Bulgaria

Angel Ganev
DGKV

Simeon Simeonov
DGKV

Lena Borislavova
DGKV

Over the past few years cases of fraud, especially those facilitated by the modern technical means of communication (cyber frauds), have increased dramatically. In the most common scenario they have a cross-border nature, where the fraud is committed abroad, but the misappropriated assets (usually cash) are transferred to different jurisdictions worldwide, including Bulgaria.

This article will dissect the most common and widely used scheme of cyber fraud and its repercussion on a local level, as well as the mechanisms and statutory underpinnings for recovery within the legal framework of Bulgaria. It should be pointed out, however, that the main purpose of the article is not to analyse fraud from a criminal law perspective, but to present the following steps and legal solutions for the effective reimbursement of the victim and recovery of the misappropriated funds. Therefore, the emphasis will be placed on the *civil* remedies rather than the criminal analysis.

The article also highlights some of the key challenges and problems faced by local practitioners in the process of asset tracing and recovery, as well as the most effective ways to deal with them. In conclusion, some recent trends and developments will be also discussed.

1 Important legal framework and statutory underpinnings to fraud, asset tracing and recovery schemes

A fraud has two main dimensions – a criminal and a civil one. The criminal dimension mainly deals with the detection and punishment of the offender, while the civil dimension is related to the recovery of misappropriated funds by their legitimate owner. Accordingly, there are two parallel and (relatively) independent layers of legislation in Bulgaria relating to the fraud: asset tracing and recovery.

As regards the criminal aspect, the main pieces of legislation are the *Criminal Code* (**CC**) (promulgated, State Gazette No. 26/2.04.1968, effective 1.05.1968), the *Criminal Procedure Code* (**CPC**) (promulgated, State Gazette No. 86/28.10.2005, effective 29.04.2006) and the *Anti-Money Laundering Measures Act* (**AMLMA**) (Promulgated, State Gazette No. 27/27.03.2018, amended SG No. 94/13.11.2018, effective 1.10.2018); while the civil law aspect is covered by the *Law on Obligations and Contracts* (**LOC**) (Promulgated, State Gazette No. 275/22.11.1950, effective 1.01.1951), the *Civil Procedure Code* (**CivPC**) (Promulgated, State Gazette No. 59/20.07.2007, effective 1.03.2008) and the *Law on Credit Institutions* (**LCI**) (Promulgated, State Gazette No. 59/21.07.2006, effective 1.01.2007).

From a criminal law perspective, the CC provides for the legal definition of "fraud" and some specific types, while the CPC provides for the legal procedure followed by the competent authorities (investigation, prosecution and criminal courts) to pursue and charge the offenders.

The AMLMA, together with the CC, provides for the legal notion of *money laundering*, determined as a form of *subsequent* criminal activity (a predicate offence) and usually preceded by misappropriation of assets/funds. Whenever there is only a suspicion of money laundering and/or proceeds of criminal activity are involved, the AMLMA provides for the possibility of imposing conservatory measures by the civil court upon an explicit request made by the prosecution authorities. In the context of a fraud, followed by a potential money laundering case, the imposition of conservatory measures secures the satisfaction of a future claim of the state for confiscation of the property – subject of money laundering – if the latter is established by virtue of a final court decision.

The applicable civil legislation, however, is more complex. Thus, the LOC and CivPC provide for the principal set of civil substantive and procedural legal tools, while the LCI provides for some auxiliary legislation which is also relevant to the steps and ways of recovering misappropriated funds. Some other laws could also be of significance in the aftermath of a fraud, depending on the case (e.g. the *Code of Private International Law*, the *Bar Act*, the *Law on Commerce*, etc.).

In terms of civil substantive law, the LOC provides for specific legal claims and remedies, based on the *unjust enrichment* doctrine, which is a focal point in recovery schemes. According to this doctrine, any person who received something without cause or for an unfulfilled or lapsed cause, must return it. In addition, when a person is enriched in any other way at the expense of another, the law imposes an obligation upon the recipient to make restitution. Under the relevant Bulgarian legislation, in the lack of legal relationship between the legitimate owner of the funds and the beneficiary (usually a part of the fraud scheme), the unjust enrichment doctrine serves as the only legal ground to claim the funds back from the recipient.

The LCI also contains some provisions, relevant to asset tracing and recovery schemes. More specifically, it establishes the notion of *bank secrecy*, which is especially important insofar as effective asset tracing is inevitably linked to the need of obtaining information from the local bank, especially during the first hours after commitment of a fraud. The LCI also provides for the possibility of lifting bank secrecy upon a court order in some specific cases.

As regards notable legal instruments, one of utmost importance is the *conservatory* (interim relief) measure, imposed by the civil courts under a procedure provided by the CivPC upon a request of the interested party, which aims at maintaining the *status quo* while the civil proceedings for recovery of the misappropriated funds are still pending. Another useful legal tool is the possibility for the claimant to request a *default judgment* (decision rendered *in absentia*), which is very common in fraud cases and subsequent civil actions, as fraudsters are normally not willing to reveal themselves to the public.

2 Case triage: main stages of fraud, asset tracing and recovery cases

2.1 Cyber fraud: Modus Operandi

In its very essence, fraud is a false representation of a matter of fact by false or misleading conduct, for the purpose of acquiring material benefit for the fraudster or for another, resulting in a legal injury of the victim.

In recent years, however, a specific type of fraud has become widely popular, namely *cyber* fraud, or a fraud committed and facilitated by the modern ways of communication, such as the Internet. Cyber fraud contains all the elements of an "ordinary" fraud, adding some complexity with regards to the mechanism of execution, facilitated by specific technical means and devices.

A case of cyber fraud normally evolves from hacking the email or the entire computer system of a person, quite often a large international company with multiple business and income streams and headquarters spread worldwide, where the communication channels are mainly maintained electronically (i.e. through non-personal communication). After a time of observation of the hacked email/system, the attackers usually create a fraudulent domain (a misspelt version of the original one).

In fact, attackers use a palette of techniques, such as deployment of websites with real-like URLs, re-creation of attachments to genuine e-mails, using specialised software to make them visually identical, etc. From the fraudulent domain, the hackers start sending emails to the potential victims (the so-called *phishing*). In some cases, the victims are wealthy individuals, which are defrauded using a similar scheme. The ultimate victim, in the most common scenario, is a legal entity and a business partner with particular obligations to the one whose email/computer system is hacked. The deceiving messages could be sent by hackers either from the original email account or from another, posing as the original. In fact, the victim is deceived to effect a payment, usually due in the ordinary course of business between the parties so that no doubt will arise about the grounds for payment. The only difference set by the fraudsters is the *destination* of payment, which is normally in a remote jurisdiction, with Bulgaria being quite often among these places, along with Hong Kong, China and Singapore; in some cases, these are also the places of business of the victims. If questions are raised by the victim about the sudden change of destination and beneficiary, it is justified by various reliable excuses – technical reasons, current audit, etc. Accordingly, after a certain period of processing, the victim pays the requested amount to the newly designated bank account, by which the fraud is committed. The victim and its trusted party (who inadvertently helped the scheme) have nothing to do but to discover the malicious activity sooner or later and (eventually) report the fraud to the competent police and investigation authorities at the place of commitment. Undoubtedly, such schemes are often facilitated by an *insider*; however, for the purposes of this article we have not conducted specific research to that point.

In a specific group of cases, the victim is a financial director or controller (or holds a similar position) of a large multinational company, who is deceived to believe that a senior staff member asked him or her to effect a payment to a particular destination offshore (either with or without reasonable justification). In some rare instances, the false instructions could be even received over the phone.

The typical local beneficiary of the funds is a *shell* company, established by the fraudsters (usually shortly before the attack) for the sole purpose of absorbing the misappropriated funds and retransfer them later. The fictitious representative/s of the company usually stay hidden and in general refrains from public appearance for understandable reasons.

Cyber fraud is more complex than ordinary fraud as it involves a large number of parties (besides the fraudsters), institutions (large companies, banks) and last, but not least, multiple remote jurisdictions which, as a rule, handle the fraud and its consequences in a very different legal manner. Traditionally, in cases of cyber fraud, the misappropriated funds amount to millions.

2.3 Counter actions and recovery of funds

Whenever a fraud is detected and reported, there are some basic critical steps to be taken in order to secure eventual recovery of the misappropriated funds or at least to limit the damages: (a) establishing a contact with the local bank (the beneficiary's bank where the funds were transferred) in order to obtain the fullest possible information about the transaction; (b) imposing conservatory measures with a view to retaining the funds (if any) in the bank account; and (c) commencing civil action in order to recover the funds.

a) Establishing a contact with the local bank

As it may be expected, once money has left the victim's account, it is transferred through multiple bank accounts in different jurisdictions, until final misappropriation by fraudsters. Logically, the local bank, which is the initial destination of the misappropriated funds, is the foremost source of information, especially with regard to the fundamental question as to whether the funds are still available in the bank at all. Other relevant information could be also obtained exclusively from the local bank, in particular details about the beneficiary (a future defendant in the civil action to be brought), the specific amount available, further

transfers, etc. If, unfortunately, at the time of the alert, the amount is no longer available in the designated account, the bank may at least provide the necessary information and documents to help chase the funds to other banks and jurisdictions. Lastly, the bank is the only proper source of information at this early stage about other potential freezing/injunction orders or other conservatory measures imposed by third parties (including measures imposed under the AMLMA upon the request of the prosecution authorities, see *Section 5* below) with regard to the same account and/or account holder, as they may significantly affect the recovery of the funds.

The most significant issue here is the reluctance of Bulgarian banks to provide information, mainly due to bank secrecy constraints and some other reasons. Bulgarian law does provide for an official legal definition of the term "bank secrecy". Pursuant to the LCI, the notion of bank secrecy embraces "*all facts and circumstances concerning balances and operations on accounts and deposits held by clients of the bank*". These include information on the person who opened and closed the account, the availability of funds, the transfers made within the country and abroad, dates and amounts, receiving accounts, the grounds for the transfers, as well as some other specific documents related to account balances and operations. On the other hand, the IBAN or any information related to bank loans or taxes are not covered by the definition of bank secrecy.

The protection granted to bank secrecy requires that this information is kept strictly confidential and is revealed to third parties, including law enforcement bodies, only in limited circumstances and in accordance with the procedural requirements described in the law. The main grounds on which bank secrecy can be revealed are provided for in LCI, but some sector-specific laws do contain additional grounds. With the 2015 amendments of the LCI the law maker accommodated for a better legal framework in the context of civil fraud litigation cases, envisaging explicitly that bank secrecy can be revealed on the basis of a *court order*, when this information is of relevance for the case pending before the court. This allows for shorter timelines for tracing the assets, as the court order is not subject to an independent appeal procedure and is immediately enforceable.

The local bank is important, but not the only source of information. As Bulgarian law does not recognise the so called "search order", as known in some other jurisdictions, the only thorough and legitimate search of a debtor's property status could be made by the bailiff within already commenced foreclosure proceedings upon an explicit creditor's request. Yet, some limited public sources of information are available to the creditors, so that enforcement against potential additional assets of the debtor is secured. The checks which are normally conducted include verifications with the Commercial Register and the Register of Non-profit Legal Entities, as well as the Real Estate Register, maintained with the Registry Agency of the Republic of Bulgaria, the Central Special Pledges Register, held with the Ministry of Justice and the Central Depository (the latter maintains a register of book-entry shares, any transactions thereof and special pledges over the latter). However, our practice shows that the local recipient of a fraudulent payment barely has other property than the misappropriated funds.

b) Imposition of conservatory measures

If the misappropriated funds are still available with the local bank, the next important step is to secure the *status quo* until final settlement of the fraud case and the following civil claim. While not mandatory from a legal perspective, this step is strongly recommended as it guarantees that the funds will remain blocked until the legitimate owner, having successfully set out its case before a court of law, proceeds to enforcement against the misappropriated funds. Interim measures under Bulgarian law include freezing of bank accounts, attachments of movable assets, receivables and real estate property of the debtor, shares or company participations, suspension of forcible execution proceedings, transactions, etc.

An interim measure may be requested either *prior* to or *along* with the initiation of a civil lawsuit. Where it is obtained prior to initiation of claim proceedings, the court determines a deadline by

which the creditor should file its statement of claim against the debtor; this term may not be longer than one month. In the event of a failure by the creditor to initiate litigation by this deadline, the court will revoke the interim measure. The principal purpose of the interim relief injunction is that the debtor's assets remain frozen and cannot be transferred for the time the statement of claim is under review. Thus, by the imposition of interim relief at an earlier stage, the creditor gains a higher chance to receive payment of its receivables.

c) Initiation of civil action for recovery of the funds

Under Bulgarian law, ownership title when it comes to amounts of money (in cash or that available in a bank account) is evidenced by the fact of possession in the sense that the person who possesses the amounts shall be deemed their legitimate owner unless proven before a court of law that such person received the amounts without *just cause*. In the case of a fraud this means that, having received the funds under its account, the beneficiary/ account holder shall be legally presumed the legitimate owner of the funds until proven otherwise before a court of law. The main implication of this (refutable) presumption is that, once the local account is officially *credited* with the funds, the bank may no longer unilaterally *withdraw* and return them to the sender (the defrauded party). Instead, the latter will have to resort to the civil court and to prove within ordinary civil proceedings that the funds were fraudulently wired from his or her account without legal cause whatsoever, and to seek a court decision ordering the account holder to pay the sum back. Therefore, the claim shall be based on the *unjust enrichment* doctrine and shall be brought before Bulgarian courts of law upon the statement that no legal relationship or other just cause underlies the fraudulent transfer and that the latter has been put into motion solely on the basis of a fraud committed against the victim.

In terms of timing, the decision of the first instance court is subject to appellate and cassation appeal, where the duration of the court proceedings may vary and often takes a long time which cannot be predicted, depending also on whether the parties appeal the court decisions on each instance. Based on our experience, the approximate timing for each instance may vary from approximately one to three years. Another important factor influencing the duration of judicial proceedings is whether the conditions for the claimant to request a default judgment are met. As already pointed out, it is very rare for the defendant to actively participate and defend in such cases. In the normal scenario, the defendant (the local beneficiary) does not react and no one reveals in the court. In this case, the CivPC provides for the possibility of rendering decision *in absentia* (a default judgment), if specific procedural prerequisites are met. The procedural conditions for the court to follow are: (i) the defendant has not submitted a statement of response within the statutory deadline; (ii) the defendant does not attend the first court hearing; (iii) the defendant has not declared explicitly that he wishes the case to be reviewed in his absence; and (iv) the claim is apparently founded. If the court favours the request for a default judgment, the latter enters into force *immediately* and significantly facilitates further recovery of the funds. Based on a positive judgment, entered into force, the creditor may obtain a writ of execution and launch foreclosure proceedings for recollection of the misappropriated funds.

3 Parallel proceedings: a combined civil and criminal approach

It is a common practice in Bulgaria that criminal and civil proceedings are initiated and pending simultaneously. As each of them has different purpose and development, they are relatively independent. Criminal proceedings are aimed at punishment of the offenders while the main goal of the civil proceedings is recovery of the funds. Although Bulgarian law allows the filing and review of a civil claim within criminal proceedings, due to a number of procedural specifics and time constraints, this option is either not applicable or not recommended.

In the most common scenario, the banks (both the local and the corresponding ones abroad) are the first to face signs of a fraud. Pursuant to the AMLMA, once a suspicious transaction (wire transfer) is detected, Bulgarian banks are obliged to report the case to the prosecution authorities and the director of the Financial Intelligence Directorate of the Bulgarian State Agency for National Security (SANS), which is normally followed by the initiation of a *criminal case* in the form of investigation proceedings, conducted by the competent authorities. Pursuant to the CPC, a criminal investigation (the first phase of a criminal case) might be commenced either upon a signal/warning letter, filed by any third person or *ex officio*, at the sole discretion of the prosecution authorities, if there is any available information concerning a crime committed. Importantly, in a standard case, criminal proceedings would be commenced for a money laundering crime rather than a fraud (please see *Section 5* below for the issues associated with this approach). Usually, at

the same time, the victim seeks legal assistance in the relevant jurisdiction where the money was transferred in an attempt to recover it.

Usually, in practice, a criminal proceeding will significantly hinder the civil one, mainly due to the fact that the prosecution in Bulgaria is slow, highly ineffective and suffers from a number of other shortcomings. On the other hand, as the criminal proceedings often precede the initiation of a civil case, the imposition of protective measures by prosecution authorities may be useful at the very beginning of a fraud case as it could potentially protect the money until further imposition of conservatory measures by the potential claimant. This is necessary as the interim measures, imposed by the prosecution authorities, could be lifted at any time without the knowledge and consent of the victim, upon the sole discretion of the prosecution authorities.

4 Key challenges

4.1 Time and information constraints

Needless to say, a key challenge in international fraud cases is the *time* factor. The electronic means of communication make wire transfers, transmission of messages, etc., happen literally in seconds. Very often, at the time the fraud is discovered, fraudsters have already managed to draw out the misappropriated funds. In such scenario, the options for an adequate response on a local level are very limited as the availability of the funds is an absolute precondition for any further recovery actions. Therefore, the connection with the local bank, the supply of sufficient information and the imposition of protective measures should happen literally within a day or two so that the victim has a bare chance of recovering the funds.

Another significant constraint is the lack of *information* at the time of receiving the first alert from the client. A lot of details are needed in order to initiate a viable action plan for recovery. As a first source of information, banks are very often reluctant to provide details as this could easily be viewed a breach of bank secrecy. In addition, legal practitioners are not equally positioned compared to the state investigation bodies which may, almost without limitation, receive information from all public and private institutions and other sources, including banks. Even more difficult, if not impossible, is the receiving of information from the prosecution authorities themselves, which, due to the specifics of criminal cases and for other reasons, firmly refuse to provide information, even to the victim. In such an adverse environment, the building of good relationships with local banks is necessary for legal practitioners in order to achieve successful assistance.

4.2 Parallel criminal proceedings and interim measures imposed under the AMLMA

Another key challenge in the process of recovering misappropriated funds is the pending criminal proceedings (usually in the form of preliminary investigation) at the time of starting recovery actions. Upon a signal for a suspicious bank transaction, the director of the State Agency for National Security (SANS) may issue a written order suspending it, in order to analyse the said operation or transaction and, eventually, confirm the suspicion. After carrying out the abovementioned analysis, the director shall inform the competent prosecution authorities, providing the necessary information. Following this information, the prosecutor may file to the competent

court a motion for imposition of conservatory measures, which usually (but not necessarily) take the form of attachment of immovable property or bank account/s. The intended purpose of such conservatory measures is to prevent transfers of money, acquired as a result of unlawful activity, so that the financial security of the Member States is secured. Pursuant to the binding case law of the Bulgarian courts, the prosecution authorities are entitled to request imposition and the court may favour such request even without the need of existence of a launched criminal investigation or a court procedure. The problem is that, due to the wide scope and legal possibilities of the AMLMA, the authorities tend to qualify any suspicious transaction (including obvious cases of fraud) as a money laundering case and to launch a criminal investigation on that ground. At the same time, the practice shows that such money laundering criminal cases are barely pursued by the authorities once they are initiated and the conservatory measures are imposed. Instead, in most of the cases, they are (unofficially) suspended immediately after initiation and no actual investigation activity is undertaken whatsoever. Since the pending criminal proceedings are the only ground for the validity of the attachment, until their official termination the attachment exists and hinders recollection of the funds by the victim (under the applicable law, attachments are executed in the order of their imposition). The only legal solution in such scenario is challenging the court ruling ordering the interim measure imposed by prosecution authorities; however, it may take considerable amount of time and struggle. The legal tool is a request for revocation of the conservatory measure, filed to the civil court which has imposed the attachment. It is only the civil court which deals with the matters related to the conservatory measures imposed under the AMLMA. Only the latter has the powers to reverse its own previous ruling for imposition and to lift the attachment. The entire process of filing a request before the court for lifting of the attachment and potential appeal in case the first instance court does not favour the request, may take roughly three to six months. If the appellate court upholds a potential negative court ruling, a request for lifting may be filed anew.

5 Cross-jurisdictional mechanisms: issues and solutions in recent times

5.1 Relevant EU legal tools and mechanisms

EU legislation creates a number of legal tools which are also relevant to cross-border fraud cases. From a criminal law perspective, EU legislation guarantees that criminals can be pursued across borders and repatriated, thanks to the *European arrest warrant*. Judicial authorities cooperate through the European Union's Judicial Cooperation Unit (Eurojust) to ensure legal decisions made in one EU country are recognised and implemented in any other EU country. The EU also works to improve internal security and to have a coherent approach towards organised crimes. This includes taking action against organised criminals and helping national police forces work better together through the European Police Office (Europol).

In addition, the European Parliament and Council have adopted a regulation on the mutual recognition of freezing orders and confiscation orders (the new legal framework (Regulation (EU) 2018/1805) was published in the Official Journal of the EU of 28 November 2018 (O.J. L 303/1)). It establishes rules for the recognition and execution by a Member State of a freezing order issued by the judicial authority of another EU country in a *criminal* proceeding. This could either be a freezing order issued for the purpose of securing evidence in a criminal proceeding, or a subsequent confiscation order to permanently stop offenders from benefiting from their criminal conduct and prevent criminal property from being laundered or reinvested, potentially fuelling further criminality.

On a *civil* law level, a notable legal tool is *Regulation (EU) No 655/2014 of the European Parliament and of the Council of 15 May 2014 establishing a European Account Preservation Order procedure* to facilitate cross-border debt recovery in civil and commercial matters. The regulation establishes a unified procedure enabling a creditor to obtain a European account preservation order which prevents the subsequent enforcement of the creditor's claim from being jeopardised through the transfer or withdrawal of funds up to the amount specified in the order. However, in most cyber fraud cases, the fraud concerns persons located and funds originating from countries *outside* the EU. Thus, the regulation provided by the private international law and some international treaties shall also be applicable. For instance, pursuant to the Bulgarian Code of International Private Law (promulgated, State Gazette No. 42/17.05.2005), Bulgarian courts of law have jurisdiction to *secure* a claim over which they do not have international jurisdiction, if the subject matter of the conservatory measure is situated in Bulgaria and the anticipated judgment of the foreign court could be recognised and enforced in Bulgaria. The specific procedure for applying and obtaining a conservatory measure is again regulated by the CivPC (please see *Section 3.3(b)* above).

5.2 Unofficial channels of information and cooperation

Speaking about cross-jurisdictional mechanisms, the unofficial channels of information and cooperation could be in many cases very effective. As an example, the information exchanged through the corresponding international banks could be obtained long before the victim knew about the fraud and the competent authorities have commenced investigation. Another effective instrument, which is increasingly used in such cases, is the *private* criminal investigation, assisted by proper technical experts. The investigative and *digital* forensic support provided by them could be often a viable option for the victim in the process of obtaining timely information and asset tracing.

6 Technological advancements and their influence on fraud, asset tracing and recovery

The growing role of the Internet and the new technologies in the context of cybercrimes and civil fraud is well recognised. On the one side, new technologies have drastically changed the ways of doing business; methods of communication between companies have shifted from traditional face-to-face interactions to that of email and other modern forms of communications, payments through electronic devices and different software applications are even more common than traditional payment methods, etc. These developments have increased the opportunities for fraud, which has inevitably increased the number of actual fraud cases and their diversity in relation to the mechanism of commitment.

On the other hand, however, new technologies are increasingly used to prevent and detect fraudulent transcations and behaviour. Improved system security, automated data analysis, data audit and risk assessment softwares, encryption, data mining, two-step verifications, and others serve for better and more efficient fraud detection and subsequent investigations. Nevertheless, the most crucial factor for effective recollection of the fraudulently acquired funds remains the fast intervention of the law enforcement bodies and legal practitioners involved.

7 Recent developments and other impacting factors

One of the most recent and important developments in the field of fraud, asset tracing and recovery is the EU proposal from the beginning of 2019 for a directive on combating fraud and counterfeiting of non-cash means of payment (including electronic wallets, mobile payments and virtual currencies). The directive is aimed at upgrading and modernising the existing rules in the fight against fraud in the EU Single Market. Some of the main provisions concern harmonised definitions of common online crime offences, such as hacking a victim's computer or phishing; as well as harmonised rules for penalties and clarifications of the scope of jurisdiction to ensure cross-border fraud is tackled more effectively.

Another recent development on a *local* level is the inclusion of computer-related crimes and frauds like phishing, other forms of social engineering and fake cryptocurrencies in the National Risk Assessment with respect to money laundering activities, published by the SANS on 09.01.2020 (available in Bulgarian at https://www.dans.bg/

bg/msip-091209-menu-bul/rezultatirisk-mitem-bg). SANS has allocated a medium risk level (out of four levels of risks, indicated in the document) for these computer crimes on the territory of Bulgaria and has highlighted the existing difficulties for asset recovery. If a business, obliged to comply with the anti-money laundering legislation, establishes that they are exposed to this type and level of risk, they have to undertake appropriate measures and internal procedures to combat money laundering based on cybercrimes and civil fraud cases.

Angel Ganev heads the Bankruptcy & Insolvency and Litigation & Arbitration Practice Group at DGKV. His practice group includes more than 20 litigators specialising in complex commercial disputes and insolvency cases with a strong cross-border focus, as well as highly regarded asset recovery and anti-fraud subgroup. He is an experienced litigator with more than 18 years' practice in international arbitration, commercial litigation, and cross-border insolvency. Angel also acts on a regular basis as an arbitrator including in arbitration proceedings administrated by the ICC Court of Arbitration.

He also provides legal counsel to significant foreign investors on complex issues with regard to competence of courts, applicable law and recognition and enforcement of court judgments across borders.

Professional Memberships: Sofia Bar; IBA; FraudNet; INSOL Europe; Member Chartered Institute of Arbitrators.

angel.ganev@dgkv.com

Simeon Simeonov is a Senior Associate and a proactive member of the litigation team, participating in the cornerstone disputes led by the law firm. He specialises in commercial litigation and insolvency. His professional experience encompasses civil and commercial litigation, including representation in a number of debt recovery court proceedings and public procurement procedures, consultations on mortgage secured bank loans, real estate law, etc.

simeon.simeonov@dgkv.com

Lena Borislavova is an Associate at DGKV. A graduate of the Master's programme (LL.M.) in Law at Harvard Law School, USA. She specialises in mergers and acquisitions, commercial law, corporate governance and foreign investments. Lena assists major international companies in staying up to date with the latest local regulatory changes and applying the best practices for doing business in Bulgaria.

Lena is recognised in the 2018 European edition of Forbes' 30 Under 30 list of top young lawyers and policymakers.

lena.borislavova@dgkv.com