POPOVICI NIȚU STOICA & ASOCIAȚII
Attorneys at Law

Published by Financier Worldwide Ltd
©2020 Financier Worldwide Ltd. All rights reserved.
Permission to use this reprint has been granted by the publisher.

TALKINGPOINT June 2020

AML in Romania

FW discusses AML in Romania with Irina Petrila and Frederica Taccogna at FTI Consulting and Alexandru Ambrozie at Popovici Nitu Stoica & Asociatii.

THE PANELLISTS

Irina Petrila
Senior Director
FTI Consulting
T: +44 (0)7976 861 523
E: irina.petrila@fticonsulting.com

Irina Petrila is a senior director in FTI's financial services practice, based in London. Prior to this role, she worked for several large investment banks, including Deutsche Bank, Credit Suisse and Barclays, where she performed various roles within compliance and anti-money laundering (AML) and counter terrorist financing (CTF) operations. She has also led workstreams and projects ensuring effective enhancements of existing financial crime frameworks for firms undergoing both regulatory investigations and ad-hoc remediation programmes.

Federica Taccogna
Senior Managing Director
FTI Consulting
T: +44 (0)20 3319 5651
E: federica.taccogna@fticonsulting.com

Federica Taccogna is a senior member in the financial services practice of FTI in London and assists the senior management and boards of a wide range of financial services clients and regulators globally advising on investigating and remediating regulatory and financial crime matters. Ms Taccogna has previously held senior risk and compliance positions in the banking sector and has experience of working on complex market abuse and conduct matters.

Alexandru Ambrozie
Partner
Popovici Nitu Stoica & Asociatii
T: +40 (21) 317 7919
E: alexandru.ambrozie@pnsa.ro

Alexandru Ambrozie leads the white-collar compliance and defence group, and is also co-head of the banking & finance, capital markets and tax practices at Popovici Nitu Stoica & Asociatii. He has extensive experience in tax, banking & finance and capital markets and public procurement, assisting leading financial institutions, private equity firms and other high-profile companies. His in-depth understanding of fiscal, public procurement, EU funds and other regulatory practices enables him to lead the defence on numerous white-collar criminal and compliance investigations, representing clients in regulatory and criminal investigations carried out by various prosecution and administrative authorities.

FW: To what extent is financial crime growing in frequency and complexity? How would you summarise recent trends in Romania?

Petrila: As economies continue to grow and technology reaches new levels of complexity, financial crime is becoming more sophisticated, posing one of the biggest risks to global markets and society. Developments in FinTech, virtual currencies and blockchain have made combating money laundering and terrorist financing a moving target – which firms across the world are struggling to keep pace with. In the last decade, Romania has been facing a number of challenges relating to anti-money laundering (AML) and counter terrorist financing (CTF) deficiencies, political instability and corruption, while still focusing on fulfilling the relevant criteria for adopting the euro currency in 2024. In 2019, Romania addressed one of the challenges and enhanced its AML/CTF framework, by transposing the European Union's Fourth Anti-Money Laundering Directive (4AMLD) into legislation. The country is yet to implement the Fifth Anti-Money Laundering Directive (5AMLD) and has been formally notified by the European Commission to do so in February 2020.

Ambrozie: There has been a substantial increase, at least in frequency, of financial crime. According to the Activity Report for 2019 issued by the Public Ministry, in 2019 the number of cases brought to court for purely money laundering offences increased by about 36 percent to 292 cases, compared to the previous year when there were 215 cases, and by about 450 percent compared to 2010. The number of purely money laundering offences is still very low, but the growing trend and the likelihood of significantly more money laundering investigations are clear when looking at the number of other financial cases usually linked to money laundering – 1300 tax evasion cases in 2019 – and the estimation regarding the Romanian shadow economy ranging from 28 to 45 percent. The digitalisation of the financial services industry, the increasing number of FinTech solutions and the increasing number of cyber crimes are all factors that will probably contribute to the growing trend of money laundering. Money laundering-related risks affect not only financial institutions, but also investors and the M&A landscape in Romania. Although the primary focus remains on the quality of assets, buyers pay significantly more attention to the target's compliance programme, which includes AML and anti-corruption policies. Bearing in mind that the successor's liabilities, which were not previously identified and mitigated, become the liabilities of the buyer, it is highly recommended to perform robust AML

and anti-bribery & corruption (ABC) due diligence prior to the transaction.

FW: Could you outline some of the key legal and regulatory developments in Romania affecting anti-money laundering (AML)? Do companies need to accept that they now operate under heightened scrutiny, and react accordingly?

Ambrozie: Romanian reporting entities should rapidly learn how to effectively ride this regulatory AML avalanche that arrived in the summer of 2019 and continues in 2020. First, Romania has transposed 4AMLD, albeit with a considerable delay. The main changes brought by the new legal framework cover the following main topics. First, a broadened scope of the reporting entities, which now includes the gambling sector too. Second, reducing the threshold for cash payments to the equivalent of €10,000. Third, mandatory application of risk-based assessment. Fourth, mandatory application of simplified, standard or enhanced due diligence on an individual assessment basis. Fifth, the creation of a national ultimate beneficial owner (UBO) register. Finally, increased sanctions – up to 10 percent of the total annual turnover for legal entities. Further, the National Bank of Romania (NBR) and the Securities Commission issued separate, enhanced regulations applicable to the entities they each supervise. In addition, regulatory authorities increased their onsite and offsite supervisory actions in order to evaluate to what extent the reporting entities are complying with AML requirements. Only one month after the term for compliance with the new AML requirements, the NBR requested that financial institutions send their updated AML procedures and policies for review. Moreover, at the beginning of this year, the AML Office issued the secondary norms to the AML law, which significantly extended the types of companies that should comply with the AML requirements. These include business and other management consultancy activities, activities of holding companies, and renting and operating real estate by owners or landlords. And very recently, in April, the Ministry of Public Finances published a draft law which would fully transpose 5AMLD. The new upcoming regulation establishes new rules for the authorisation of exchange services between virtual currency and fiat currency and custodian wallet services, and extends its scope to art dealers, real estate agents and real estate developers.

Taccogna: In July 2019, Romania transposed 4AMLD into law – Law 129/2019 regarding the prevention and combating of money laundering and terrorist financing. This was followed by a government ordinance in January 2020 – Ordinance 102/2020 – setting out the norms for applying the provisions of Law 129/2019. The ordinance was approved by the president of the National Office for Prevention and Control of Money Laundering (ONPCSB), which acts as the Romanian Financial Intelligence Unit (FIU). While ONPCSB focuses on supervising firms which do not fall under the supervision of other Romanian authorities, the NBR acts as the country's prudential supervisor. With the adoption of the new legislative measures, firms will have to update their AML/CTF frameworks to ensure full adherence to the new requirements. Some firms in Romania are subsidiaries and branches of other EU companies where 4AMLD has already been implemented. Therefore, for some of these entities the changes may not come as a surprise, as their parent companies will have already adjusted their AML/CTF frameworks.

FW: How would you describe AML monitoring and enforcement activity in Romania? What problems may arise for multinational companies as a result of the extraterritorial reach of certain laws, and greater collaboration between national agencies?

Petrila: Although in previous years monitoring and enforcement in Romania was primarily focused on fraud and corruption, the adoption of Law 129/2019 extended the focus to include monitoring for potential money laundering and terrorist financing activities. Collaboration between authorities and prudential supervisors will continue to increase, ensuring a robust AML/CTF supervisory approach for Romania. The NBR, since 2019, has investigated 17 banks on suspicion of opening personal and corporate accounts where the underlying transactions did not have a rational purpose. As a result, the Directorate for Investigating Organized Crime and Terrorism (DIICOT) opened a criminal case on the suspicion that at least one of these banks was involved in money laundering. This is an indicator the regulator has turned up the heat on AML/CTF enforcement. As such, both local as well as multinational firms should prepare for scrutiny and ensure that their AML/CTF frameworks do not lack the adequate enhancements. Other difficulties faced by firms will include adhering to laws set out by the Romanian government, as well as laws set out by foreign governments, where these laws are super-equivalent. Firms will have to analyse and consider adequate measures to meet both local and extraterritorial requirements.

> "COLLABORATION BETWEEN AUTHORITIES AND PRUDENTIAL SUPERVISORS WILL CONTINUE TO INCREASE, ENSURING A ROBUST AML/CTF SUPERVISORY APPROACH FOR ROMANIA."
>
> IRINA PETRILA
> FTI Consulting

Ambrozie: AML and sanctions enforcement are a top priority, according to both the AML Office and the Public Ministry. Multinational companies are

under tighter scrutiny in Romania, not only because of the extraterritorial reach of certain laws, which is visible in Romania too, but also because Romanian prosecution and financial authorities are significantly more prepared to deal with white-collar crime than they were 10 years ago. For example, early this year, an official of the National Bank of Romania stated that 16 to 17 banks were involved in a rather awkward transaction related to money laundering, which led to the opening of a criminal investigation by Romanian prosecutors. According to the statements, although the frauds were external, Romanian credit institutions failed to apply robust customer due diligence on their clients. This is a serious example of the vision of Romanian authorities. Regarding cooperation between national agencies, it is well known that Romanian authorities cooperate in many cross-border investigations, not only cyber frauds related, but also on corruption and money laundering. But what is less well-known is that many of these investigations are started by Romanian authorities which, in recent years and with the support of host-country authorities, have raided headquarters located in Austria, France and Germany, to name a few, in relation to the activities of various multinational companies in Romania. In addition, the Romanian AML Office received 251 information requests from foreign FIUs and 9040 suspicious activity reports (SARs) in the process of cooperating with FIUs in 2018. All in all, multinational companies should be aware that Romania is actively cooperating with foreign enforcement agencies and increasingly investigating the financial activity of multinational companies.

> FIRMS SHOULD ALSO FOCUS ON IMPLEMENTING ROBUST TRANSACTION MONITORING AND REAL TIME PAYMENT SCREENING SYSTEMS AS PART OF THEIR AML/CTF FRAMEWORK ENHANCEMENTS.
>
> FEDERICA TACCOGNA
> FTI Consulting

FW: What steps should companies operating in Romania take to ensure adequate processes, programmes and policies are in place to support AML?

Ambrozie: An effective AML programme should be based on an annual risk-assessment aimed at identifying money laundering and terrorist financing risk factors to which the company is exposed. Such an evaluation should also establish the procedures and policies in place to mitigate money laundering and terrorist financing exposure. Well-designed AML policies should contain the following. First, a risk-based procedure for customer due diligence. Two, ongoing monitoring of clients and clients' transactions, so that the company has a current understanding of a client's risk profile. Three, sanction screening procedures to ensure compliance with international sanctions orders. Fourth, effective training of employees. Fifth, direct and effective involvement of senior management in the implementation of AML policies. Sixth, well-established procedures to report suspicious activity. Seventh, heightened awareness of the specific money laundering and terrorist financing risk factors to which the company is exposed. Eighth, effective whistleblowing channels and procedures. Finally, recordkeeping rules. The aim of such a programme is to enable companies to prove that their AML policies and procedures are in line with the risk profile of the company and capable of preventing fraud and money laundering and terrorist financing. Considering the new AML requirements, financial institutions are expected to invest heavily in AML compliance. Besides constant revision of their AML policies, this also implies an increased number of AML and Know Your Client (KYC) specialists. What we currently see is that implementation of AML requirements is fragmented as part of employees' onboarding procedure, ongoing monitoring, double-checking initial checks, and so on. Unfortunately, this strategy erodes the effectiveness of AML policies, as it involves employees from too many departments, inconsistent standards for customer due diligence and a lot of suspicious activity false alerts. In light of this, financial institutions in particular should invest more in technology and data analytics platforms.

Taccogna: Local and foreign firms in Romania should focus on updating their current AML/CTF framework to ensure adherence to Law 129/2019. Among the additional measures that firms will have to consider are the need to have a defined risk appetite framework supported by a business-wide risk assessment to understand their AML/CTF risks and the effectiveness of their controls. Firms should also focus on implementing robust transaction monitoring and real time payment screening systems as part of their AML/CTF framework enhancements. Internal policies and procedures will also have to be updated to reflect the new requirements. Therefore, staff will have to be trained to ensure that the new measures are applied both correctly and consistently across the firm. Firms must also consider whether their compliance monitoring function is robust enough to adequately address any compliance deficiencies, while simultaneously performing horizon scanning to identify upcoming regulatory developments. In response to an ever-changing regulatory landscape, companies must be prepared to overhaul legacy systems and take remedial actions with respect to their existing customer accounts.

FW: In what ways can companies utilise technology to help manage risks arising from AML?

Petrila: Technology can be a huge asset to a firm's AML/CTF framework, saving time and costs by making processes more

efficient. To use transaction monitoring systems as an example, with the appropriate calibration of rules and scenarios, such tools can effectively identify suspicious transactions, potential indicators of money laundering and terrorist financing, and transactions in breach of the firm's risk appetite. This can be achieved with good quality data. However, where the data is poor in quality and the rules and scenarios have not been correctly determined and calibrated, this can place a significant strain on staff managing the number of alerts generated. Alternatively, poorly calibrated systems could improperly reduce the number of alerts generated, which increases the likelihood of missing potentially genuine money laundering and terrorist financing threats due to lack of human supervision and input.

Ambrozie: Financial institutions are already obliged to develop and implement adequate and efficient IT systems as part of their AML programmes and control mechanisms. Such IT systems should cover the entire activity of the company, the whole client portfolio and all transactions that have associated money laundering and terrorist financing risks. The IT programme should be able to monitor, collect and assess data and information related to clients and transactions and to facilitate adequate internal and external reports. However, we have not yet seen a broad shift from traditional methods to technology-based compliance. Even if the human factor should remain an important part of AML compliance, integrating tailored IT systems – such as investigations tools and alert engines, data-aggregation platforms and machine learning (ML) – into the day-to-day business should ensure more efficient compliance.

FW: What overall advice would you give to organisations in terms of marrying technology with protocols, to enhance the efficiency of their AML capabilities and allow them to detect unusual behaviour and identify red flags?

Ambrozie: Whereas financial institutions are at least familiar with the idea of implementing technology-based compliance, for other reporting entities, using technology to identify clients and monitor transactions and client behaviour is still a novelty. They have to speed up the pace, otherwise significant fines will come into play. In the case of companies with a large volume of clients and transactions in countries with which they are unfamiliar, they should focus on implementing innovative IT systems in order to detect, assess, manage and prevent money laundering and terrorist financing risks. Such systems will help companies reduce the number of false positives, reduce human error, enable them to aggregate data from public sources, news, data providers and litigation portals, offer reliable quantitative metrics to asses money laundering and terrorist financing risk across related relevant factors, ensure more consistent information for filling SARs, enable an automatic risk scoring and up-to-date client risk profile, and offer flexibility for a risk-based approach, even in the case of regulatory changes or changes in the behaviour of clients due to general measures unrelated to the client, such as the 'perfect storm' created by the coronavirus (COVID-19) pandemic. Small companies or companies which do not have associated medium or high money laundering and terrorist financing risks should consider implementing technology-based systems only after evaluating their money laundering and terrorist financing risk profile, the type of available data and its support format, and the costs related to periodic review and adequate training for employees. It is important to note that a standalone IT system or an AML programme which is not tailored to the specifics and risk profile of the company is not particularly relevant for compliance purposes as it does not properly detect, assess and mitigate money laundering and terrorist financing risks, leaving the company to face the exact risk exposure it would have if it did not have any kind of AML policies or control mechanisms in place.

Taccogna: By implementing the correct technology, firms can manage the new requirements imposed by recent laws and regulations. Technology can also enable firms to identify transactional patterns, suspicious activities and unusual behaviour, making it easier to uncover potential money laundering and terrorist financing risks and report them accordingly. Marrying technology with protocols can enhance efficiency in terms of AML/CTF. In the UK, for example, the Financial Conduct Authority (FCA) promotes the concept of using technology to support AML/CTF compliance, especially with respect to customer due diligence and ongoing monitoring of business relationships.

> "AN EFFECTIVE AML PROGRAMME SHOULD BE BASED ON AN ANNUAL RISK-ASSESSMENT AIMED AT IDENTIFYING MONEY LAUNDERING AND TERRORIST FINANCING RISK FACTORS TO WHICH THE COMPANY IS EXPOSED."
>
> ALEXANDRU AMBROZIE
> Popovici Nitu Stoica & Asociatii

FW: Going forward, do you expect the risks posed by money laundering in Romania to increase over time? Do companies need to continually improve their system in order to deal with current and emerging threats?

Petrila: The risks posed by money laundering and terrorist financing in Romania will increase over time if insufficient progress is made with respect

to tackling the risk of financial crime and, implicitly, money laundering and terrorist financing. Firms need to adhere to the new AML/CTF legislative frameworks and ensure that their systems and controls are reviewed and updated on a regular basis. By doing so, firms will protect their reputation. If a firm's integrity is damaged, this can limit direct investment, and the willingness of other businesses to continue to trade with it. Authorities must ensure that they efficiently and effectively supervise the industry, while supporting, not stifling, economic development. It is crucial, in this, that authorities work together, as well as with international stakeholders, to better understand and combat money laundering and terrorist financing.

Ambrozie: Despite the constant and significant amounts of money and time invested in AML compliance, we regularly hear about big scandals involving money laundering and terrorist financing offences, highlighting that criminals regularly seek, and often manage, to bypass AML procedures, policies and control mechanisms put in place by financial institutions. This is all the more applicable to Romania. The complexity and sophistication of cyber crime, fraud and money laundering and terrorist financing offences emphasise the idea that even a robust and tailored AML programme is in fact a net with some holes in it, which enables fraudsters to circumvent some controls. Thus, even a small hole in the compliance net is able to sink, or to some extent make irrelevant, efforts to implement an AML programme. All in all, companies should harness a strong compliance culture by involving experienced people in AML programmes, as well as utilising appropriate IT systems capable of allowing them to actively and efficiently fight against money laundering and terrorist financing. ■

This article first appeared in the June 2020 issue of Financier Worldwide magazine. Permission to use this reprint has been granted by the publisher. © 2020 Financier Worldwide Limited.

FINANCIER WORLDWIDE corporatefinanceintelligence