictions.

For example, unknown entities presented to the court powers of attorney authorising them to represent the interests of a plaintiff residing in a Western European country. It followed from the circumstances of the case that the plaintiff's suit was initiated maliciously as an attempt to appropriate the victim's assets via a court judgment taken on the grounds of falsified evidence. During interrogation carried out by the foreign police, the plaintiff testified that the suit had been initiated groundlessly at the demand of his acquaintance. He also confessed that the powers of attorney were issued to an unknown person appointed by this acquaintance. Copies of those case files were transferred into Russia by foreign advocates. However, the investigator refused to initiate a criminal case based on the protocols of the interrogations composed by his foreign colleagues.

The legislation entitles an investigator to seek international cooperation in obtaining evidence from abroad. The process of this procedural action is complicated by strict regulation and bureaucratic delays. If it is necessary to carry out an interrogation, examination, seizure, search, court examination or other procedural actions stipulated by the Russian Criminal Procedure Code in the territory of a foreign state, the court, the public prosecutor, investigator, the head of an investigatory body or inquirer shall direct a request for performing these actions to the competent bodies or officials of the foreign state in conformity with an international treaty with the Russian Federation or with an international agreement or based upon the principle

of reciprocity. It is very important that a request cannot be filed at the stage of a pre-investigative check, which makes it impossible for an investigator to obtain evidence from abroad until the criminal proceedings are initiated.

Another actual problem stems from the dualism of the legal profession in Russia. The law does not prohibit a person lacking any legal qualification from rendering legal services (excluding criminal defence and some other specific forms of legal assistance). This ambiguity creates a favourable environment for committing fraud against foreign clients who are not aware of it. For instance, a foreign entity hired a private lawyer to recover a debt from a seller of goods through court procedures. The lawyer had been reporting to his client via email about his successful work and provided the copies of civil court judgments. For more than a year he had been receiving fees from the foreign entity. The fact of deception was discovered only when the entity hired another law firm for initiating the enforcement proceedings. It became clear that the lawyer had never filed a civil suit in the court, but had simply forged all the documents that were presented to the client.

Fraudsters actively use foreign entities' lack of information about national realities and their inability to verify the provided information. The following case can serve as an illustration. For example, a company from South Korea made several attempts to conclude a supply contract with major petroleum companies in Russia. All the offers were ignored or rejected by the producers. Before long, a representative of a third company contacted the foreign firm and stated that he was acting as an intermediary of one of the major companies. He declared that he was able to supply the required materials. After signing the contract, the representative of the intermediary company requested US$10,000 to be transferred to him for freighting a ship. The required sum was duly transferred to him. However, the navigation monitoring system showed that the ship moved to Europe instead of its planned destination in Eastern Asia. For an explanation, the intermediary company representative said that the ship had broken down and was headed to a dock for repairs and for that he required an additional US$10,000 for freighting another ship because, according to the contract with the shipping company, the previous payment would be returned in two months. After receiving the second payment, the so-called representative of the intermediary company stopped all communication with the foreign company.

Another common type of fraud is committed by local management against a foreign corporation. The roots of such crime are similar to that previously discussed: an inability to check all of the information provided by employees. The following case may serve as an illustration. A Chinese corporation had a subsidiary in Russia which was headed by a foreign manager as CEO. All other managerial positions (including CFO, COO, commercial director) were held by locals. Several years ago, one of the local managers informed the CEO that in order to continue receiving contracts from large Russian firms, they had to invent some sort of financial incentive for their managers. As direct payments from the foreign company's account could be regarded as corruption, the manager suggested creating an independent company which would receive payments for its services, cash them out and then use them as a source for paying illicit financial incentives. The new company would be able to render such services by unofficially subcontracting all the services to the employees of the foreign company. In other words, the foreign company paid fees to the firm, while all the services were rendered by its own staff using its own equipment. Even all the accounting was kept by the financial department of the foreign company. Eventually, this situation raised the suspicions of the compliance officer at the head office and he initiated an internal investigation. It helped to discover that the whole plan was devised by one of the local managers only to enrich himself through this scheme. In actual fact, absolutely no payments were made to the managers of large Russian firms; all accumulated money was simply stolen.

Therefore, the misrepresentation of information is often a common *modus operandi* of cross-border frauds. Several times in the course of internal investigations our white collar crime team was able to discover situations where the signs of embezzlement were concealed by shading factual details of business activity from the head office. For example, local management often overstated the real pricing of repairs or communal services. This let them conclude hugely overpriced contracts with affiliate contractors and share the excess monies. For example, a compliance department's attention was drawn to the activity of a local manager responsible for picking contractors for maintenance

and repairs of the premises of the company who hadn't taken sick leave or a vacation for five years. Analysis of the contracts which he supervised showed that each of them had been overpriced three- to five-fold. The contractual performer of the works and services acted as an intermediary, while works and services were performed by a sub-contractor. But the sub-contractor's fee was several times lower and all the excess income was appropriated by the intermediate contractor. It must be noted that, as in many other cases, our team discovered that local executives who weren't actually involved in this fraud did their best to hide this incriminating information from the head office, as they perceived it as a sign of their incompetence. This approach is one of the most conducive factors that facilitates the committal of cross-border crimes by local management against foreign head offices.

So, in summary, our experience demonstrates that the following factors simplify the commission of cross-border crimes:

- impossibility to verify the information provided by a contractor from abroad;
- a complicated procedure for gathering evidence from foreign jurisdictions;
- the application of cyber technologies;
- an excessive trust in local management;
- shortcomings of internal regulation in a company;
- a conflict of interest that prevents local executives from 'washing dirty linen in public'.

When providing legal services for foreign clients, our team usually advises them to follow some simple rules in order not to be deceived:

1. To avoid working with individual legal consultants abroad, because the law doesn't provide sufficient protection against abuse from their side. Only trusted and well-known firms should be hired for representation abroad.
2. To engage independent consultants for carrying out internal investigations separately from the local staff who may not be interested in uncovering the truth.
3. To avoid letting local managers pick subcontractors without a transparent procedure.
4. To implement internal policies in local offices in accordance with Russian labour legislation (which requires translation of the internal policies into Russian and notifying every employee against signature).
5. In case any assets are present in the local market, to monitor official court databases in order not to miss a maliciously taken legal action based on a forged power of attorney.
6. To implement antifraud digital technologies aimed at prevention of hacking and phishing mailing attacks.
7. To carry out training for personnel conducted by criminal law specialists experienced in internal investigation of fraudulent incidents in this particular jurisdiction.
8. To think in advance what evidence would you be able to present to the state authorities in the case a prospective counterpart commits an offence.
9. To analyse in advance whether it would be expedient to spend time and money on an attempt to initiate criminal proceedings that most likely would be waived according to local practice.

Notes

[1] http://crimestat.ru/analytics, 2021 report on the state of crime in Russia.

Maxim Alekseyev
Senior Partner, Head of Asia-Pacific Desk, ALRUD Law firm, Moscow

Maxim is the Co-founder, joint Senior Partner and Head of the Asia-Pacific Desk at ALRUD Law Firm. Maxim specialises in advising clients on international trading matters, regulatory and economic developments, domestic and international tax planning, strategic M&A, risk management, good governance, contentious investigations and dispute resolution.