vinciworks

What to expect in AML, fraud and financial crime in 2025

What to expect in AML, fraud and financial crime in 2025

The world of anti-money laundering (AML), fraud and corruption is rapidly evolving, and 2025 is shaping up to be a pivotal year. With new technologies - think AI - upping the threat levels in cryptocurrency-related crimes, cybersecurity breaches and supply chain abuses coupled with stricter global regulations, it's going to get harder for businesses to stay ahead of the curve. And with governments and regulators moving towards proactive measures, demanding not just compliance but accountability, significant penalties await those who fail to prevent financial crime.

What are the trends, challenges and strategies in financial crime that businesses need to navigate in 2025? From evolving sanctions regimes to increased fraud risks to the benefits and dangers of AI, it's evident that this year is a pivotal one for businesses who want to maintain compliance, avoid corruption and survive and thrive in a landscape that seems to be getting more complex.

Expect crypto scams to continue. Only now they are more sophisticated

Despite a series of huge scandals in the cryptocurrency world over the past few years, cryptocurrencies remain popular, some would say mystifyingly so. But then again it's hard to deny the allure of what are often exciting and innovative opportunities - not to mention the "get rich quick" schemes - that the digital currencies appear to offer.

The crypto world represents a democratisation of access to money in a way that was not possible before. But despite the hype and short term highs, the crypto world remains a highly volatile, loosely regulated world. Yes, digital currencies don't require stodgy banks or heavy regulations but the very nature of their ability to bypass intermediaries has always meant that the more popular a currency becomes, the more prone it is to money laundering and corruption. And what users in 2025 need to know is that these crypto scams are becoming more and more sophisticated.

What to expect this year? Crypto scammers will likely use cutting-edge AI tools to make their scams seem more genuine. AI-generated deepfakes can be used to mimic real influencers and lure investors into legit-seeming projects. Be sure to double-check the identities of anyone you're dealing with, especially when large sums of crypto are on the line.

Expect more DeFi (decentralised finance) scams too. Thanks to DeFi platforms' anonymous transactions and complex smart contracts, keep an eye out for fake DeFi apps or scams where creators hype up a new project, raise funds and then vanish. Check where you put your money, research every project and, above all, avoid schemes promising "guaranteed" returns - a classic red flag. Make sure the platform you're working with has a good reputation and a track record of security and transparency.

As governments will likely ramp up crypto regulation in 2025, scammers might get even more creative in avoiding detection. They might impersonate regulators or law enforcement, creating fake "compliance" alerts to scare people into sending funds. Get familiar with your country's crypto laws and regulatory bodies, and never, ever trust random "official" messages claiming you're in trouble or need to pay a fine. A little scepticism goes a long way in the world of crypto.

Failing to prevent fraud is going to have bigger implications

The offence, failure to prevent fraud, is going to matter to businesses more than ever this year. The UK government just published its much-anticipated guidance on this new corporate criminal offence which was introduced as part of the Economic Crime and Corporate Transparency Act 2023 (ECCTA). This means that the new offence will come into effect this coming September.

The guidance fundamentally changes the expectations around how companies manage and mitigate fraud risks. Under this guidance, businesses or even specific people are now directly accountable for putting preventive measures in place to stop fraud from occurring within their organisations. Essentially, if a business fails to implement adequate procedures to prevent fraud, it could face significant fines and legal consequences, even if leadership wasn't aware of the fraudulent activity.

Failure to prevent fraud is part of a package of changes brought in by the ECCTA to increase corporate criminal liability and corporate transparency. It represents an increased focus by both the former and current government on targeting economic crime.

The stakes are being raised and businesses need to prepare. Businesses will need to implement clear, documented and effective anti-fraud processes. Companies are staring down the barrel of fines, reputational damage and possibly restrictions on their operations.

Failure to prevent fraud could directly impact your company's bottom line. Customers, investors and partners increasingly value transparency and ethical business practices and if your company is caught up in a case that involves fraud and corruption, especially one that is due to inadequate prevention measures, it could impact your stakeholder and consumer confidence.

What could you do now? Create a culture in your company that actively discourages fraud and corruption. Conduct fraud risk assessments and invest in quality employee training on fraud prevention. And don't forget to upgrade your monitoring tools so you can spot potential fraud before it becomes a problem. That will also demonstrate to regulators and to your clients and consumers that you are committed to staying ahead of risks.

In 2025, failure to prevent fraud will matter because it's not just a legal requirement; it's going to become a business imperative. The companies that take it seriously will be the companies that are more protected from financial and reputational harm.

Cybersecurity gets complicated

In 2025, companies are going to have to get proactive about their cybersecurity as cyber threats become more sophisticated. But that's where things might get complicated.

Companies are going to turn to tools driven by artificial intelligence (AI) to identify vulnerabilities and suspicious behaviour in real-time. But guess who will also be wielding AI? Those cybercriminals you are trying to stay one step ahead of. Ransomware attacks, data breaches and phishing scams will evolve this year, as cyber criminals try to exploit what they can. From remote work setups to connected smart devices, everything is vulnerable.

Companies need to prepare for AI-generated malware, sophisticated deepfake scams and autonomous cloud attacks, where hackers use automation to breach networks and access sensitive data quickly. Companies will need to consider AI-based threat detection to stay a step ahead and invest in automated cloud security solutions that can counter fast-moving attacks . Emphasis will be placed on zero-trust architecture, a security model that assumes no one is safe and continuously verifies everyone.

With human error still accounting for most breaches, you will also want to prioritise employee education on cyber hygiene. Training should become more frequent and more realistic as they try to help people spot the latest scams.

Regulatory demands around cloud security are also going to get tighter. UK companies that rely on cloud services should ensure compliance by strengthening their cloud infrastructure and consider unified security platforms for easier compliance management and real-time threat monitoring.

Governments around the world are likely to try to push stricter regulations, like requiring businesses to report incidents faster and invest in better security measures. For consumers, it might mean more privacy protections. But for companies, it's a clear sign that in 2025 cybersecurity is going to be a real business priority.

Russia and North Korea will not get any nicer

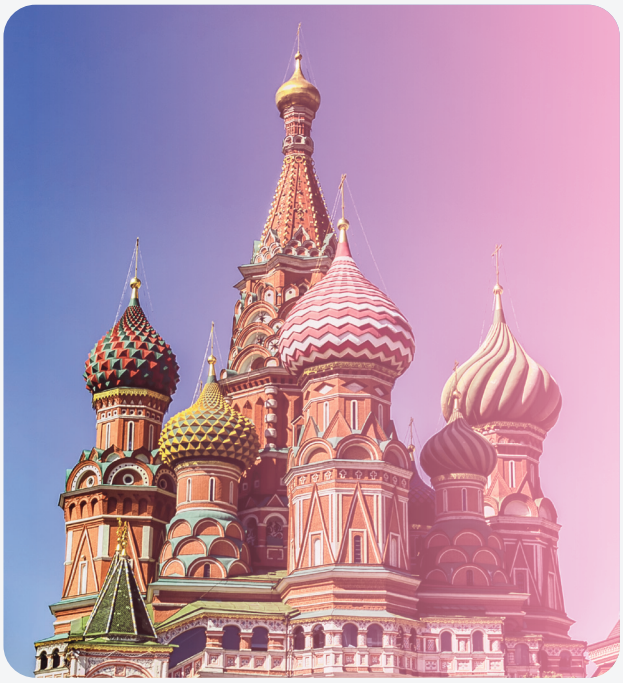
In 2025, there will be intense global efforts to prevent financing of nuclear and military proliferation for the two main global bad actors, Russia and North Korea.

Russia's ongoing geopolitical manoeuvres - the war with the Ukraine is nearly three years old - and North Korea's neverending nuclear ambitions ensure that it is no surprise that according to the 2024 US National Proliferation Financing Risk Assessment prepared by the US Treasury, these two countries are the highest risk threat actors for proliferation financing (PF). This is significant due to the scale of Western sanctions on Russia. The risk of doing business with Russia or sanctioned entities connected to Russia can now come with PF risks. And the fact that Russia does business - often using complex transaction structures - in Turkey, the United Arab Emirates and China means that this has big implications.

What can businesses expect this year? They can expect regulators to further tighten the screws on any channels that could potentially be involved in PF. This means stricter screening on transactions and partnerships, especially those in industries like technology, energy and chemicals. Banks and financial institutions will especially feel the heat, with likely requirements to implement even more advanced monitoring tools to flag suspicious activity in these regions. Governments might mandate closer tracking of cryptocurrency and digital asset transactions as both countries leverage these to bypass financial systems.

If Russia and North Korea are on your business radar, be prepared. There will be a need for tight controls, more oversight and you will want to make sure even the smallest deals are clean. And the US, EU and other allied nations are set to continue expanding their lists of sanctioned entities linked to these countries. Make sure your companies' compliance team conducts due diligence and double-checks everything for risk exposure, stays vigilant and continuously updates and screens your sanctions lists.

This year, there will likely be more precise digital tools to identify funds coming in and out of these sanctioned regions. Monitoring tools are increasingly focused on capturing hidden relationships and transactions that could support nuclear, chemical or biological weapons development. Pay close attention to any third parties who may have even a remote connection to these regions. In 2025, even an unintentional mistake with a sanctioned entity could lead to real trouble.



Lebanon is greylisted. Doing business there will be even trickier this year

The world of financial crime forever changed after the terrorist attacks of 9/11. At the time, US government officials declared that the fight against financing Al Qaeda was as critical as fighting Al Qaeda itself. It was understood that cutting off terrorist financing was critical to preventing them carrying out mass casualty attacks.

Since then, the regulated sector, and in particular banks, law firms and financial institutions, have found themselves at the forefront of tackling terror financing. Not only is this a money laundering issue, but it also impacts sanctions compliance. With billions of dollars under the control of sanctioned terrorists, understanding how to counter the risk of terrorist financing is crucial to a comprehensive sanctions compliance framework.

Terrorist financing has huge implications in 2025 for Lebanon, specifically as the country was just greylisted by the Financial Action Task Force (FATF). This flags Lebanon as a jurisdiction under increased scrutiny and financial institutions around the world will be looking closely at Lebanese transactions for signs of potential financial crime.

For Lebanon, this could mean stricter international banking relationships and increased transparency if the country wants to avoid further economic isolation. Expect Lebanese banks and businesses to ramp up their anti-terrorist financing controls, with new regulations and reporting obligations to track suspicious transactions more effectively. For companies interacting with Lebanon, expect a cautious approach to engaging with Lebanese entities. There will be a need to ramp up due diligence, making sure to screen all transactions and

partnerships that could be flagged as risky. There will be a need for clear documentation and verification from your Lebanese counterparts and additional checks on clients, suppliers or financial flows that could involve Lebanese counterparties. Expect these transactions to take longer and compliance costs to increase.

Exporters and importers dealing with Lebanese companies may face delays or disruptions due to this heightened scrutiny by banks on payments and trade finance arrangements. Small businesses and those in regions with strong ties to Lebanon, such as MENA and Europe, will feel the burden most. But whether directly involved with Lebanon or operating in industries with ties to the region, companies will need to proactively address these risks to be compliant in this era of heightened regulatory scrutiny.

The WUC case ruling is a game changer for supply chains

The recent case in which the Court of Appeal found it unlawful that the National Crime Agency (NCA) decided not to open a money laundering investigation into the trade of cotton to the UK from Xinjiang region of China will have real implications for business' supply chains this year.

The cotton trade in Xinjiang has been subject to serious allegations of forced labour, slavery and human rights abuses perpetrated against the Uyghur ethnic group by Chinese authorities. The World Uyghur Congress (WUC) alleged that the product of such abuses – the cotton transported to the UK – is therefore criminal property. But the NCA refused to investigate businesses trading in this cotton, so the WUC brought a judicial review.

The High Court rejected it but the WUC appealed the High Court's decision, and this past June, the Court of Appeal found that the NCA made an error in law in deciding not to investigate under the UK's Proceeds of Crime Act (POCA). This ruling expands the application of POCA, putting companies at increased risk for asset recovery, fines and even criminal prosecution for failing to conduct adequate due diligence on their supply chains.

Couple that with the recent passage of the Economic Crime and Corporate Transparency Act (ECCTA) and this year we could see more companies and even senior managers found criminally liable for economic crimes within their supply chains, and failing to conduct adequate due diligence.

All this means a heightened scrutiny on supply chains, especially with companies operating in regions associated with human rights abuses. Companies must now ensure their products are free from any connection to these abuses or face legal consequences. This includes the possibility of prosecution for dealing with "criminal property," such as goods produced through forced labour, even if those goods have been paid for at market value. And forget about the "adequate consideration" loophole, where companies could avoid liability by paying market value for the goods. Now, suspicion or knowledge of forced labour in the supply chain is enough to be criminally liable.

Businesses will need to enhance their due diligence processes, map their supply chains thoroughly and implement updated monitoring systems. Supply chain transparency will be required in 2025 and will need risk assessments and contractual safeguards to stay on the right side of the law while navigating an increasingly complex global trade environment

This case sends a clear message to businesses worldwide: compliance with human rights standards on your supply chain is no longer optional.

Be prepared for regulators to take an even more proactive approach

Regulators are stepping up their game this year. They have been increasingly moving from a reactive - “let’s wait for the crisis to happen" - mode to a proactive - “let’s prevent the crisis from happening” - approach. But this year, this shift in mindset is going global, which means this is the year that it will land, hard.

The US DOJ launched a whistleblower pilot program this past year that incentivizes voluntary reporting of corporate misconduct by offering financial rewards, especially for significant violations. The SEC allowed the Cloopen Group to avoid penalties in its compliance failures thanks to self-reporting, collaboration and remedial actions, such as firing employees involved in fraud and improving internal controls. The European Council established the Anti-Money Laundering Authority (AMLA) to prevent money laundering and terrorism financing through enhanced supervision of high-risk entities across the EU

And then there’s the UK’s Economic Crime and Corporate Transparency Act (ECCTA) which is coming into force this year. The Act focuses on proactive prevention rather than reactive enforcement. It also introduced the senior manager offence, a significant change in corporate criminal liability. Prosecutors no longer have to prove that “the directing mind and will” of a company was behind wrongdoing. With ECCTA, any senior manager who has engaged in criminality around fraud, tax evasion, sanctions breaches, money laundering, false accounting and bribery can find their actions result in corporate prosecution.

And it’s not just your businesses’ operations but your supply chains too. Senior managers will need to ensure that due diligence is conducted across the supply chain on a risk-based and ongoing basis, to ensure there is no criminality in any of the goods or services purchased in the supply chain. If not, the proceeds of these goods can become criminal property, and dealing in criminal property is a money laundering offence.

This shift is driven by a combination of emerging risks and advances in technology that make early detection more feasible. Waiting for scandals to erupt is so 2024. With tools like predictive analytics and real-time monitoring, suspicious activity can be flagged and financial crimes can be prevented before they take root.

This could change how you approach compliance. You need to anticipate risks and ensure there are safeguards throughout your operations. Regulators will expect companies to know their supply chains inside out, spot red flags early and develop robust systems to manage vulnerabilities. This might create more work up front, but you are also reducing the likelihood of costly enforcement actions or reputational damage.

Businesses that adapt quickly, embrace technologies for compliance and invest in employee training, will not only meet these new expectations but also build trust with regulators, stakeholders and customers. In this new landscape, staying ahead of the curve is no longer optional—it’s a competitive edge.

This year, efforts to prevent AML, fraud and corruption are going to be more complicated. Emerging technologies are reshaping compliance frameworks, impacting regulators and effecting regulation. Businesses need to keep an eye on both national and international laws while thinking proactively, staying agile and making sure compliance is a focus at every level of their company. It's not just about staying within the legal frameworks, it's also about building and maintaining trust in a complex world.

How VinciWorks can help

eLearning **Courses**

VinciWorks makes compliance training and eLearning that works.

Available in every language you speak. Built by us.

Ready for you.

Training your staff in anti-money laundering (AML) needs to be more than a tick-box exercise. Companies and law firms can easily fall out of compliance or get caught up in dirty money without a robust AML framework. Packed with realistic scenarios, real-life case studies and customisation options, our suite of AML courses will help you stay protected.

Learn more

Bribery schemes can lead to the loss of money, reputational damage and legal action. Companies and law firms need to know how to manage and mitigate their bribery risks. With gamified learning, customised content and real-life scenarios, VinciWorks' suite of anti-bribery courses will ensure your entire staff is trained to avoid corruption.

Learn more

Modern slavery training helps your company or firm avoid being connected to activity that violates regulations, either directly or by proxy through supplier relationships. With a range of options, our modern slavery training suite is designed to meet the needs of an entire team, from general staff to procurement teams.

Learn more

About us

We believe compliance enables business. Compliance is an opportunity to be one step ahead, so your organisation can focus on advancing the business.

For over 20 years, VinciWorks has been at the leading edge of re-envisioning compliance tools and training. Our creative and driven team works hard everyday, challenging the traditional compliance industry to become forward-thinking, interactive and engaging. From our vast library of 800+ courses, to the award-winning Omnitrack training and compliance management software, to a curated catalogue of world class resources, VinciWorks is here to support your organisation every step of the way.

We constantly have our finger on the pulse, being the first to adapt our products to new regulations and market changes that impact our customers' businesses. Our flexible solutions ensure that every one of our products is tailored to our customers' unique business needs, placing them at the heart of everything we do.

www.vinciworks.com
enquiries@vinciworks.com
+44 (0) 208 815 9308