E-BOOK

Your fincrime time machine: what 2025 holds for the financial crime industry

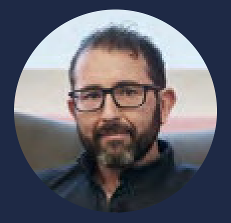
Contents

Thank you to the contributors

Views expressed in this report are personal and not those of the organisations the contributors work for, unless explicitly stated.

Dr. Nicola Harding
Chief Executive Officer,
We Fight Fraud

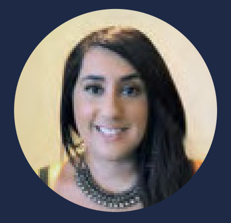
Ray Blake
Presenter of The Dark Money Files podcast & FinCrime SME at Risk Alert 24/7



Ian Christie
Co-Founder,
FincSelect

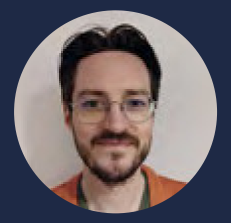
Pallavi Kapale
Senior Financial Crime Officer,
Bank of China

Ian Mynot
Director,
Advanced Financial Crime Consulting

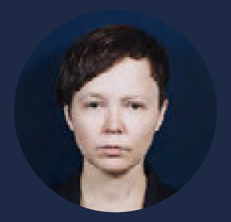


Pinnie Balachandra
Enterprise Customer Success Manager,
Hummingbird

Dr. Firas Nadim Habach
Swiss Head of Financial Crime Compliance
Revolut



James Coveney
Head of Data Science,
Zempler Bank



Ester Eggert
Head of Product,
Salv

Jessica Cath
Partner, Financial Crime,
Thistle Initiatives

Taavi Tamkivi
CEO and Co-Founder,
Salv

George Rhodes
Senior Fraud Specialist,
Transunion

Introduction

The fight against financial crime took on new dimensions in 2024, shaped by a mix of regulatory tightening, sophisticated fraud tactics, and technology. That's the message from industry experts who shared their reflections with us, looking back at 2024 and predicting what lies ahead.

Their voices describe an industry at a pivotal moment, where innovation and collaboration are both a necessity and an opportunity. Have you ever thought how useful it would be to have a time machine so that you could travel into the future?

Well, our gift to you is exactly that. We asked a range of industry experts across Europe what the world of fincrime will look like by the end of 2025. The insights in this report come from a range of senior executives at companies including Revolut, Bank of China, and TransUnion, with certain themes popping up time and again throughout.

Artificial intelligence (AI) has been everywhere in 2024, so it's unsurprising to find it mentioned extensively, with contributors expecting AI to have a significant impact across all fincrime disciplines.

Alongside the opportunities, AI presents risks. First, from fraudsters who use the same tools to increase the scale and effectiveness of their operations. And second, from limitations within our organisations, such as poor-quality data or training the AI on flawed processes.

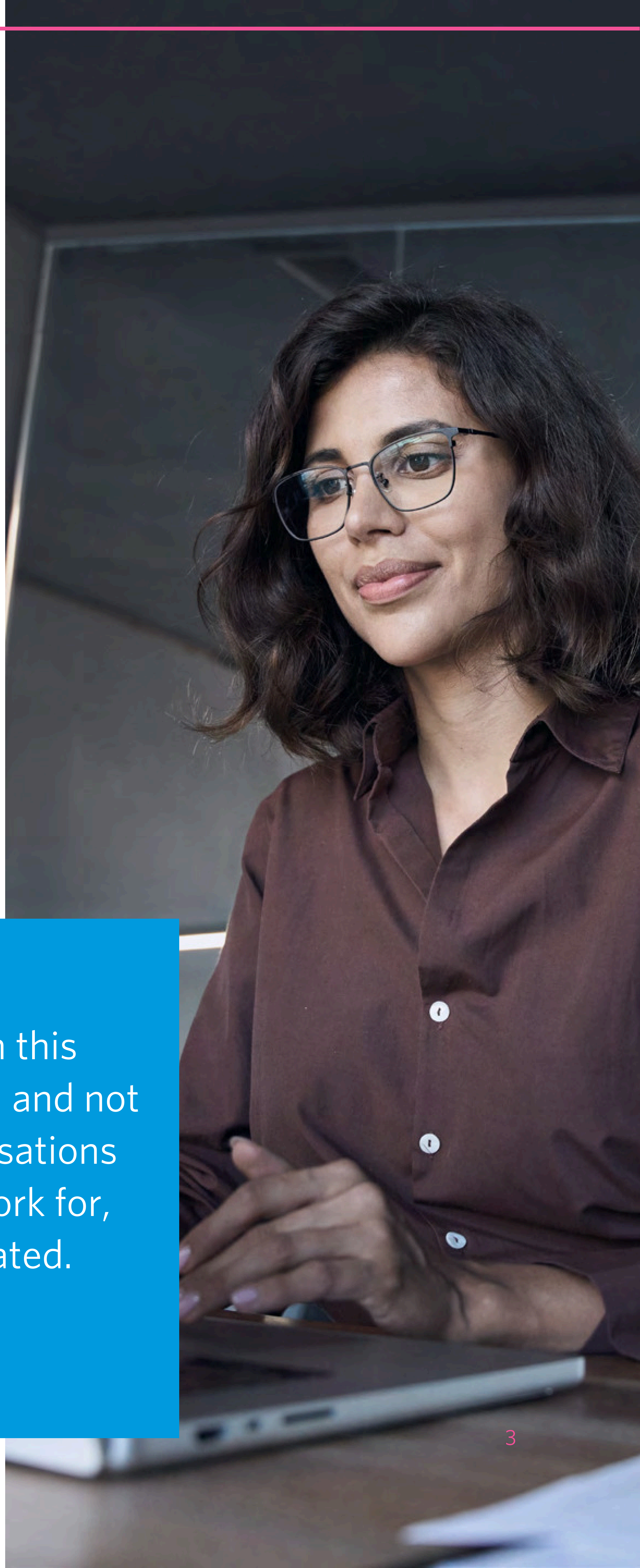
Another unifying thread in these insights is the importance of collaboration—whether through public-private partnerships, real-time data sharing, or cross-sector teamwork. These experts featured in this e-book agree that no single organisation can tackle the challenges that lie ahead alone.

Finally, 2024's regulatory tightening, particularly around digital assets and reimbursement for fraud victims, has set the stage for more robust compliance systems in 2025.

While there's a pattern across all responses, the experts all offer a very unique perspective. Dr Firas Nadim Habach, Head of Financial Crime and Compliance at Revolut, emphasises the transformative potential of blockchain and smart contracts in automating regulatory processes. Jessica Cath, Partner, Financial Crime at Thistle Initiatives calls for firms to take a tech-first approach, carefully prioritising investments in AI and machine learning to mitigate risk in their most vulnerable areas. Meanwhile, Dr Nicola Harding, CEO of We Fight Fraud, warns that the industry's overemphasis on AI will push criminals to double down on social engineering.

As we enter 2025, this e-book offers a reflection on lessons learned and a forward-looking guide for fincrime professionals. Let's get into it...

Views expressed in this report are personal and not those of the organisations the contributors work for, unless explicitly stated.



A mismatch between crime fighters and criminals

"Make sure that everything you're doing is building towards creating a safer environment that reduces fraud. Otherwise, why are we here at all?"

Dr. Nicola Harding

Dr. Nicola Harding

Chief Executive Officer,

We Fight Fraud

Follow on LinkedIn

Dr. Nicola Harding
Chief Executive Officer,
We Fight Fraud

Looking back at 2024

I think 2024 has been the year of regulation — a trend we're going to see continue into 2025. Authorised Push Payment (APP) fraud regulations in the UK received a lot of attention, but Russia implemented a really similar piece of legislation about a week before. It tends to be all eyes on the UK, because we're often early adopters of regulation and, because of the global use of English, the UK tends to be a fraudsters playground, where new tactics get tried out.

On tactics, we have a greater raft of tools available, not just to fraudsters, but to everyone in general. ChatGPT, AI translation services, voice distorters, mobile editing capabilities on TikTok and CapCut. Basically anything that ordinary people use, criminals will use too.

So 2024 has been the year where we've seen regulation start to respond to the threats that all these new tools bring. And as a result, financial institutions are being kind of led with the stick rather than the carrot.

Key trends for 2025

In a nutshell, I think as an industry, we'll run towards AI and ways of stopping AI attacks. There's an overemphasis on AI because, at a societal level, we're all a bit afraid of it, because it might take all of our jobs.

And because of that, I think criminals will move away from technology, reducing their risk by targeting the individual more. So you've got this kind of battle of AI, where fire meets fire. And as a result, the criminals are starting to go against that trend and straight for people, with a bigger focus on social engineering.

If there's a technology aspect, it gets more risky for criminals, because they have to buy that technology from somewhere. For example, with Call ID spoofing: websites were shut down that held the details of customers, which led to arrests.

So if you're a criminal engaging in technology specifically to commit fraud, even if you're paying Bitcoin, there's a risk. But one on one over the phone with a potential victim, there's less risk and it's much harder to detect. Plus, we just aren't doing enough in the education and awareness space to target-harden victims.

So to summarise, I think there's going to be another mismatch between what the industry is doing and what criminals are doing.

Preparing for what's next

Fraudsters don't want people talking to each other about scams because, when they first come across a potential victim, they don't want that person to suspect it's a criminal attack. Fraudsters want us fresh and unaware because then they can be most effective. So we need more public visibility of fraud, financial crime and scams, and we need people to talk to each other about it.

And within the industry, I just don't think we're seeing the information flows that we need in order to get ahead of criminal attack. We need to be actively sharing threat intelligence, with financial institutions cooperating with each other and with governments.

How can fincrime professionals be more effective in the year ahead?

Don't take things at face value. Collaboration has been a key buzzword, but we're not actually seeing it in mainstream practice. And I think it's where we need to get to. Think about what you're are hearing at events, the information you're given and think about how that fits with your experience and your day to day.

Because collaboration is not talking to each other at a conference. That's not doing: that's observation. I'd much rather see advisory boards, for example, where people actually work together, with actions and an end product that exists to improve the industry as a whole.

Make sure that everything you're doing is building towards creating a safer environment that reduces fraud. Otherwise, why are we here at all?

Burnout, balance and the future of fraud prevention

George Rhodes
Senior Fraud Specialist,
Transunion

"It is important for practitioners to recognise burnout and prioritise mental wellbeing – this is what will make them successful in the long term."

George Rhodes

George Rhodes
Senior Fraud Specialist,
Transunion

Looking back at 2024

Fraud has continued to be a key challenge throughout 2024, with 40 per cent of all reported crime in England and Wales being related to fraud and – according to TransUnion's Consumer Pulse survey – 2 in 5 UK consumers being targeted for fraud in the last 12 months.

In parallel, consumer demand for convenient and personalised digital experiences has continued to grow, alongside the need to feel safe and secure when transacting online – in fact, 74 per cent of UK consumers ranked security of personal data as 'very important' when choosing who to transact with online. This creates a fine balance for business leaders (across diverse functions of fraud prevention, digital propositions, and product leads) who must ensure their strategies are friction-right.

Key trends for 2025

TransUnion is at the forefront of the UK identity and fraud ecosystem, with our objective to be our clients' "First Call" partner as they confront emerging typologies. Threat vectors our experts are discussing with our clients include:

The rise of AI and machine learning -
fraudsters have always been quick to adopt to new technologies, using them to scale operations and commit fraud with greater speed and precision. As AI democratisation lowers the barriers to entry, fraud rates are likely to rise and become more sophisticated, from deep-fake identities to manipulated identity and non-identity documents.

Synthetic identity fraud to become less hidden -
one of the fastest-growing global typologies in recent years, particularly in markets like the US, TransUnion expects greater focus in 2025. Often disguised as other typologies, the root cause often links to full or partial synthetic identity, inextricably linked to the proliferation of available data, including through breaches.

Devices to remain an accelerator to scalable fraud –
the rise of online activity means that devices connected to the internet are increasingly used as the tool to commit fraud, from overseas SIM farms to phone hacking in city centres to bot attacks.

Preparing for what's next

To meet the above challenges, leaders should consider the following:

Win control of the 'AI arms race' - AI provides the opportunity to fight fire with fire. By automating processes and investing in analytics, organisations can free up investigation teams to focus their resources where they're needed most and take a more proactive stance on fraud prevention.

Reimagine how we define identity –
identity is no longer just a combination of name, date of birth, and address; so much of who we are now exists online. To adapt, we need to consider a consumer's digital footprint and the story it tells and – specifically – the linkages between our physical and digital identity, and the devices we use. Only by combining these perspectives can we effectively distinguish between genuine and synthetic identities.

Leveraging biometrics and associated capabilities –
the UK has established itself as a global leader in the use of biometrics to help authenticate and engage with consumers, however, there is still further runway for this evolving technology. For example, we expect a shift to non-native, standalone biometrics technologies, which will leverage defences such as passive liveness checks and one-to-many matching.

How can fincrime professionals be more effective in the year ahead?

There is always a proliferation of techniques, technologies and tools to be considered for implementation, however, Fincrime practitioners should also prioritise personal and professional development. This means keeping up to date with market trends, learning how to respond to emerging threats, and increasing cross-sector collaboration.

Perhaps more importantly, though, is taking sufficient time to switch off and recharge. Our roles require us to juggle many competing items, from staying ahead of fraudsters to keeping internal stakeholders happy. This can take its toll, which is why it is important for practitioners to recognise burnout and prioritise mental wellbeing – this is what will make them successful in the long term.

What excites you most about the future?

We often talk about how well fraudsters innovate... but nothing breeds innovation faster than when fraud fighters rally together against a common cause. The technologies that have come to market in recent years to help solve for the threats faced today are extraordinary, but what is more encouraging is the talent entering the industry - anti-financial crime will always require a human-first approach, and we need fresh ideas, diverse experiences and new perspectives.

We are fortunate that - as fraud practitioners - there is a genuine purpose and passion to what we do. The technologies and processes that firms adopt are great facilitators of being able to prevent financial crime, but it's the people that make the real difference.

The road to crypto regulation and EU AML reform

Ian Mynot

Director,

Advanced Financial Crime Consulting

Follow on LinkedIn

"It's fair to say that despite successive directives, EU AML efforts have failed by a very large margin."

Ian Mynot

Ian Mynot
Director,
Advanced Financial Crime Consulting

Looking back at 2024

The key development in 2024 at an EU level was the adoption of the new AML package in April, consisting of the following elements:

- An AML Regulation which, for the first time, introduces directly applicable requirements on to firms, rather than requirements being implemented indirectly via directives. Therefore, it introduces a single EU rule-book for regulated firms to follow.
- A new AML directive (the 6th AML directive) providing new requirements on Member States.
- The introduction of the Anti-Money Laundering Authority (AMLA). This will oversee the AML supervisors across the EU, gathering data to understand risk and performance, set standards and also directly supervising the most risky entities.
- The Transfer of Funds Regulation, which requires crypto firms to capture and send certain customer information alongside a transaction, in order to improve the ability to trace illicit transactions.

These developments represent significant change. At the heart of the AML package is a recognition by the EU that the existing approach requires significant improvement. Indeed, it's fair to say that despite successive directives, EU AML efforts have failed, by a very large margin.

Industrial-scale money laundering has been experienced in the EU as demonstrated by a catalogue of high profile cases. This includes but is not limited to the succession of laundromat schemes in which European and UK structures were abused in the 2010s to allow billions of euros of funds from Russia to be assimilated into the global financial system. The package seeks to respond to these failings.

As well as the Transfer of Funds Regulation, 2024 was also a year that saw a focus on crypto regulation more broadly, as national competent authorities prepared to implement the Markets in Crypto Asset Regulation (MiCAR). MiCAR goes beyond AML and introduces wider regulation to provide transparency, protect consumers and encourage responsible growth in the industry. Crypto firms were watching keenly, in order to decide which jurisdiction to apply for a licence in, and then start to prepare for these applications.

Coupled with these developments on crypto regulation, after a supressed market at the start of the year, crypto asset prices surged towards the end of the year, on the back of the results of the US presidential election.

Preparing for what's next

AMLA will only be fully operational in 2028. So the implementation timeline for these changes appears, on the face of it, quite long. However, in 2025 it will start to recruit staff to its headquarters in Frankfurt, some systems and data will transfer from the European Banking Authority, and consultation will take place on some of the new rules.

What does this mean for regulated entities? The package as a whole brings with it more prescriptive requirements which will require significant work. It would be wise to assess these requirements as soon as possible because there will likely be increasing scrutiny on compliance by supervisors, particularly for large and high risk businesses who may fall under direct supervision from the AMLA.

Coupled with this, national regulators will be under increasing scrutiny from AMLA in the future. Regulators will be keen to show their effectiveness and robustness so that they can avoid censure. Over the coming years, we can expect to see enhanced scrutiny of firms, and an increase in enforcement actions for AML failings.

Large international banks will be a focus, but in addition it has been made clear that Crypto Asset Service Providers (CASPs) may also fall under direct supervision. Many CASPs are currently focused on preparing licensing applications under the Markets in Crypto Asset Regulation (MICAR) which introduces wider regulation to introduce transparency, protect consumers and encourage responsible growth.

However, CASPs that deprioritise improving their AML programmes will do so at their peril. Taking the opportunity to mature AML programmes in 2025 will prepare CASPs for likely attention from national supervisors in the run up to the AMLA going live.

And for the bigger CASPs that provide services across the EU and beyond, operating under multiple registrations and licences, if they do not focus on AML now, direct supervision from the new pan-European regulator is a distinct possibility.

Adapting to disintermediation: AI and blockchain in compliance

"What excites me most is the opportunity to be part of a movement that not only transforms banking but also enhances the security and integrity of financial systems."

Dr. Firas Nadim Habach

Dr. Firas Nadim Habach

Swiss Head of Financial Crime Compliance,

Revolut

Follow on LinkedIn

Dr. Firas Nadim Habach
Swiss Head of Financial Crime Compliance,
Revolut

Looking back at 2024

Reflecting on 2024, one of the most significant developments was the EU's accelerated push towards regulation in the digital asset space. The European Commission introduced the Markets in Crypto-Assets (MiCA) regulation, which aims to create a comprehensive regulatory framework for crypto markets within the EU. This is expected to help mitigate financial crime risks in a sector that has been increasingly exploited by bad actors. According to a Chainalysis report, in 2023 alone, $20 billion worth of cryptocurrency transactions were linked to illicit activities, a figure that continues to drive the need for regulation and compliance structures in the sector. The rapid rise in digital asset transactions, estimated to exceed $5 trillion in 2024, underscores the importance of such regulatory measures to ensure the integrity of the financial ecosystem.

Additionally, the collapse of FTX and Silicon Valley Bank in late 2023 highlighted the vulnerability of both traditional and digital finance to mismanagement and fraud. These events exposed systemic risks, with FTX's bankruptcy revealing over $8 billion in customer liabilities. This underscores the necessity for robust financial crime prevention measures to protect consumers and maintain market confidence.

Key trends for 2025

In 2025, one of the most defining trends in the financial crime industry will be the continued maturation of artificial intelligence, particularly large language models such as ChatGPT. As AI becomes increasingly integral to financial crime prevention, the financial services industry is expected to allocate $25 billion to AI technologies by 2025, according to PwC estimates. This investment will be crucial in enhancing transaction monitoring systems, with AI helping institutions manage the sheer volume of transactions.

The use of AI in areas like KYC and AML will be transformative. For example, the use of AI-driven algorithms can improve fraud detection by identifying suspicious patterns across multiple data sets. By 2025, global spending on KYC and AML solutions is projected to surpass $10 billion annually, as per Grand View Research. These AI solutions are expected to drastically reduce operational costs while improving efficiency in detecting fraudulent activities, reducing the time it takes to identify financial crime.

Furthermore, blockchain technology will continue to disrupt financial crime prevention. According to Deloitte, the value of blockchain's contribution to combating financial crime could reach $3.1 billion by 2025. Blockchain's transparency and immutability make it a powerful tool for identifying illicit activity, particularly in the growing realm of decentralised finance (DeFi).

Preparing for what's next

To stay ahead of the curve, the financial industry must embrace a hybrid approach that combines traditional financial crime controls with the innovative potential of blockchain and AI. The increasing use of neobanks and fintechs like Revolut and Chime—which have disrupted the traditional banking model by offering low-cost financial services—has led to an industry-wide shift toward disintermediation. In 2024, neobanks are estimated to serve over 200 million users worldwide, with growth projected to continue at a compound annual growth rate (CAGR) of 40%.

As the disintermediation trend accelerates, financial institutions must ensure that their compliance and financial crime frameworks evolve. The integration of AI-powered KYC and AML technologies will be essential in managing these new types of risks. Moreover, blockchain-based compliance solutions that leverage smart contracts to automate regulatory processes will provide further transparency and control.

Traditional financial services must also embrace collaboration with blockchain and AI experts, leveraging external partnerships to navigate the rapidly changing landscape. Cross-sector collaboration will be critical, particularly in developing shared AI models and regulatory technologies that can be applied across both traditional and digital finance. In fact, 80% of financial institutions are expected to adopt AI and machine learning technologies by 2025 to enhance compliance, according to Accenture.

How can fincrime professionals be more effective in the year ahead?

In 2025, financial crime professionals will need to broaden their horizons and challenge their understanding of both traditional finance and emerging technologies. Continuous learning will be vital as the industry increasingly embraces new tools. According to a 2024 survey by the Association of Certified Financial Crime Specialists (ACFCS), over 70% of financial crime professionals reported that AI and machine learning are integral to their strategy for the next five years, suggesting that these technologies will be central to staying ahead of new risks.

Professionals should focus on adopting a holistic approach to fraud detection and prevention by integrating AI with human insight. AI can flag suspicious transactions, but the interpretation of these alerts and the strategic decisions made thereafter will continue to rely heavily on the expertise of professionals. Additionally, professionals must be proactive in engaging with the evolving regulatory landscape, as over 50% of global financial institutions expect increased scrutiny from regulators in 2025, especially in the wake of high-profile failures and systemic risks in 2024.

What excites you the most about the future?

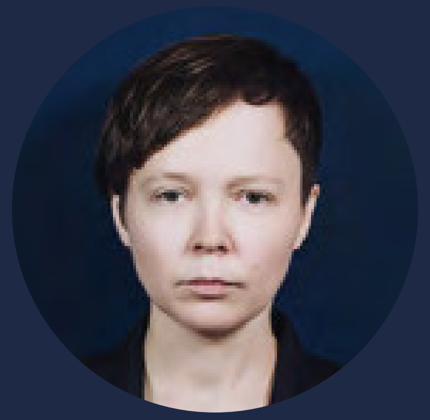
The future holds immense promise, especially with the growing integration of blockchain and AI in revolutionising financial crime prevention. According to McKinsey, blockchain's transparency and decentralised nature could reduce global money laundering costs by over $8 billion annually. What excites me most is the opportunity to be part of a movement that not only transforms banking but also enhances the security and integrity of financial systems.

This technological revolution will allow us to collaborate more effectively across sectors to address fraud and financial crime. The potential for blockchain and AI to work together to create real-time, transparent, and immutable financial ecosystems is enormous, and I look forward to playing a role in shaping that future. As the industry moves towards greater innovation, this collaboration promises to elevate both security and efficiency in financial systems, ultimately benefiting all stakeholders.

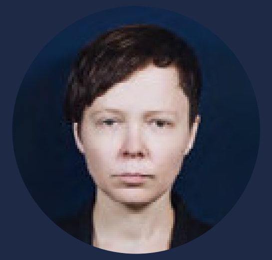
Why smarter work equals smarter AI

“AI, in general, has very limited capability to detect something that you haven’t seen before, because it learns from your past actions.”

Ester Eggert



Ester Eggert
Head of Product,
Salv
Follow on LinkedIn



Ester Eggert
Head of Product,
Salv

Looking back at 2024

The defining theme for 2024 was confusing legislation. Take mandatory reimbursement in the UK—it's a significant move, and the first legislation of its kind. So other jurisdictions are watching to see how it plays out in practice.

Similarly, the Instant Payments Regulation (IPR) is coming into force in the EU on January 9th 2025, yet the details haven't been fully published or understood. It's unclear at the national level how it's going to be implemented.

When I spoke to a couple of banks recently, they told me that no one really understands how IPR is going to work yet. That uncertainty sums up 2024: big changes arriving fast, while the industry tries to figure out how to respond effectively.

Key trends for 2025

If the theme of 2024 is confusing legislation then this paves the way for 2025: the year where we have to deal with it all. There's no point arguing against it or pointing out why something's not possible. The question financial institutions will be trying to answer is: what changes will they make to adapt in the smartest and most effective way?

Preparing for what's next

Looking ahead, organisations need to rethink how they work to enable deeper use cases for AI. Because the purpose of AI is to automate as much manual work as possible. But when it comes to financial crime detection, AI has very limited capability to identify something you haven't already detected. It learns from what you've been doing. Yes, it can provide incremental enhancements, but it's not going to deliver major breakthroughs on its own.

To take things to the next level, you need more data than just your own. So when AI is combined with collaboration, it can learn from broader intelligence and deliver far greater results.

It's about transforming how you work in the first place. If we want AI to become smarter, then how we work must become smarter first. By bringing collaboration and AI together, organisations can evolve beyond simple optimisation and really harness the power of both worlds.

Continuous learning and leveraging data more effectively

Jessica Cath

Partner, Financial Crime,
Thistle Initiatives
Follow on LinkedIn

"Our industry and community is incredible, with a whole host of intelligent, creative and interesting people all looking to create frameworks that work."

Jessica Cath

Jessica Cath
Partner, Financial Crime,
Thistle Initiatives

Looking back at 2024

2024 marked a pivotal and downright crazy year for financial crime risk management, shaped by significant challenges and developments in both technology and regulation. The key challenge has been the rise in fraud and cyber-enabled financial crimes. The proliferation of AI-driven fraud schemes, including deepfake scams and synthetic identity fraud, has challenged traditional detection methods. On top of this, regulatory tightening—such as the new APP fraud mandatory reimbursement requirements in the UK—has forced firms to adapt rapidly. This has often been in the context of challenging economic environments and smaller budgets, making adaptation even harder.

Globally, geopolitical tensions have further complicated AML and sanctions compliance, as firms grapple with dynamic and fragmented requirements across jurisdictions. Sanctions lists continue to change frequently and have become ever more complex.

Key trends for 2025

Looking ahead to 2025, several trends are poised to redefine the landscape. Chief among them is the integration of AI and ML in detecting, predicting, and mitigating risks. This is something we've all been talking about in the industry for a few years, but it's really establishing itself within financial crime control frameworks, and we're seeing some exciting new monitoring capabilities. Real-time transaction monitoring powered by generative AI will become mainstream, enabling more precise identification of anomalous behaviours—not just in the FinTech space, but also in more traditional sectors like wealth management.

Another key trend will be the increasing collaboration between public and private sectors, involving financial services as well as sectors such as social media, marketplaces, and telecommunications. Cross- sector information-sharing initiatives—something we've discussed for a long time—must now move forward at pace. In the UK, we've seen the Information Commissioner's Office (ICO) provide clear guidance and expectations on data sharing for fraud prevention. Additionally, initiatives like those launched by Meta in collaboration with several financial institutions will only continue to grow.

Preparing for what's next

To prepare for these shifts, the industry (and governments) must adopt a proactive, technology-first approach—but in a sensible, commercially-driven way. Firms will continue to face economic challenges in the UK, so any investment needs to be carefully considered and risk-based, prioritising expertise and the deployment of cutting-edge tools like AI/ML-driven analytics in areas with the highest exposure to financial crime risk. Any technology development must also consider people and process—these three components are essential for ensuring an effective anti-financial crime control framework.

How can fincrime professionals be more effective in the year ahead?

For individual financial crime professionals, the focus in 2025 should be on continuous learning and leveraging data effectively to integrate with various technology solutions. We encounter many firms that have invested in new technology but don't fully leverage its features due to a lack of understanding or because the data isn't clean enough for the tool to function properly. Developing expertise in financial crime technology is key but also a real challenge—MLROs need to be experts in regulatory change, people management, risk management, communication, and now, data and technology.

To navigate this effectively, MLROs should seek external support and advice when needed, but also ensure they have a solid team in place, supported by strong management information (MI) and monitoring processes to manage the tools they have in place.

What excites you the most about the future?

Personally, there are two things that excite me most about the future. The first is the technical developments—there's so much opportunity to monitor suspicious activity more effectively than ever before. But the second is simpler. I'm excited to continue working with the incredible people in the financial crime space. Our industry and community is full of intelligent, creative, and interesting individuals all striving to create frameworks that work.

By embracing innovation and continuing to collaborate, the industry can rise to meet the challenges of 2025 and beyond, turning threats into opportunities for meaningful change.

Why effective collaboration starts in-house

"What excites me is the shift towards proactive measures such as predictive analytics, behavioural risk modelling, and pre-emptive system designs that prevent crimes before they happen."

Pallavi Kapale

Pallavi Kapale
Senior Financial Crime Officer,
Bank of China
Follow on LinkedIn

Pallavi Kapale
Senior Financial Crime Officer,
Bank of China

Cultivating a culture of collaboration: the essential ingredient for preventing financial crime

Financial crime has a common enemy: organised networks that exploit financial systems for illegal profit. While the details of these networks vary—ranging from cybercriminals and money launderers to corrupt officials and human traffickers—they are united by their shared reliance on exploiting vulnerabilities within the global financial ecosystem.

Historically, financial crime detection has been reactive—catching fraud after it occurs. What excites me is the shift towards proactive measures such as predictive analytics, behavioural risk modelling, and preemptive system designs that aim to prevent crimes before they happen.

So, what needs to change? There is no one-size-fits-all solution.

From silos to building synergies

Developing a robust and comprehensive risk management framework requires integrating teams responsible for AML, fraud prevention, cybersecurity, and sanctions compliance. This cohesive and collaborative approach enables organisations to evaluate a wide range of risks, from potential cybersecurity breaches that could compromise sensitive data to operational vulnerabilities that could disrupt business continuity.

By facilitating open communication and sharing insights across these critical areas, teams can better identify threats, assess their impact, and implement effective strategies to mitigate risks.

Risk assessments - made to measure

Is your customer base primarily composed of vulnerable demographics? Understanding how to identify vulnerable and high-risk customers is crucial for effective risk management. For instance, recognising money mules during the onboarding process can be particularly difficult, as individuals might initially open accounts with good intentions but later become involved in fraudulent activities.

This highlights the importance of conducting thorough risk assessments, which are essential in evaluating the effectiveness of your Know Your Customer (KYC) procedures. It's vital to analyse how customer profiles were integrated into your systems to ensure potential risks are detected early and managed appropriately.

From silos to building synergies

Fraud prevention has often relied on a tick-box approach, but this strategy needs to evolve to effectively deter fraudulent activities. Fraud prevention should be considered a two-way conversation. One of the most powerful tools in this process is asking the right questions.

It's crucial to provide comprehensive fraud prevention training for all employees, with a specific focus on the First Line of Defence (1LOD). Staff should not just be trained to perform tick-box checks but also to engage customers in meaningful conversations when red flags arise. Based on my experience in fraud prevention, tick-box approaches are common but insufficient. We need to explore new training methods that encourage authentic, probing interactions with customers.

Collaboration amongst the 3LOD

It's essential to routinely convene teams from the Anti-Money Laundering (AML), fraud, cybersecurity, and legal departments to exchange insights, identify trends, and discuss relevant cases. Establishing shared goals across these departments will foster collaboration. By aligning them under a unified mission—such as the objective of reducing overall exposure to financial crime—rather than focusing on isolated metrics for each team, organisations can enhance their effectiveness.

Focus on training and awareness

Training should extend across all the 3LOD functions to help staff understand the broader financial crime ecosystem. For example, every Suspicious Activity Report (SAR) you receive should be investigated, and feedback should be provided on what was done well and what could be improved. On the fraud side, examine every loss to identify any patterns, and once again, explain what was good and what could be improved.

Although this approach may create extra work, it promotes a culture of collaboration that nurtures a healthy environment for preventing financial crime. Additionally, sharing findings with the 1LOD and communicating with branch staff can help identify unusual activities early on.

Fincrime's gradual AI boom

“Being able to share real-time data time in a way which is not anti-competitive is one of the most important things we could do in all areas of fraud and financial crime.”

James Coveney

James Coveney

Head of Data Science,

Zempler Bank

Follow on LinkedIn

James Coveney
Head of Data Science,
Zempler Bank

Looking back at 2024

The most significant change in the UK was the introduction of the Payment Systems Regulatory (PSR) APP scams Reimbursement Policy in October 2024. This, along with the PSR publishing bi-annual industry fraud metrics by institution, has had a material impact within the payments industry. All UK financial institutions impacted by the regulation have made significant investments in reducing APP fraud, both in terms of protecting their customers and tackling the use of their accounts by money mules. Alongside the internal efforts within each institution, many fraud technology providers have developed new products specifically targeting the reduction of APP fraud.

Key trends for 2025

I think we'll continue to see the use of AI by technology providers and, increasingly, by financial institutions themselves. The former is fairly well established, but internal use of AI is still at varying levels of maturity across the industry. In particular, I anticipate a shift towards approaches such as perpetual KYC and risk monitoring. This means algorithms and rules won't operate independently but will evolve as our understanding of fraud risk grows throughout the customer lifecycle.

I also expect fraudsters to continue using AI, with techniques like voice spoofing becoming more common, particularly in scams. This will drive innovation within the industry to develop countermeasures against these emerging threats.

Preparing for what's next

Clearly, the use of AI will be crucial, but I think a lot of focus will be placed on smarter and more personalised communication with customers. The Consumer Duty regulation mandates more personalisation, but it's also a very effective tool in fraud prevention. Moving away from generic, one-size-fits-all communications and instead asking customers questions more specific to the transaction they're making will help detect fraud more accurately and improve the customer experience.

Being able to use this richer data in algorithms would undoubtedly enhance the performance of AI, both in terms of fraud detection and preventing false positives. In particular, it would provide key data points for harder-to-detect fraud, such as sophisticated scams.

How can fincrime professionals be more effective in the year ahead?

One thing we could do as an industry is share data more widely and effectively. Initiatives like **Pay.UK's Enhanced Fraud Data** could have a significant impact on fraud prevention within the payments system. Being able to share real-time data in a way that doesn't undermine competition is one of the most important things we could do across all areas of fraud and financial crime. Things are definitely moving in the right direction, but current data sharing is still generally limited in sophistication and often reactive, rather than proactive.

What excites you the most about the future?

Given my role as Head of Data Science, seeing where we go with AI is particularly exciting. There's a lot of noise about AI bringing us to the cusp of major transformation across society and work, but I think the reality will be more gradual. Many organisations still have limited use of AI within financial crime, which provides one of the most compelling use cases. I think there's a long way to go before we see it embedded across all areas of an organisation's operations. Nonetheless, its use will certainly continue to become more widespread.

For me, the most interesting aspects of AI are the broader societal questions it raises. Issues like ethics and fairness are value judgments and can't be solved by technical experts alone. I'm fascinated to see the journey we go on as a society in balancing the pros and cons of AI as it becomes more pervasive in our daily lives. Undoubtedly, this will become a more prominent concern for politicians and regulators, so I expect—and hope—that responsibility will be as important as effectiveness when developing AI.

An AI inflection year: how 2024 sets the stage for 2025

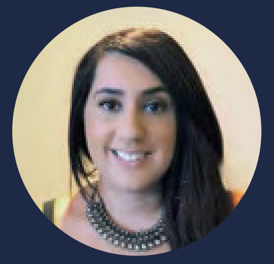
“By automating tedious processes, compliance teams can redirect their focus to higher-value, strategic work.”

Pinnie Balachandra

Pinnie Balachandra

Enterprise Customer Success Manager,
Hummingbird

Follow on LinkedIn



Pinnie Balachandra
Enterprise Customer Success Manager,
Hummingbird

Looking back at 2024

As 2024 comes to a close, it's clear that—like so many other industries—generative AI (GenAI) has taken center stage in the financial compliance landscape. But as AI's technical capabilities continue to grow by leaps and bounds, those on the ground have seen the conversation shift from general model performance to its applicability in solving industry-specific challenges.

At **Hummingbird**, we've observed a pivotal year where financial institutions of all shapes and sizes looked to AI to solve longstanding problems. In particular, we saw three themes dominate the year: the push for better data integration, the drive to automate manual workflows, and the unlocking of novel use cases tailored to compliance needs.

Data integration: Building bridges across systems

Data fragmentation and siloed systems are the perennial problems facing compliance teams. At most financial institutions, legacy systems often sit alongside newer platforms, creating gaps and roadblocks. But this is one area where Large Language Models (LLMs) have introduced a game-changing capability: their ability to ingest, interpret, and synthesise heterogeneous data types stands to transform the landscape.

For compliance teams, this means reconciling transaction data, customer profiles, and external watchlists into a unified format, enabling better risk assessment. The practical application of LLMs here isn't just about ingesting data; it's about contextualising it. For example, at Hummingbird, we've seen teams leverage AI to interpret historical and real-time data streams, accelerating investigations and ensuring no anomaly goes unnoticed.

Compliance automation: From tedious tasks to strategic work

For decades now, compliance professionals have often spent the bulk of their time on manual, repetitive tasks. Whether it's reviewing case files, manually transferring case data into Suspicious Activity Reports (SARs), or cross-referencing data sources, this work requires constant system and context-switching and is prone to errors.

But 2024 marked a turning point in the development of automation tools designed specifically for compliance workflows—intelligent automations that allow teams to set incredibly specific conditions for each automated action and receive an always-up-to-date audit log in return. These features—transparency, security, and auditability—are non-negotiable in this space, and in 2024, we saw a shift with the rise of automation tools purpose-built for compliance workflows. These tools allow teams to define specific conditions for automated actions, with comprehensive, up-to-date audit logs ensuring transparency and security. By automating tedious processes, compliance teams can redirect their focus to higher-value, strategic work.

New value: tailored Compliance AI use-cases

The early days of GenAI adoption were marked by generalised co-pilot tools, but—based on what we've observed—most of these tools ultimately have fairly limited functionality. When AI model capability is designed into purpose-built solutions, on the other hand, these new, more customised AI features bring entirely new value to compliance teams.

At Hummingbird, we've focused on the latter approach, building compliance-specific features like our CDD-oriented AI File Summarisation and the AML-focused SAR Narrative Generation. These new tools, which are built using customised model architecture and fine-tuned to meet compliance-level standards for transparency and reportability, allow investigators to reduce manual effort in areas of the compliance workflow that were previously seen as unavoidable. These innovations are reshaping how compliance teams operate, shifting their role from task execution to strategic decision-making.

Looking ahead to 2025

As we head into 2025, we believe that the momentum around GenAI in financial compliance will only continue to grow. Specifically, we foresee three key trends:

1. Greater emphasis on explainability and trust
   Regulators and institutions alike will demand transparency in how AI models make decisions, driving further refinement of auditability features. But innovation and new AI use-cases will continue to proliferate.
2. Expansion of real-time capabilities
   With financial crimes evolving rapidly, tools that can process and act on data in real time will be indispensable. We're already seeing this in the fraud space, and expect it to spread to other practice areas.
3. Integration with broader compliance ecosystems
   We expect to see tighter integration between GenAI solutions and existing compliance platforms, helping create truly seamless workflows and allowing teams to access impactful, actionable insights.

At Hummingbird, we're excited to support compliance teams as they navigate this rapidly evolving landscape. The challenges ahead are complex, but the opportunities to innovate have never been greater. Together, we can create safer, more efficient, and more resilient financial systems.

UK companies house reform: it’s not over yet

“Economic criminals use corporate entities for much the same reasons that burglars use gloves.”

Ray Blake

Ray Blake

Presenter of The Dark Money Files podcast & FinCrime SME at Risk Alert 24/7

Follow on LinkedIn

Ray Blake
Presenter of The Dark Money Files podcast & FinCrime SME at Risk Alert 24/7

Looking back at 2024

In recent years, Graham Barrow and I have regularly sought to highlight how criminals exploit UK corporate entities. Specifically, we've examined how the ease of forming companies online via the Companies House website has played into the hands of criminals. The passage of the UK's Economic Crime and Corporate Transparency Act in 2023 — granting Companies House extensive new powers and responsibilities to address these abuses — was widely welcomed. However, those closely involved in the UK anti-financial crime sector were less sanguine about the reform.

When a law is passed, the general public and politicians often assume that the problem is fixed. It's presumed that the powers are immediately applied and are entirely effective. Yet, as is often the case, that is not the reality here. Economic criminals use corporate entities for much the same reasons that burglars use gloves. They continue to exploit the UK corporate registry, taking advantage of its cheap and easy access to these tools of their trade. This exploitation will likely persist for some time. Let's briefly explore why.

First of all, there are currently around 6 million active companies listed on the UK registry. Companies House now has the responsibility to assess the bona fides of all these companies, as well as the 2,000-3,000 new entities added every day. It's unrealistic to expect this to be resolved overnight. Furthermore, many of the powers granted to Companies House under the 2023 Act are not yet available and require secondary legislation.

The first of these new powers came into effect on 4th March 2024. From that date, Companies House began the process of cleaning up information on the existing registers and challenging newly submitted data. Companies House anticipates that "work will be ongoing over a number of years as we remove incorrect or fraudulent information from the register in priority order."[1]

Companies House has outlined a plan for implementing other measures under the Act, including identity verification for officers of new and existing companies. This plan has milestone points scheduled throughout 2025 and 2026, but it notes that it depends on the passage of 50 statutory instruments over an 18-month period. Even if everything proceeds smoothly, Companies House projects that "implementation activity and transitional periods will continue until completion in 2027."[2]

Throughout this period of reform, Companies House is providing transparency and acknowledges the problems those of us in the industry see. In its first strategic intelligence assessment, it states, "It is almost certain that the scale of money laundering through UK limited companies is underestimated."[3]

The extensive new powers granted to Companies House are a welcome step forward, but the implementation of these measures will take time and sustained effort. With millions of active companies to assess and numerous statutory instruments to pass, the task of cleaning up the UK corporate registry is monumental. While the passage of the UK's Economic Crime and Corporate Transparency Act in 2023 marks a significant step forward in combating financial crime, the journey is far from over.

[1] Economic Crime and Corporate Transparency Act: outline transition plan for Companies House, 16 October 2024
[2] ibid
[3] Companies House strategic intelligence assessment, 24 October 2024

Hybrid threats: cyber crime meets traditional financial crime

> “The growing recognition of financial crime as a global challenge requiring cross-sector collaboration is inspiring.”
>
> **Ian Christie**

Ian Christie
Co-Founder,
FincSelect

Follow on LinkedIn

Ian Christie
Co-Founder,
FincSelect

Looking back at 2024

2024 was marked by several transformative developments across the fincrime landscape: The rise of cryptocurrency adoption for payments, the resurgence of Bitcoin's value, the introduction of the APP fraud reimbursement scheme, and the growing challenges posed by socio-political conflicts, such as those involving Russia and Israel.

A rise in the adoption of cryptocurrencies as a mainstream payment mechanism was coupled with Bitcoin and other cryptocurrencies experiencing a sharp increase in value in November. This adoption brings new risks, including an increase in crypto-enabled financial crime. Decentralised finance (DeFi) platforms and peer-to-peer transactions, while innovative and inclusive, are increasingly exploited for money laundering, illicit financing, and sanctions evasion. The anonymity afforded by cryptocurrencies remains a double-edged sword—ushering in financial inclusion while creating vulnerabilities for criminal exploitation.

We also saw the UK financial industry prepare for and implement the PSR's APP Scam Reimbursement Scheme in October. This was coupled with an expansion of anti-fraud legislation, which saw traditional financial crime teams and MLROs expand their roles to include fraud expertise in both controls and systems.

In parallel, geopolitical tensions, particularly the ongoing conflicts involving Russia and Israel, added more complexity to the fincrime landscape. Sanctions evasion strategies became more sophisticated, with bad actors leveraging cryptocurrencies and alternative financial systems to bypass restrictions. Financial institutions also faced a rise in fraud and cyberattacks linked to politically motivated groups, placing further pressure on institutions to bolster their defensive measures.

These developments underscored the urgent need for enhanced surveillance mechanisms, real-time risk assessment tools, and cross-border collaboration to counter emerging threats effectively.

Key trends for 2025

2025 is poised to be transformative for financial crime prevention, driven by several key trends:

Mass adoption of cryptocurrency and associated risks
The continued rise in Bitcoin's value and the mainstream adoption of cryptocurrencies for payments will redefine the fincrime landscape. While cryptocurrency adoption has democratised finance, it also introduces new challenges, such as detecting illicit transactions in a decentralised environment. Financial institutions will need to invest in blockchain analytics tools capable of identifying patterns, tracking transactions, and mitigating risks associated with crypto-enabled crime.

Challenges from geopolitical conflicts
Socio-political instability, including the prolonged Russia-Ukraine war and tensions involving Israel, will continue to fuel financial crime. Sanctions will remain a critical geopolitical tool, but their enforcement will become increasingly difficult as international players grapple with adherence to international law while criminals refine their evasion tactics. Financial institutions must strengthen their sanctions compliance frameworks and adopt AI-driven tools to monitor cross-border transactions for signs of circumvention.

Hybrid threats: cyber crime and fraud meets traditional financial crime
Cyber-enabled threats, often linked to geopolitical actors, will increasingly merge with traditional fincrime tactics. For instance, ransomware attacks are likely to target financial systems more frequently, with ransom payments often demanded in cryptocurrencies. This hybrid threat landscape will require a unified approach that combines cyber security measures with anti-financial crime expertise. Similarly, the increase in fraud, including APP scams and the use of deepfakes and AI, will force financial crime tactics to adapt at speed.

Preparing for what's next

To adapt to these changes, the fincrime industry will need to embrace several strategies:

Advanced blockchain analytics
As cryptocurrency adoption grows, financial institutions must deploy advanced blockchain analytics tools to trace transactions and identify suspicious activity. These tools should integrate seamlessly with existing AML and fraud detection systems, providing real-time insights into crypto transactions.

Enhanced sanctions compliance
In light of geopolitical tensions, sanctions compliance must evolve to meet the challenges of 2025. Institutions should prioritise real-time transaction screening tools that incorporate AI and machine learning to identify patterns indicative of sanctions evasion. Collaboration with regulators and intelligence agencies will also be critical to staying ahead of bad actors.

Cross-border collaboration
Tackling financial crime in a globalised world requires stronger cross-border cooperation. Financial institutions, regulators and law enforcement agencies must work together to share intelligence and align on strategies for combating emerging threats, particularly those linked to geopolitical instability and crypto-enabled crime.

Cyber Resilience for Financial Systems
Institutions must strengthen their cyber defences to counter the hybrid threats emerging from the convergence of cybercrime, fraud and traditional financial crime. This includes implementing advanced threat detection systems, conducting regular penetration tests, and training staff to recognise and respond to cyber-enabled financial crime tactics.

How can fincrime professionals be more effective in the year ahead?

Embracing crypto regulation will be key to greater effectiveness in 2025.

Fincrime professionals should focus on navigating and shaping the regulatory environment surrounding cryptocurrencies. Proactively engaging with regulators to establish clear, actionable guidelines for crypto compliance will enable institutions to mitigate risks while harnessing the opportunities presented by digital assets. Building expertise in cryptocurrency transactions, smart contracts, and DeFi will also be essential for staying ahead of emerging threats.

What excites you most about the future?

The intersection of mass cryptocurrency adoption and cutting-edge technology excites me the most about the future. Blockchain's potential to revolutionise transparency and efficiency in financial systems is immense, offering a unique opportunity to combat financial crime at its core.

Also, the growing recognition of financial crime as a global challenge requiring cross-sector collaboration is inspiring. The willingness of governments, financial institutions, and technology providers to work together signals a promising shift towards a more united and resilient approach to financial crime prevention. Despite the challenges, 2025 holds the potential for significant progress in building a safer and more transparent financial ecosystem.

In summary, 2025 will demand bold, innovative approaches to tackle a variety of challenges. By embracing advanced technologies, adapting to regulatory changes, and fostering collaboration, the fincrime industry can not only mitigate risks but also seize opportunities for meaningful impact.

Collaboration and intelligence sharing is happening in a big way

“We haven’t seen the year of AI in regtech... yet. That will happen in maybe three or four years time.”

Taavi Tamkivi

Taavi Tamkivi

CEO and Co-Founder,
Salv

Follow on LinkedIn

Taavi Tamkivi
CEO and Co-Founder,
Salv

Looking back at 2024

I would call out three trends for 2024: increasing volume and complexity of regulations, evolving best practices towards higher collaboration, and the increasing overlap of the fraud and AML worlds.

Regulation-wise, it's like there's always something new for fincrime fighters to think about. 2024 was the year of the EU AML Package and the introduction of the AMLA. It came after very long discussions and debates, with Salv contributing best practices around effective collaboration. Now that the AMLA's live, its selected path and defined guidelines will massively dictate what happens over the coming years in our space across the EU.

Then in the UK, we had mandatory reimbursement for authorised push payment (APP) fraud, which is directly impacting financial institutions in the UK itself of course. But it's also interesting for crime fighters across continental Europe as we'll see a similar reimbursement legislation introduced soon.

The second trend, crime fighting industry best practices, is really in people's hearts and minds. 2024 saw lots of discussion around collaboration, along with some successes and some failures. It's been a dominant theme on almost all conference panels and keynotes, the famous AMLR Article 75 being at the centre, as well as the existing practices covered under existing regulations. As we head into 2025, we'll see this chatter turn into action that defines better ways of fighting financial crime.

Finally, we saw the fraud and AML worlds come closer together. When we talk about the size of the authorised push payment fraud problem across Europe, especially in regions where instant payments are heavily used, these fraud cases are falling between the AML and fraud teams. Quite often, in larger banks, AML people are resolving the APP fraud cases and in fintechs, there are fraud teams more heavily involved. So, these two distinctly different disciplines have learnt now that they need to be merging closer together—and I believe the industry can benefit from that.

While it's promising to see politicians and regulators involved to resolve the APP fraud problem, it's important to remember that it's still a hundred or maybe a thousand times smaller of a problem than the money laundering and terrorist financing happening around the world. It's not always tangible, but it's there. So, the risk is we focus too much on APP fraud, then we might forget or we deprioritise the biggest problems we face: proceeds made from drug and human trafficking, bribery and corruption, earnings from war crime that are funding terrorism.

Key trends for 2025

We will start to see the outcome of new regulations — financial institutions bringing in new policies and procedures, bringing in new technologies and forming new partnerships. I'm thinking of the AMLA especially and the new EU organisation which is being created to support it. The first Head of the AMLA, Bruna Szego, was elected in late November. And this person will step into the role and begin building up the whole organisation, which will lead all European regulators in the years to come. I don't want to over-estimate the importance of one person, but there's a face of the AMLA organisation, who is responsible for shaping its future, which is super exciting.

The next driver on my mind is the continued adoption of collaborative fincrime solutions. In some countries, collaboration efforts were closed down and are getting started from scratch again. But at the same time, we also saw a strong pattern of banking associations starting their search for a collaborative platform they can use to bring their members together with, which is promising. I anticipate that many of these countries will find a suitable platform, make a decision in 2025, and begin implementing it. I really hope that whichever platforms are chosen, they'll be able to speak to each other, or we'll still be sitting in silos.

At Salv, we have a collaborative platform for fincrime live in two EU countries, partial presence in three more, connecting over hundreds of private and several public sector entities domestically and cross-border , which is a great start, but I expect to see as many as ten countries running trials by the end of 2025.

Finally, I feel like we're still in this funny period with AI, where lots of companies are still soul searching. In financial services, you're dealing with discreet information, regulation and a lot of complexity. So there's lots of risks to consider and balance. It's simple enough to have virtual assistants and other cool AI tools working around the edges, but it's very hard to implement these bulletproof AI systems at true scale, following hard requirements like banking secrecy, GDPR, auditability, data retention etc. So, for me, in the regtech space, we haven't seen the year of AI yet. That will happen in maybe three or four years time.

It will definitely happen, but the industry needs more time.

What excites you most about the future?

Unsurprisingly for me, it's collaboration and intelligence sharing. That's a bet we made five years ago, a crazy idea we had after we spoke to a couple of customers wanting to exchange counterparty intelligence between themselves, with no clear procedural, technical nor legal basis for doing it.

We were a super young company at the time, and from that idea, we got invited to an FCA hackathon where we started to test this idea out for real. So, I'm super excited to fast forward five years and see that it's actually starting to happen on a large scale. People, organisations and legislators are all talking about collaboration and what happens next. The processes are in place, the legal framework clear, business cases are getting defined, and our technology has been tested and used for years by hundreds of companies.

We've had this vision for five years and so, emotionally, that's the most exciting part, to see it beginning to come true.

Conclusion

Anyone working to fight financial crime knows that the landscape is constantly evolving. Criminals move and think quickly, while financial institutions, governments and law enforcement devise methods to stop them.

The challenges raised in this predictions e-book highlight a growing idea: collaboration, innovation and adaptability in fincrime have become essential. Although we don't have a time machine to predict the future, the experts in this report give us a clear roadmap for tackling the challenges to come.

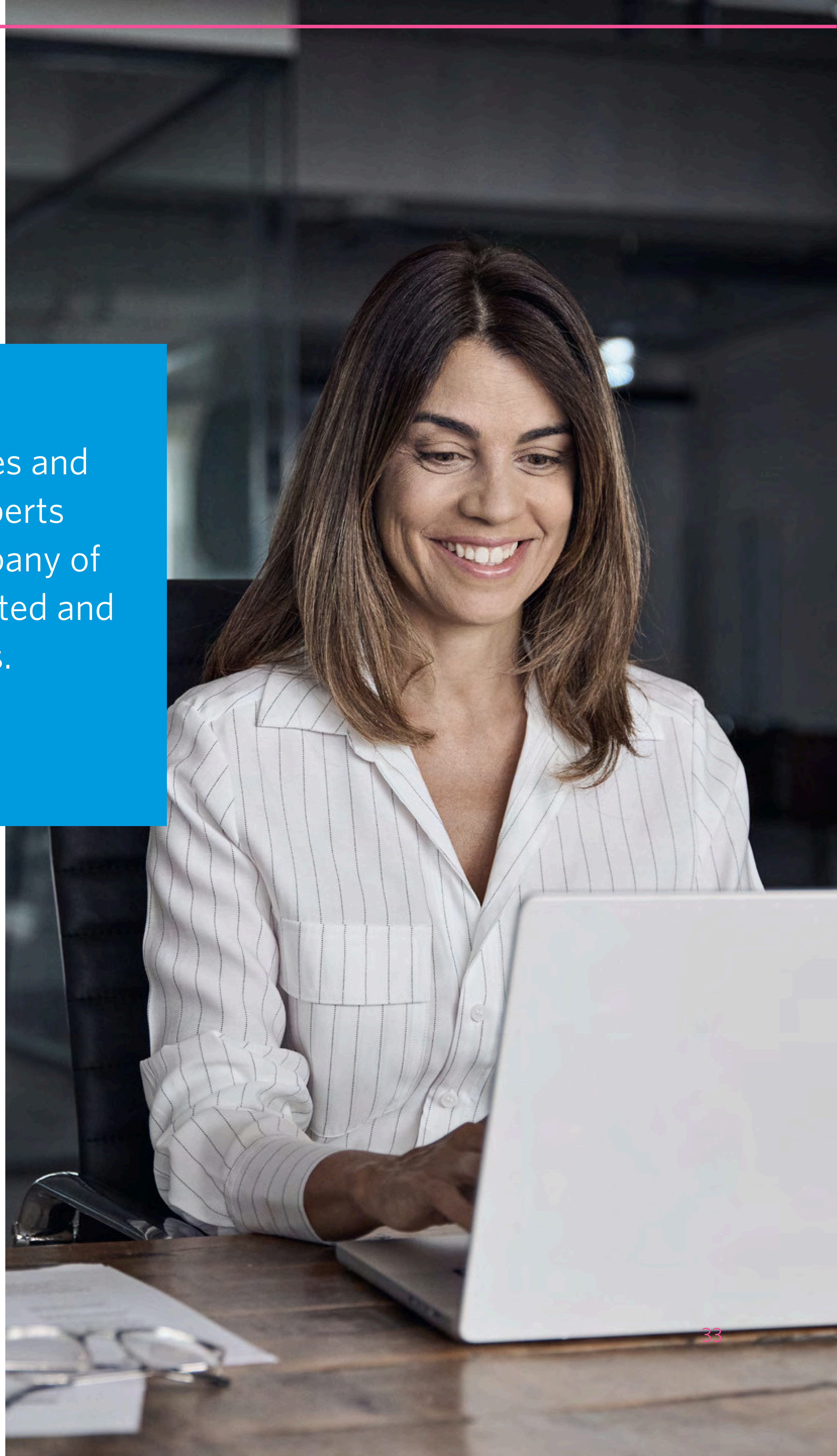
AI will play a central role, both for criminals and the industry, as organisations win back control of the AI arms race through targeted investments and stronger cross-section collaboration. Similarly, new regulations will demand not only improved tools but also a cultural shift toward proactive, risk-based approaches.

Beyond the technological changes to come, contributors emphasised the human dimension of this fight. From addressing burnout among practitioners to fostering a spirit of collaboration across public and private sectors, the financial crime community must invest in its people as much as in its tools.

The year ahead is filled with opportunity. Institutions that embrace emerging technologies, strengthen cross-sector partnerships, and remain agile in the face of regulatory change will be well-positioned to lead the charge against financial crime. By doing so, they won't just safeguard their operations—they will help shape a financial system that is more secure, ethical, and resilient.

Perhaps one of the most encouraging findings in this report is just how rewarding the sector is to work in. Despite the stresses and challenges, our experts delight in the company of their smart, dedicated and creative colleagues.

Despite the stresses and challenges, our experts delight in the company of their smart, dedicated and creative colleagues.



About us

Salv empowers financial institutions to beat financial crime with a SaaS platform that helps them detect money laundering, share intelligence, and stop fraud.

Criminals work in networks, so financial organisations should too. With the world's first fincrime platform that enables intelligence sharing, Salv helps banks, fintechs, and payment service providers fight financial crime more effectively and recover 80% more stolen funds.

More than 100 companies across Europe use Salv to centralise their AML data, exchange intelligence, automate repetitive tasks, and reduce false positive alerts. As a result, they can beat more criminals and protect their customers better.

Led by a team of crime fighters and data scientists who helped scale fincrime operations for Wise and Skype, Salv is a regulated partner and licensed KYC data processor on a mission to make the world a safer place by beating financial crime.

Our customers

LHV · TRUELAYER · coop Pank · zen · Bigbank · SEB · inbank · montonio · OP Bank · Luminor

rewire · KROO · MONEVIUM · deVere · Swedbank · JUNI · Citadele · Taptap Send · change · swile

Contact us

Book a Salv demo today sales@salv.com salv.com