REPRINT

R&C risk & compliance

THE INTERSECTION OF FRAUD, SANCTIONS AND ORGANISED CRIME

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JUL-SEP 2026 ISSUE

www.riskandcompliancemagazine.com

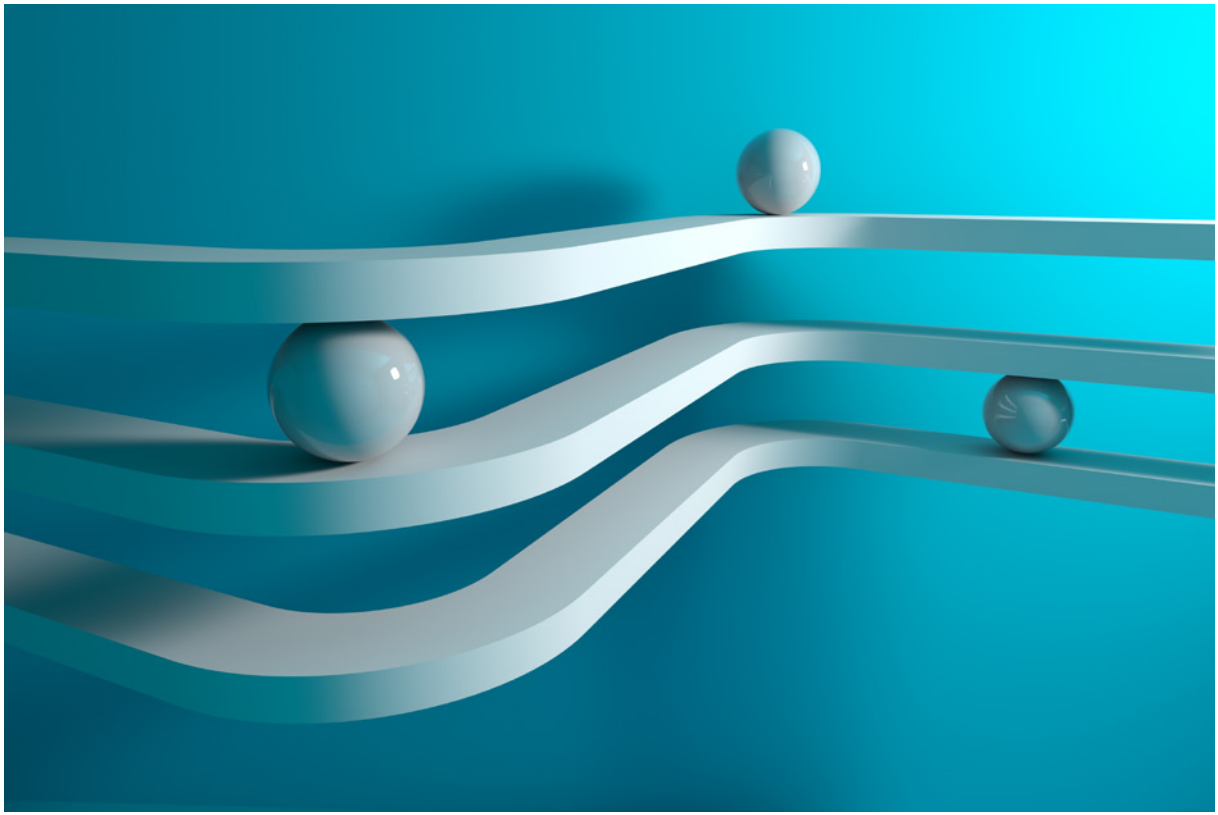
Visit the website to request
a free copy of the full e-magazine

FTI CONSULTING™

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

HOT TOPIC

THE INTERSECTION OF FRAUD, SANCTIONS AND ORGANISED CRIME



PANEL EXPERTS

Stella Mendes
Global Leader of Financial Services,
Senior Managing Director
FTI Consulting
T: +1 (212) 841 9363
E: stella.mendes@fticonsulting.com

Stella Mendes leads FTI Consulting's global financial services practice, focusing on financial institutions, bank governance and regulations. With more than 25 years of diverse banking industry experience, she leads AML, BSA and OFAC reviews and risk assessments for banks, money service businesses, credit union and other financial service providers. Ms Mendes has previously served as president and chief operating officer for First National Bank of NY and as the compliance and BSA officer.

Alma Angotti
Senior Managing Director
FTI Consulting
T: +1 (771) 248 2089
E: alma.angotti@fticonsulting.com

Alma Angotti is a financial crime compliance and sanctions expert with over 25 years of experience in regulatory enforcement and consulting. She held senior roles at the SEC, FinCEN and FINRA, where she led AML enforcement programmes. At FTI Consulting, she advises global financial institutions, fintechs and crypto firms on compliance, risk and investigations. She serves on advisory boards for digital asset initiatives and is approved as an independent compliance monitor by multiple US regulators.

Nicole Costaldo
Senior Managing Director
FTI Consulting
T: +1 (646) 453 1205
E: nicole.costaldo@fticonsulting.com

Nicole Costaldo is a senior managing director in FTI Consulting's data & analytics practice, based in New York. Ms Costaldo provides advisory services by helping private and public organisations use advanced analytic techniques to unlock value from their data. She quickly gets up to speed and navigates complex technical infrastructures to identify key systems, assess data quality and construct analytical models to solve various business challenges and quickly report and visualise data complexities and summary findings.

Jesus Ornelas
Senior Managing Director
FTI Consulting
T: +1 (347) 721 2467
E: jesus.ornelas@fticonsulting.com

Jesus Ornelas has wide range of experience providing financial institutions with compliance and investigative services to address and meet regulatory requirements pertaining to BSA/AML, sanctions, fraud and financial crime-related matters. Since joining FTI Consulting, he has been a contributing leader in a wide range of engagements with multinational banks, money services businesses and financial services companies. He has also completed numerous forensic transaction 'lookback' reviews as part of government investigations.

R&C: How is the reclassification of organised crime as national security or terrorism threats reshaping fraud and sanctions enforcement priorities?

Mendes: Illicit activity is illicit activity. From a financial institutions' (FIs') operations perspective, the reclassification does not change anything. Rather, it reshapes how governments are thinking about the threat and how that results in changes in enforcement. Fraud was traditionally seen as an economic crime. Today, it is often considered as strategically destabilising a nation or location. This reclassification has shifted the way sanctions are used. Historically, sanctions were used as a foreign policy tool to implement force. Now, they are used more as a way to undermine a geopolitical objective. There has also been a shift in the way teams are organised, which allows for better communication and coordination when escalating priorities. As a result, fraud teams are now looking more for networks than individuals.

Costaldo: Historically, unlike the teams that monitored sanctions compliance, the teams that managed fraud were separate, isolated and siloed. There has been a shift, especially with the adoption of artificial intelligence (AI) and the need for complex data analysis, to bring the related information from each of these types of compliance vehicles together. There is now a lot more synergy and consolidation of information. For example, a crime may end up being money laundering, but it started as fraud via an account takeover.

Angotti: Reclassifying organised crime does not, on the face of things, change much. Regardless of the change, FIs must still perform their risk assessment to identify where they have risks and determine how they can detect and prevent illegal activity. One way things are changing, though, is a subtle shift in the makeup of the proceeds of crime. The US dollar is still the currency of choice for criminals, but as stablecoins become more popular, they are becoming a bigger part of the composition of illicit funds. Compared to other kinds of digital assets, stablecoins have become a particularly effective vehicle to evade sanctions because they are an actual payment method and are able to hold their value.

Ornelas: The reclassification of organised crime as a national security issue has really highlighted the risks associated with technology and digital currencies. While they are innovations, they carry a lot of risk, especially when they originate from certain geographies like Russia or Iran. There are threats coming from those regions that require greater coordination globally, even beyond the enforcement efforts of a single nation.

R&C: How effective are current sanctions frameworks in targeting the full lifecycle of organised crime-linked activity, from production to financial flows?

Costaldo: Unless they have advanced network capabilities to really be able to connect the dots, it will be challenging for organisations to identify this activity themselves. Larger organisations and multinational organisations will have more of a picture, especially large clearing FIs. On the other hand, if there are banks that are highly connected to fintechs that create an amazing layering mechanism for criminals, they will lose that visibility very quickly. Sanctions frameworks are not designed to capture the activity from production to financial flows, but they are supposed to get that end part of the flow. I have heard law enforcement say that it is actually really helpful for them to then connect the dots to where production is happening, to be able to break down the entire supply chain of criminal networks that function like an enterprise.

Mendes: The government and certain banks have gotten better at targeting the full lifecycle of organised crime-linked activity, but are still pretty far behind. Current sanctions frameworks in place are moderately effective, however sanctions are probably the least effective framework right now of targeting organised crime due to its complex nature. It is just like looking for needles in haystacks. The only way to be really effective when it comes to sanctions is to restrict global mobility. However, we are now limiting access to people who should have access to the financial system. It is a delicate balance. Another challenge government and banks face is organised crimes involving synthetic drugs, illegal mining, counterfeiting and human trafficking. These crimes tend to be operated in areas with weak government, and in corrupt jurisdictions where there is more risk and lack of compliance.

> **"Fraudsters and money launderers are adaptive. We are seeing how organised crimes involved in fraud and laundering now operate in much lower monetary points compared to years ago."**
>
> *Jesus Ornelas, FTI Consulting*

Ornelas: Current sanctions frameworks face significant limitations in addressing the full lifecycle of organised crime activity, particularly as illicit schemes increasingly originate in or transit through foreign jurisdictions. FIs – especially banks and fintechs – often lack visibility into these cross-border risks, leaving their fraud and sanctions controls untested against the evolving methods of transnational criminal networks. Contemporary organised crime now operates through lower value, highly fragmented transactions that blend seamlessly into legitimate financial flows, enabling illicit funds to circulate undetected for extended periods. This latency allows fraud to proliferate, victims to be exploited and proceeds to be layered across multiple jurisdictions before any meaningful red flags emerge. By the time suspicious patterns become discernible, FIs may already face substantial exposure, including inadvertent sanctions violations.

Angotti: It is harder now for FIs because we have gone from lists of designated persons and entities and targeted countries for sanctions to sectoral sanctions and other sorts of more targeted sanctions regimes. These are more difficult to investigate and understand than just a list of checking a list of designated individuals or countries. Also, it can be very difficult to identify sanctions evasion, export controls violations or prohibited investment targets which can be difficult to see in transactions. It is a matter of deep due diligence on products and services at higher risk of sanctions evasion. For foreign banks in higher-risk jurisdictions, the pressure to better identify evasion often falls on the US correspondent bank. US banks are often the ones that identify potential sanctions violations through their correspondents – and they do not want to face sanctions violations penalties because their correspondents missed something.

> **"FIs have always been the front line of efforts to disrupt organised crime activity, but there is more emphasis on realisation of their importance now."**
>
> *Nicole Costaldo, FTI Consulting*

R&C: To what extent are FIs now the primary battleground in efforts to disrupt organised-crime activity?

Costaldo: FIs have always been the front line of efforts to disrupt organised crime activity, but there is more emphasis on realisation of their importance now. Perhaps this is the inertia needed to invest again in technology. Technology and centralised information unlocks immense value for banks – from having a better understanding of their customers' identity and behaviour, to being able to better grow their business, earn customer growth and ultimately better serve their customers, while also maintaining compliance with their regulatory obligations.

Mendes: Historically, FIs were always a central point in the compliance framework. But, now the connectivity is what is different. FIs now are not just looking for suspicious activity, but also shell companies, layering, trade anomalies, cyber crimes and crypto off-ramping behaviour. They have kind of become a mini financial crime investigative unit looking at things for which they historically never had responsibility. Human trafficking is a big area that banks historically did not look for, but are now playing a critical role in identifying. Without involvement of the banks, it is hard for authorities to pull those things together because it is about following the money and for what the money is being used.

Angotti: Banks have always been the primary battleground. The reason criminals commit crimes is to make money. They are not typically doing it just for sport. 'Follow the money' has always been the best way to get to the criminals. If we go back to the beginning of federal law enforcement, the agents were looking at money. Remember, they convicted Al Capone for tax evasion. We are starting to see more real public-private partnerships as banks and fintechs collaborate with law enforcement. This kind of information sharing is critical because both sides only have a piece of the puzzle. They need to cooperate to put the puzzle together. Banks want to help stop human trafficking, drug trafficking and fraud, but it can be hard for them to do so without knowing the nuances or how typologies are changing, sometimes in very subtle ways. Law enforcement might have that information first.

Ornelas: A lot of FIs are emphasising their partnership with law enforcement. This relationship focuses on addressing how banks share their intelligence and partner with the right law enforcement network on the receiving end of a suspicious activity report to prevent getting dinged, but also to be able to share information in real time. In the case of human trafficking, timing is a really important component. How can we prevent some of that from happening if a report is submitted three months later?

R&C: What role do professional money laundering networks play in connecting fraud, sanctions evasion and cartel financing?

Angotti: Professional money laundering networks have always played an important role. Organised crime is a business and it has the same kind of operational structure that legitimate businesses do. Someone in the organisation has to organise movement of massive amounts of money around the world, often. On the one hand, some parts of this have become easier with the onset of fintechs, digital assets and stablecoins. Digital assets and stablecoins are fully traceable and the blockchain can provide a lot of good information to law enforcement. Of course, old standards are also still very popular – trade finance, for example, is a popular way to move large amounts of money without anyone knowing the source of the funds.

Costaldo: Money laundering networks put criminal organisations' money to work. Because these networks are the ones moving the money, they are able to avoid being caught by even well-established sanctions controls. Add fraud on top of this, and it makes it hard for authorities to identify the true parties involved, as information is being sold on the dark net, stolen through theft or handed over through scams that make account takeover

a common practice for criminals and a means to easily access and move money through payment networks and FIs while impersonating trusted, low-risk customers, thereby circumventing even the best compliance controls. To a criminal, these money laundering networks are priceless.

Ornelas: Some professional money laundering networks can serve as the financial link between fraud, sanctions evasion and cartel financing in a single interconnected system. By consolidating proceeds from online scams, illicit trade and drug trafficking, and then moving those funds through shell companies, crypto channels, trade-based schemes and high-risk jurisdictions, they blur the origin of illicit money and make it appear indistinguishable from legitimate financial activity. These networks exploit regulatory blind spots, especially low value, high volume transactions and mule account flows, allowing fraud proceeds to mix seamlessly with funds tied to sanctioned actors or cartel operations. In doing so, they can provide the expertise, anonymity and global reach that criminal groups need to scale their operations – making professional launderers the critical link that transforms separate criminal enterprises into a unified, transnational financial ecosystem.

R&C: How are fraud schemes evolving as a core revenue stream within cartel and transnational criminal operations?

> **"The US dollar is still the currency of choice for criminals, but as stablecoins become more popular, they are becoming a bigger part of the composition of illicit funds."**
>
> *Alma Angotti, FTI Consulting*

Angotti: A good example of such a scheme is North Korea. Nearly 50 percent of North Korea's gross domestic product comes from fraudulent activity. Twenty-five percent comes from hacking digital assets and cryptocurrency fraud, and 25 percent comes from IT worker fraud. Criminals send talented IT workers all over the world to do legitimate work and send the money they make back to North Korea, often through China – this is a perfect example of the intersection of fraud, sanctions, national security and money laundering.

Ornelas: Sanctions exposure is no longer confined to transactions involving well-known illicit actors or high-risk jurisdictions. FIs must now contend with the possibility that proceeds from foreign fraud operations – including forced labour scam compounds, cartel run digital enterprises and criminal networks with state backing – are entering the financial system under the guise of routine consumer activity. What once appeared to be low risk, everyday transactions may in fact be the final stage of a complex, transnational fraud ecosystem.

R&C: In what ways is technology – particularly AI, cryptoassets and digital platforms – changing the scale and sophistication of fraud and laundering?

Mendes: The financial industry is evolving rapidly, shaped by advancing technology and the shifting geopolitical landscape. Fraudsters and money launderers are also using sophisticated technology – but for the purpose of funding their criminal activities. Innovation brings efficiency and opportunity, but it also introduces new risks. To stay ahead of the curve, resilience depends on preparation. To combat AI driven fraud, old tools will not protect organisations effectively. Good guys need to continuously evaluate emerging tools carefully and assess their fraud analytics and real-time monitoring.

> **"FIs now are not just looking for suspicious activity, but also shell companies, layering, trade anomalies, cyber crimes and crypto off-ramping behaviour."**
>
> *Stella Mendes, FTI Consulting*

Ornelas: Fraudsters and money launderers are adaptive. We are seeing how organised crimes involved in fraud and laundering now operate in much lower monetary points compared to years ago. Historically, we would mostly see hundreds of thousands of dollars moving around, and now we see $100-200 moving around. These transactions contain keywords and information a novice would not understand and make it harder for an FI to figure out and connect.

Angotti: AI has allowed criminals to commit fraud cheaply and at scale. We know that criminals are

using technology to move money so in order to fight bad guys with technology is to good guys to use technology. Investment fraud involving digital assets is a large part of the increase in global fraud. so if an organisation is processing stablecoin or other digital asset transactions, it should consider blockchain analytics tools to identify the risk to its customers, as well as counterparty risk and transaction risk.

Costaldo: AI and digital currencies are truly technical innovations that will change the way of many things, due to their computing power, wide accessibility, and ability to generate content and break down international borders. These technologies make it very easy for criminals to up their ante. Coupled with our increasingly digital world and reliance on third-party relationships to manage risk, support operations and enable growth, there is a lower barrier to entry for criminals. The way in which they exploit control vulnerabilities is now supercharged, and scaled up by technology and the availability and exchange of information online. R&C