Covid-19 and the Changing Money Laundering and Terrorist Financing Risk Landscape

Remarks by David Lewis at the MENA Regtech Virtual Executive Boardroom

18 January 2021

As delivered

Thank you. It's great to join you today for this important discussion. The pandemic is a challenge for us all but it also presents opportunities – both for criminals and for us. I will talk about both. But my main message is that the pandemic has been and should be a catalyst for the adoption of RegTech, and more efficient and effective AML/CFT measures.

The MENA region, like the rest of the world, is fighting the spread of the virus.

The money laundering and terrorist financing risks that have emerged and the resilience of national regimes to combat them vary significantly from country to country. This is partially due to different approaches to confinement, social distancing measures, and available infrastructure. However, one thing is consistent, the criminal threat. Never has this been so dynamic.

In May, the FATF published its first report on the impact of COVID-19 on the global money laundering and terrorist financing landscape. Since then, we have continued to monitor developments and last month we published another update, which you can find on the FATF website. From our global network of over 200 countries, we have gathered examples of criminals profiting from the pandemic. These include fraudulent access to and diversion of government aid, to the impersonation of government officials, fake fundraising campaigns and the counterfeiting of medical supplies, and now vaccines.

As an example in the region, the Tunisia financial intelligence unit reported the misappropriation of aid given by a foreign country to its citizens stranded in Tunisia due to the pandemic. Six transfers, totalling USD 2.5 million, were meant to cover accommodation, medicines, supplies and COVID-19 tests but instead disappeared to a shell company. The suspect's assets have been frozen while the case is ongoing, but it demonstrates criminals' determination to exploit this global crisis. Cases such as this are sadly not unique. Much needed financial support is disappearing into the hands of criminals at a time when citizens, health services and communities need it most.

Criminals have used the sharp increase in online activity to develop targeted malware campaigns, ransomware or phishing attacks with fake links to government stimulus packages, infection rate maps and websites selling personal protection supplies. The pandemic also resulted in an increase in human trafficking and exploitation of workers. Most disturbing of all, with children unable to attend school and spending more time online, members reported a rise in online child exploitation.

So how has the pandemic changed the way criminals are laundering their money?

Banks, financial institutions and non-financial businesses and professions have moved interactions with customers online. Limited in-person contact is impacting customer identification procedures and criminals are quick to exploit these changes in internal controls to bypass customer due diligence.

This is why, in April last year, when the first countries went into a national lockdown, the FATF encouraged the use of technology, including FinTech, RegTech and SupTech to the fullest extent possible. Using digital or contactless payments and digital onboarding reduces the risk of spreading the COVID-19 virus. It also allows the continuation of essential financial services and the payment of government benefits to vulnerable populations. During the crisis, more than 60 million new accounts have been opened using digital onboarding.

But not every digital ID is reliable. FATF Guidance highlights how to determine whether the Digital ID system's technology, architecture and governance has suitable levels of assurance and whether it is appropriately reliable and independent. A trustworthy digital identity can improve the security, privacy and convenience of identifying people remotely for both onboarding and conducting transactions. And it can help mitigate money laundering and terrorist financing risks.

The pandemic has left many businesses or individuals in financial need. They make easy targets for criminals who may exploit them to take part in money-laundering activity. For example, by using a failing but legitimate business as a front for illegal activity. The economic volatility has resulted in a number of other money laundering vulnerabilities, such as an increase in unregulated financial services and insider trading from the large shifts in value due to the pandemic. We have also seen cases of misuse of virtual assets in COVID-19 related fraud including money mule scams that target the recently unemployed or furloughed.

So what should countries do?

Money laundering and terrorist financing are not victimless crimes. Money laundering fuels serious crime from drugs, human trafficking and child exploitation. Crime and terrorism destabilise economies, takes away trust in government and hamper economic growth, which impacts every citizen.

But countries are not powerless against these crimes. The FATF Standards are a robust legal, law enforcement and operational tools to combat these threats.

More than 200 jurisdictions have committed to implement the Standards. Each of these countries needs to fully and effectively implement the FATF's standards.

FATF Assessments to date show that while there is progress, there is still much to be done. Many countries have established laws and regulations without focusing sufficiently on the actual results achieved. They have focussed on outputs over outcomes. They need to build an effective regulatory system, ensure that the financial sector are aware of the money laundering and terrorist financing risks they face and are reporting suspicious transactions. And they need to make sure that financial intelligence units have adequate resources to analyse and pass on these reports to law enforcement for investigation. The results of assessments in the MENA region, are generally below average particularly on preventive measures and effective financial supervision.

At a time when, naturally, most countries are focused on delivering crucial medical assistance such as a national vaccination programme, their focus is less on money laundering and terrorist financing. However, the criminal threat has never been greater. More than ever, countries should use the risk-based approach of the FATF Standards to prevent money laundering and terrorist financing.

The private sector is the first line of defence against the threats we face. This is why it is a collective mission for us all. The FATF recognises the importance of deep dialogue with the private sector, and this informs all our work. It helps us understand the implications for business on the ground and ensures that businesses can operate under reasonable standards that work in practice.

Particularly now, during this global pandemic, we must increase cooperation, information sharing and dialogue.

What is FATF doing?

The change in customer behaviour has turbo charged online transactions with growing numbers of online payments in nearly every sector. Many predict that this change is irreversible. With ever-growing mountains of online transactions, identifying the anomaly is not humanly possible. We must make better use of technology, to make us more effective and efficient in weeding out criminal activity. Big data analytics and machine learning, for example, are reducing false positives that require manual review. This contributes to enhanced productivity and the standardisation of compliance efforts.

A key priority of the FATF is to explore the opportunities that digital transformation brings to fighting money laundering, including to onboard customers or detect criminal activity. In particular, the FATF is focussing on three areas:

1. Identifying the opportunities and challenges of new technologies for the private sector, supervisors and regulators;
2. Exploring the potential for data pooling, analysis and the real and perceived barriers to this including data privacy and protection, to explore new technologies that facilitate information-sharing amongst financial institutions while protecting personal information; and
3. Helping to accelerate digital Transformation for operational agencies, such as financial intelligence units and law enforcement authorities.

Artificial intelligence, machine learning and privacy enhancing technologies have the potential to transform the way we fight money laundering and terrorist financing.

The use of new technologies does not replace human intervention and judgement, it liberates and improves it.

The FATF is also continuing to monitor the developments in the virtual assets sector. In July 2020, FATF reported to the G20 on so-called stablecoins, which had raised concerns due to their potential for mass adoption. FATF clarified how its standards apply to address the risks they pose. The FATF also conducted a 12-month review of the implementation of the revised Standards on virtual assets. While we found there had been progress in implementation, governments and the private sector need to do more to effectively tackle the risks. We also recognise that FATF can do more to help.

This is why, we issued a report on virtual asset red flag indicators which will help businesses identify and report suspicious activity. It will also help them apply the risk-based approach to their customer due diligence requirements. This means knowing who their clients and the beneficial owners are, understanding the nature and purpose of the business relationship, and understanding the source of funds.

We are updating our guidance on virtual assets. This will address key issues such as who a virtual asset service provider is, how businesses can implement the travel rule and so-called stablecoins. We will also publish a second 12-month review on implementation in June of this year. All the while, we are formally assessing how well countries are implementing these measures through the mutual evaluation and follow-up process.

The impacts of the pandemic continue to evolve. The changes in both money laundering and terrorist financing activity will continue to evolve. The FATF is developing guidance to help supervisors better assess the risks that the private sector faces. This understanding will help them shape their activities. The ability to adapt to changing circumstances, such as the COVID-19 crisis, is key to effectively detect and prevent misuse of the financial system.

However, back to my main message. The opportunities from this pandemic are not only for criminals, we need to exploit it to reform and turbo charge our AML/CFT measures through the use of technology and the application of a smart, intelligence-led and risk-based approach.

That’s why this conversation today, and your efforts, are so important.

Thank you again for the opportunity to join you today.

Publications