



# Emerging Trends

## Navigating the Future of the FEC Compliance Landscape

May 2024

# Contents

01	Foreword	03
02	Trends & call to action	08
03	Interviews	22
	Steffie Schwillens	23
	Tom van de Laar & Robin de Jongh	28
	Hennie Verbeek-Kusters	32
	Norbert Siegers	36
	Patrick Özer & Jori van Schijndel	39
	Tom Loonen	45
	Hanna Deleanu & Jaap van der Molen	47
	Mark Lamers	52
	Laura van Geest	54
	Karlijn Jeurig-Koel & Wibout de Klijne	57
	Anita van Dis	63
	Timothy Goodrick	68
	Idzard van Eeghen	72
	Wim Huisman	76
	Andrea Wiegman	82
04	How KPMG can help	86
05	Acknowledgements	86
06	Contacts	87

**01**

# Foreword

---

# Foreword



**Leen Groen**

**Partner Forensic, Integrity and Compliance – KPMG**



**“Financial institutions and regulators should focus more on catching the big fish”, a sore citation from one of the professionals interviewed for this publication.”**

**Financial economic crime (FEC), such as fraud, corruption, money laundering and evasion of sanction regulations is a serious risk for society. For financial institutions, non-compliance with laws and regulations can lead to, among other things, reputational damage, including loss of trust from customers, and substantial fines and penalties. As non-compliance could reasonably result in a material effect on the financial statements, investors and auditors are putting more focus on those laws and regulations. New and amended laws are being introduced, and regulatory and enforcement authorities, as well as financial institutions, are increasing their efforts to combat FEC. In short, a lot is happening in the FEC domain.**

This publication, 'Emerging Trends: Navigating the Future of the FEC Compliance Landscape', is the outcome of a series of interviews held

by our KPMG NL Forensic Financial Economic Crime team. These interviews engaged thought leaders who are active across the FEC domain in the Netherlands, including leaders in the banking industry, academia and regulatory bodies, trendwatchers, the public prosecutor, and consultants. They shared their personal motivations and insights into trends, developments, opportunities and challenges, such as the integration of robotics and Artificial Intelligence in the area of FEC.

This publication is a great read and I trust that it brings you fresh perspectives or reinforce existing ones, and contributes to the aim of effectively combatting FEC and subsequently creating a safer society. As stated by one of the interviewees, “financial economic crime prevention is a permanent commitment”. Another interviewee stated that “the way we combat financial economic crime is an evolution, rather than a revolution”. Generally, the interviewees do not anticipate significant fundamental changes in the way FEC is combatted, but I did note, among other things, the following key messages:

- The growing maturity of FEC prevention, detection and response within financial institutions, especially banks, combined with supervisors taking a less rule-based stance, allows financial institutions to operate in a more risk-based manner. By doing so, instead of taking technical compliance as a mantra, the effectiveness of the compliance efforts will increase.

- The central government should put more energy into the fight against FEC and put it higher on the agenda, with a clear and prioritised strategy. From both a compliance and a commercial perspective, there is a need for a more holistic approach towards client management, and integrating credit risks, integrity risks and ESG risks, while paying more attention to optimising customer experience.
- There is a need for a more in-depth and data-driven analysis of integrity risks, and together with a clear FEC strategy, this should form the basis for an effective compliance framework.
- Enhancing collaboration and information sharing between public and private parties involved in combatting FEC – at both national and international level – is essential. It is widely recognised that the fight against FEC cannot be fought alone. Criminals do not stop at national borders, so nor should initiatives to share information in partnerships. We need to move towards a more continuous KYC approach (also referred to as 'perpetual KYC') by making use of dynamic customer and transaction data.
- Increased focus of enforcement authorities is anticipated on other sectors than banks, such as real estate and investment funds.
- With an influx of data scientists and a focus on more complex cases, the total number of KYC analysts will decrease, while the required level of expertise and analytical capabilities will increase.
- There is a balancing act between combatting FEC and adhering to data privacy legislation.
- The rapid development and use of new and smart technologies, such as blockchain, Artificial Intelligence, and privacy-enhancing techniques, will contribute positively to a more effective and cost-efficient fight against FEC.

In this publication, you will read more about the above and other key messages. We do not know how fast the way we fight FEC will change and whether or not there will be a paradigm shift, but it would be good to keep in mind the statement made by one of the interviewees: "changes are coming much faster than anyone has anticipated!".

Let us continue our fight against FEC and take into account the valuable insights obtained from the interviews. Finally, I would like to thank those interviewed and my Forensic team members and other KPMG colleagues who contributed to this publication.

**Leen Groen**

# Foreword



**Evelyn Bell**

**Director Forensic, Integrity and Compliance – KPMG**

**The risk that financial institutions are misused for money laundering and other forms of financial economic crime is ever-present. At the same time, financial crime is continuously changing and becoming increasingly complex. Not only because of the level of sophistication and use of new technologies by criminals, but also because of changing laws and regulations and increasing societal expectations. New laws create new crimes. Equally, new technologies create new opportunities for criminals to launder illegal proceeds. Navigating through the complex landscape of financial economic crime compliance requires organisations to be agile and purpose-driven.**

Financial institutions are expected to actively detect an ever-expanding range of crimes. This trend also follows from the expanding scope of predicate offences as reflected in the EU anti-money laundering directives. While the first directive solely focused on illicit drug trafficking as a predicate offence, the second one broadened the scope to include the activities of criminal organisations and terrorism. The list of predicate offences was further expanded with, among other things, bribery and corruption, terrorist financing and fraud (AMLD3), tax crimes (AMLD4), and environmental crimes and cybercrime (AMLD6). There will always be a financial flow linked to illicit activities, which underscores

the central role of financial institutions in the fight against financial economic crime. Through their knowledge of customers and transactions, financial institutions are uniquely positioned to assess and identify risks related to, for example, forced labour and human rights violations in their customer's supply chain. Collaboration is essential as the crime problem is too large to tackle in isolation.

I observe that financial institutions are now more than ready to shift from technical compliance to meaningful and effective compliance. But what is needed to achieve this and how can financial institutions keep pace with ever-expanding requirements and increasing societal expectations? These questions are addressed in this publication by experts and thought leaders on financial crime compliance in the Netherlands.



**Collaboration is essential as the crime problem is too large to tackle in isolation."**

It builds upon the work 'Financial Crime: A Paradigm Shift', produced by my colleagues from KPMG Australia, who interviewed worldwide experts a number of years ago. The current publication gives a unique insight into the Dutch market and the challenges resulting from the unique regulatory environment of the EU.

The aim is to assess the present landscape, discern any alterations, and pinpoint the necessary shifts in the future of financial crime compliance to advance with clear purpose.

The interviews were held between November 2023 and February 2024. On 12 and 13 February 2024, the final texts of the provisional agreements on the AMLD6 and Anti-Money Laundering Regulation (AMLR) were published. The AMLR may have an impact on the way TMNL operates.

Norbert Siegers, the CEO of TMNL, reflects upon the regulatory developments in his (updated) interview. Reflecting upon the interviews, the following thoughts about the future stood out for me:

- Significant steps can only be taken with a centralised, national risk appetite and crime prevention strategy.
- Public-private and private-private partnerships will become more effective through sharing of information, data and, most importantly, trust among the participating parties.
- Legal barriers hindering increased information sharing among institutions are expected to be addressed, given the current privacy impact arising from limitations in obtaining insights based on data.
- Current and emerging regulations force financial institutions to increasingly measure, disclose and report on social issues. This requires an organisational mindset that strategically focuses on change, adaptation and transparency vis-à-vis stakeholders, while balancing the commercial goals.

- New technologies bring opportunities for criminals and, consequently, new forms of crime can only be tackled if institutions embrace new technologies.
- Effectiveness in the fight against FEC requires a diverse workforce that can bring in different perspectives, and a focus on opportunities rather than only on risks.

Overall, the paradigm shift requires a holistic view of financial crime compliance which expands beyond single financial institutions. The transition to a new way of thinking – one that recognises and balances interests of different parties in a partnership – can unlock new opportunities for financial crime prevention. A future-proof financial crime compliance vision and strategy starts with understanding the emerging risks and opportunities, while placing these in the current societal context. I hope that our clients and other stakeholders find this publication useful as a starting point for understanding their risk environment and delivering on their promises. Having listened to these different perspectives, I am confident that we can contribute to the fight against financial crime as long as we work as a collective on the basis of trust.

**Evelyn Bell**

**02**

**Emerging  
trends & call to  
action**

---



## EMERGING TRENDS

Thought leaders and experts in the FEC domain foresee an increasing complexity due to increased geopolitical tensions, ever-expanding laws and regulations and a more challenging and complex threat landscape as a result of new technologies, which are also misused by criminals to commit new forms of fraud. Based on our interviews with 19 thought leaders, we have identified six major trends that we believe will change the financial crime compliance landscape in the next five to ten years:

### 01 Advancing with purpose



Enhance effectiveness of crime prevention efforts with the end-goal in mind.

### 02 Maturity in Compliance



Increased focus on the design of quality assurance, monitoring and reporting processes.

### 03 Data- and technology-driven progress



Data and technology have the potential to transform financial crimes compliance. Progress is also held back by laws and regulations.

### 04 Dynamic threat and regulatory landscape



Geopolitical developments impact the fight against FEC. Threat landscape is impacted through the use of new technologies by criminals.

### 05 Convergence and automation of monitoring capabilities



Integrated customer monitoring using different data sources to create one single customer view and promptly respond to emerging risks. The automation of case management activities.

### 06 Increased information sharing and data privacy



Deliver greater results and disruption of criminals through strategic data sharing using public-private and private-private partnerships.

# KPMG Point of view

## Our view on the identified emerging trends



### Advancing with purpose

Financial institutions will enhance the effectiveness of their crime prevention efforts by focusing more and more on the end goal instead of the process itself and by placing trust in their own mature risk management systems. This end goal considers the institution's contribution to society – in the form of crime prevention – rather than mere technical compliance. This shift requires courage: courage to invest in new technologies and courage to be patient, as it takes time to achieve desired results and courage to consider new approaches.

Advancing with purpose requires a financial crime compliance strategy and clear communication on what an institution aims to achieve with its strategy. It is expected that the end goal will increasingly consider the spirit of the law. To be effective, it is essential that the strategy is clearly communicated throughout the organisation and fosters a culture where trust can be placed in the institution's own mature risk management frameworks.



### Maturity in compliance

The move from a rule-based approach to risk-based compliance is already taking place. We expect this to continue over the next decade. With this shift, we also observe that regulators will increasingly scrutinize the organisation's compliance framework's maturity rather than focus on low-hanging fruit, such as whether or not a specific document is available in the client file.

Regulatory focus on the maturity of compliance is expected to go hand in hand with an increased focus on the design of quality assurance, monitoring and reporting processes, the organisational governance and tone at the top. We believe that institution-wide risk assessments, such as the systematic integrity risk analysis (SIRA) will serve as a better basis for the institution's risk and control framework, as it will be increasingly data- and technology-driven. We also believe that more maturity in compliance requires a strong risk culture where knowledge of people across the organisation is brought together rather than remaining within existing silos.

As institutions are maturing in compliance, we also expect the customer to be engaged as a 'partner in compliance' rather than a subject of investigation. Financial institutions will increasingly seek means to incentivise customers to support them in meeting their regulatory obligations and fighting financial crime.

03



### Data and technology driven progress

It is generally acknowledged that data and technology have the potential to transform financial crime compliance. Although the use of data will increase, we also understand that data will never be perfect. Sound decision-making is possible with less than perfect data, as long as data limitations and potential biases are understood and evaluated. Effective data governance, including risk-based approaches to data lineage, will enable the institution to understand and rely on data output.

We believe that financial institutions will also look to move away from disjointed technology systems to an integrated solution supported by strategy. It is essential for financial institutions to define critical measures of success throughout the implementation process while taking a long-term horizon. In this vein, institutions are also increasingly realising that it is no longer efficient and effective to build all their technology systems in-house, because other parties can simply do it better at lower cost. Therefore, they are reconsidering their approach towards outsourcing.



### Dynamic threat and regulatory landscape

Geopolitical developments increasingly impact the fight against financial economic crime. Especially Russia's invasion of Ukraine in 2022 has led to a surge in sanctions and export controls, prompting thematic investigations from the regulator DNB on sanctions screening capabilities. U.S. sanctions against China began in 2018 and also affect financial institutions that have a U.S. presence or nexus. The geopolitical shifts also impact law enforcement in the area of financial economic crime. For the Dutch FIU and Public Prosecution Service, for example, the exchange of intelligence with Russia is no longer possible, and they must be wary of 'hidden' intelligence requests coming from aggressive state actors.

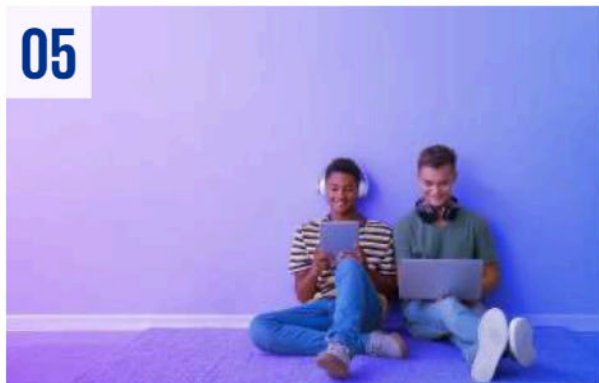
The threat landscape will also continue to evolve. As noted above, new technologies can bring new opportunities for the effectiveness and efficiency of financial crime prevention. However, they can also be misused by criminals to perpetrate new forms of crime. One example is what we call the 'double-edged sword' of AI. AI has the capability to optimise financial crime compliance; yet, at the same time, AI also makes it easier than ever before to commit crimes. Think of deepfakes and synthetic identities (entirely fictional identities created by combining diverse data sets using AI).

We expect these fake identities to be increasingly utilised to apply for credit cards, loans, or other financial products. Once the criminals max out the credit line's profits, they disappear, leaving financial institutions with substantial losses.

Such easily scalable forms of crime will pose significant challenges to traditional financial crime prevention efforts. Current data quality issues will pale in comparison to the difficulties of distinguishing synthetic persons from real ones (e.g., also consider AI calling customer service centres, while the responder is unable to detect that this is not a real person).

The shifts in geopolitical relations and changes in the threat landscape caused by technological advancements also impact the regulatory landscape. The EU's sweeping reforms of its AML/CTF framework will keep institutions, compliance officers, regulators and other stakeholders very busy in the coming years.

05



### Convergence and automation of monitoring capabilities

Another trend we have identified is that the financial industry will shift towards integrated customer-monitoring capabilities, meaning that different data sources, including those related to the customer's transactions, as well as the customer's credit risk or ESG risk exposure, will be used to create one single customer view. Institutions are moving from static KYC reviews, driven by time or events, towards perpetual KYC (p-KYC). By employing near real-time data to evaluate risks and incorporating this data directly into the customer risk assessment, financial institutions can significantly improve their understanding of risk and respond to emerging threats and trends. Seemingly disparate risk indicators will be connected, resulting in enhanced detection capabilities and a deduplication of efforts.

The automation of case management activities, including data collection and structuring, will expand, and we expect AI to assist in writing case narratives (e.g., preliminary customer risk assessments). Complex cases will be handled by analysts with in-depth expertise and strong analytical skills. This requires teams of analysts with not just legal expertise – which has been predominant in the industry thus far – but also with data science, technical and behavioural expertise. With the use of technology and by taking a client-centric approach, the customer experience will improve, as questions posed to them will be more tailored and less intrusive.

06



### Increased information sharing and data privacy

Public-private and private-private partnerships will take an (even more) prominent role in the future of financial crime compliance. On the one hand, we expect that there will be increased information sharing supported by privacy-enhancing technologies, such as multi-party computation, and implementing robust privacy safeguards. At the same time, however, it is widely mentioned that laws and regulations cannot keep pace with the technological developments and form a significant barrier to information sharing.

In our view, central steering from the government – and even at EU level – is required to address legal barriers related to information sharing. Interviewees also expressed their belief that ways to share information will be found, despite the barriers; the drive to fight subversive crimes is bigger than the barriers. Following the example of other countries, industry leaders expressed their hope that Data Privacy Authorities will also (more) actively support partnerships in maintaining effective information-sharing arrangements whilst respecting fundamental rights at the same time. Despite challenges, it is widely recognized that joining forces is required to fight crime and protect the integrity of our financial system.

## Call to action

While most trends are part of an evolving process, we believe financial institutions should take action now to remain or become a sustainable financial crime compliance organisation. We have highlighted six calls to action for financial institutions to consider:

### 01 Define your financial crime compliance strategy

Financial institutions should define their financial crime compliance strategy with solid fundamentals such as a strong compliance culture, clear governance frameworks and a fit-for-purpose Target Operating Model (TOM).

### 02 Reconceptualize risk management processes

Financial institutions should reconceptualize their risk management processes to have an agile approach for unlikely risks that may arise suddenly and intensify other risks.

### 03 Understand your data and data limitations

Data and data limitations should be understood by obtaining insight into compliance data flows and confirm if the data actually flows through systems completely and accurately.

### 04 Assess your sanctions screening capabilities

Transaction screening methods require reassessment and refinement to adapt to further expansion of sanctions.

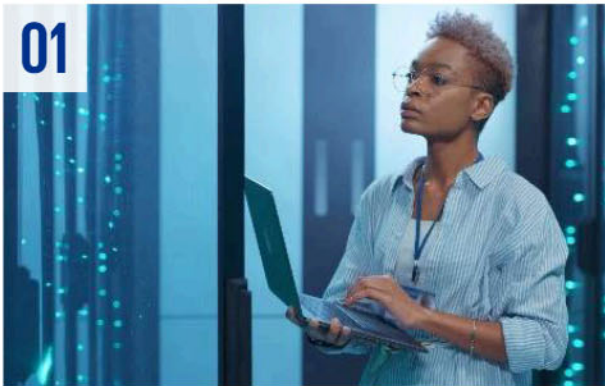
### 05 Converge automation and monitoring capabilities

A P-KYC approach should be embraced to obtain up-to-date and accurate insights of customer's behaviour. Transaction monitoring systems should be empowered by AI and ML.

### 06 Continue to join forces

Financial economic crime can be fought more effectively by joining forces cross border and beyond the banking sector. Smart technologies should be used to securely share data.

# KPMG Call to action



While taking a forward-looking approach is important, institutions should not lose sight of the past and present. Current efforts to remediate (self-)identified issues and lay a solid foundation remain important.

## Define your financial crime compliance strategy and TOM

Financial institutions should define their financial crime compliance strategy in light of their overall strategy, vision and mission, while considering (emerging) risks and threats accompanying the use of new technology. The strategy should be 'the glue' bringing and keeping together all the organisation's financial crime compliance processes, procedures and people. As part of their strategy, institutions could consider which processes they will execute themselves – taking a long-term horizon – and which processes are better off being outsourced or centralized. Outsourcing can be a viable option if the institution cannot build and maintain the required technological and human capital, skills and expertise. A financial crime compliance strategy requires solid fundamentals, such as a strong compliance culture, clear governance frameworks and a fit-for-purpose Target Operating Model (TOM). The TOM is designed to support the effective and efficient execution of the institution's strategy and contributes to building trust in the institution's own risk management framework. The Executive Board is in a position to effectively communicate the institution's financial crime compliance strategy and how it fits within the organisation-wide strategy, and allocate adequate resources.

02



### **Reconceptualize your risk management processes and risk culture**

The evolving geopolitical threat and regulatory landscape have introduced new and continuously expanding risks to financial institutions. With a heightened emphasis on personal liability for board members, financial institutions may lean towards risk avoidance and, as a result, take a tick-the-box approach to compliance.

Institutions should acknowledge that they cannot anticipate and prepare for every risk that they may encounter. Traditional risk assessments, which evaluate specific risks based on their likelihood and impact, do not account for the possibility of unforeseeable and unlikely risks that may arise suddenly and intensify other risks. Institutions should adopt an agile approach that allows them to respond rapidly as situations unfold. This approach includes using real-time or near-time data to identify emerging risks and trends among customers and transactions. Additionally, institutions should collaborate with relevant stakeholders both within and outside the institution to strengthen their risk management capabilities.

In order to promote sound and informed decision-making, the risk culture of an institution should be based on a full understanding and holistic view of risks and should align with the institution's risk appetite. Investigating the root causes of incidents – if they occur – and taking appropriate action can help to prevent future incidents. Board members should consider the extent to which dilemmas are discussed and mistakes are accepted to facilitate a culture where mistakes are openly acknowledged and addressed.





### Understand your data and data limitations

Data insights can be used to promptly respond to emerging risks and to enhance effectiveness and efficiency of financial crime compliance. To utilise the available data appropriately, institutions should first obtain insight into their end-to-end compliance data flows. Secondly, institutions should confirm whether the data actually flows through these systems completely and accurately to be able to detect and assess any data quality issues. This also implies that systems need to function, even if there are data quality issues; a good design is able to gracefully handle such issues. Thirdly, institutions should analyse their 'data drift', which entails changes over time to the data received for monitoring purposes.

Data changes can stem from an issue with data interfaces and can also indicate changes in client or business behaviour. For example, Covid had a material effect on the usage of cash or the moment of payments due to lockdowns. It is important to evaluate such changes, in relation to your monitoring, as they can point to changing or emerging risks. As a final step, the real-time data changes must be linked to the institution's risk and control framework. For example, the institution may need to adjust transaction monitoring thresholds based on renewed risk insights that follow from the data. An understanding of data limitations and opportunities is essential, as it will enable the institution to better evaluate data outcomes.

# 04



The downside to a more refined system is that it can be more susceptible to errors. As a result, institutions must design appropriate governance for their sanctions screening systems, which will ultimately enhance efficiency and effectiveness.

### Assess your sanctions screening capabilities

Geopolitical developments have increased financial institutions' sanctions exposure. Rapidly changing sanction measures, as well as the rise of instant payments, require flexible and real-time sanctions screening systems allowing for timely updates. In addition to having the appropriate technical screening capabilities, institutions increasingly need to deploy analysts with in-depth sanctions expertise to evaluate potential sanctions violations. Complexities arise, particularly with trade embargoes, dual-use goods and constructions that facilitate the circumvention of sanctions.

As sanctions expand, institutions must reassess – and potentially refine – their transaction screening methods. Whereas it used to be commonplace to screen all transactions across all locations against the same sanctions lists using the same logic, institutions should now consider if that is still appropriate. For example, screening transactions between the Netherlands and Belgium against the Canadian sanctions list may generate numerous alerts with limited added value. A more nuanced approach towards sanctions screening, which considers transaction types, countries, sanctions lists and thresholds, should reduce the number of irrelevant alerts. By refining their sanctions screening techniques, institutions can generate higher-quality alerts and have more time to respond to such alerts.



### 05 **Converge automation and monitoring capabilities to enhance AML processes**

Institutions should increasingly integrate different data sources to obtain a more complete, up-to-date and accurate picture of the customer's behaviour. In a perpetual KYC (p-KYC) approach, institutions move away from static periodic or event-driven review models to real-time monitoring using different data sources. Additionally, post-transaction monitoring alerts are integrated into the KYC process as an event trigger rather than the two being separate – partially overlapping – processes.

Although the EU Anti-Money Laundering Regulation will still require customer information to be updated at least every five years, we believe that the frequency and scope of reviews for especially the high- and medium-risk customers can be reduced by adopting a p-KYC approach. As part of this approach, institutions are forced to act upon changes as soon as they occur, limiting the need for static reviews. Adopting such an elevated approach towards KYC starts with a current state assessment. Opportunities to integrate processes, minimise inefficiencies, improve workloads, engage the customer and enhance customer experience are identified, as well as opportunities for outsourcing parts of the process to group centres of excellence or third parties.

The implementation of software to automate processes can be considered as an additional step towards an elevated KYC approach.

Additionally, financial institutions should move from rule-based transaction monitoring towards a combination of both rule-based and AI/ML-based systems to enhance transaction monitoring capabilities. The static rules remain important since they are based on AML typologies and red flags, and AI/ML can further empower the capabilities of these rules. Financial institutions may start with using AI for prioritising or auto closing certain alerts and gradually shift towards machine learning-based models for alert generation. Alerts that are currently being closed by employees will increasingly be closed with the use of AI. Financial institutions will need employees who understand these models, model limitations and potential biases.



### Continue to join forces

Organized crime is becoming increasingly diversified and does not stop at national borders, nor does the laundering of proceeds of such crimes. Therefore, parties should work together and share intelligence to rapidly respond to emerging crime trends. There are already several promising partnerships like Transaction Monitoring Netherlands (TMNL) and Fintell Alliance. We believe that only by joining forces – beyond the banking sector, but also cross-border – the fight against financial economic crime can be fought more effectively. Although there are legal barriers towards sharing data, sharing information about trends and typologies remains relevant. New technological developments combine privacy enhancing technologies with federated learning, for example, through the use of synthetic data or encrypted multi party computation. Proper application of these technologies in combination with automated compliance monitoring by independent third parties can largely eliminate privacy related risks whilst enhancing the detection power for fraud patterns within an ecosystem. Effective partnerships will benefit from central steering by the government, which should include setting priorities in the fight against financial economic crime.

Joint transaction monitoring through Transaction Monitoring Netherlands (TMNL) is considered a promising initiative by different thought leaders from both the public and private sector that we interviewed. In TMNL, five Dutch banks bring together their transaction data on corporate customers with the objective of identifying unusual patterns in payment transactions that are not exposed when the banks monitor transactions individually. TMNL limits itself to transactions involving (accounts held with) multiple banks and it focuses entirely on detecting unusual transaction patterns. Given its promise, the expansion of TMNL to other types of clients and transactions might result in even more meaningful outcomes. However, regulatory developments both at national and EU level on the permissibility and conditions under which initiatives like TMNL can be realised to their full potential should be closely monitored in the period to come.

A joint initiative that is worth investigating is whether and how the FIU can share (historic) data on suspicious transactions with financial institutions to train their AI/ML models with this data, while preserving privacy. In this way, models are trained with more data than only internally available data.

# KPMG Services

## How KPMG can help

KPMG leads the way in providing expertise and tools to help set you up for success:

- Support in establishing a policy house with interlinked procedures and underlying controls
- Monitor and assess the progress and quality of your remediation program
- Support with designing, executing or validating your Systematic Integrity Risk Analysis ('SIRA'), integrity risk appetite statement and key risk indicators
- Regulatory lineage to implement, monitor and demonstrate compliance with significant amounts of legislation
- Develop your FEC strategy and target operating model (TOM) to execute your strategy
- Develop and execute a technology strategy and operating model that supports the utilisation and development of existing and future data
- Aid in digitalisation of integrity risk management, AML and sanctions compliance programs such as the Sofy SIRA Manager and Sanctions Alert Classifier, which automate parts of your processes to enhance efficiency and effectiveness
- Implement our global KYC Managed Services solution to help you transition to enhanced KYC
- Conduct maturity assessments of your financial crime compliance processes and identify areas for enhancement
- Support with measuring and enhancing your organisation's risk culture
- Evaluate regulatory compliance and identify areas for enhancement through quality assurance or internal auditing procedures
- Validate your FEC models (e.g., KYC risk, transaction monitoring and sanctions screening models)
- Act as interim compliance officer
- Support with establishing regulatory-compliant data analysis ecosystems to enhance the detection power for fraud patterns

**03**

# **Interviews**

---



# Steffie Schwillens

Head of Financial Crime Supervision – DNB

**Steffie Schwillens is Head of Financial Crime Supervision at the Dutch Central Bank (DNB). Her primary focus is on banks, payment service providers and electronic money institutions. Prior to her role as financial economic crime supervisor, she was Head of the department Banking Supervision where she was responsible for the prudential supervision of less significant institutions, among which specialist and foreign banks and branches.**

## Personal motivation

DNB is a public party with a distinct societal character, which holds great importance for me given the substantial time I devote to my work. I take pride in working for an organisation that is firmly rooted in society. Our work is directly influenced by major events happening in the world around us, whether positive or negative. During my time at DNB, I experienced the aftermath and effects of the 2008 financial crisis, the Euro crisis, COVID-19, and the war in Ukraine. All these events directly impact central banks and us as supervisors.

Fighting financial economic crime matters considerably to society. It is important to recognize that financial economic crime is related to other crimes (including violent crimes), causing disruption and often having devastating consequences for society. It is this societal context that drives me. With financial economic crime supervision, it is my

purpose to work together with all public and private parties involved to contribute to the prevention of subversive crimes.

## Moving to a truly risk-based approach

I believe that we – as financial sector and as supervisor of the financial sector – can make a meaningful contribution to the fight against financial economic crime. With our recent focus underlining a risk-based approach, we can facilitate a transition to more effective compliance. We can achieve this by ensuring that all these smart, highly educated analysts that the banks and other financial institutions employ, direct their attention towards real risks. With the report ‘From Recovery to Balance’, DNB aims to contribute to that risk-based approach and maintain an ongoing dialogue with supervised institutions. Our goal is to understand the barriers that financial institutions encounter and to identify areas where they require additional guidance.

I want to emphasize that the law has always provided for a risk-based approach; however, the growing maturity in terms of AML/CFT risk management of an increasing number of financial institutions allows us to genuinely operate in a risk-based manner. In the past decade, there was a predominant focus on technical compliance and a perception that it was nearly impossible to meet the high standards of the supervisor, whilst the actual impact on crime prevention was perceived as limited.

This resulted in institutions being hampered in their decision-making to comply with the law. In this process, some of the side-effects of technical compliance, such as de-risking, discrimination, and elevated costs, have become apparent.

In our supervisory approach, we consistently evaluate the materiality of the issues that we encounter in our ongoing supervision. This also entails that we engage in open discussions with the sector. Sometimes we do encounter severe shortcomings that we need to act upon formally. However, institutions increasingly appear to be doing a pretty good job. In those cases, the few points for improvement we encounter, can be taken up by the institution in its learning loop in a 'business as usual' situation.

Historically, our approach to compliance has been relatively clear-cut, focusing on black-and-white decisions, e.g., either there is evidence of Ultimate Beneficial Owner (UBO) identification or there isn't. Nowadays, it is more often less evident whether an institution meets the bar and we increasingly find ourselves navigating in the grey zones. This adds complexity to our role as supervisors when making judgments. We are gradually shifting our focus towards assessments of the maturity of organisations:

How is the quality assurance process designed? Are the three lines of responsibility operating effectively? Are learning loops embedded in the process?

Lastly, I believe that most institutions should further develop themselves in their risk management efforts, particularly on the integrity risk side, which is less mature than, for example, credit risk management.

Unfortunately, the Systematic Integrity Risk Analysis (SIRA) is still rarely used as a steering document by the boards of financial institutions.

It tends to be treated as a highly theoretical exercise. Our guidance may have contributed to this in some respect. The SIRA should be more practical and where possible data driven to provide better insights and facilitate informed decision-making.

You cannot prevent that sometimes risks will materialize. For example, in your credit portfolio you will incur credit losses from time to time. Also regarding integrity risks it is impossible to fully abolish the risks in your portfolio and prevent them from ever materializing. What is important is that institutions perform thorough risk assessments, understand their portfolios, substantiate the choices made and mitigating measures taken and are able to explain this adequately to their supervisors.



**We need to step away from a culture driven by fear or an excessive focus on technical compliance, and move to a culture where we place trust in our own mature risk management frameworks.”**

### A paradigm shift

I believe that innovation and the use of new technologies, such as robotics, artificial intelligence (AI) and machine learning (ML) techniques, will change the way of working of financial institutions. Especially when coupled with more mature risk management processes. Humans will focus on more complex cases, while mundane tasks will be handled by machines. The effective use of data is extremely important for risk management.



With the rise of innovative technology, the appropriate use of models is also increasingly important. Institutions must create transparency on their model governance, testing environment, thresholds, back testing, etc. It is essential for institutions to evaluate whether the model outcomes are logical, especially in light of the results from the SIRA. Additionally, institutions should consider the risk of discriminatory outcomes and ensure privacy.

### **Supervisory change**

Currently, the results of the annual Integrity Risk Questionnaire, filled in by institutions themselves, form the basis for our risk-based supervisory approach. Certain responses carry greater weight than others, influencing the selection of institutions for further scrutiny. We are in the process of developing an additional model that incorporates data from multiple sources, such as the Anti-Money Laundering Centre (AMLC) and National Risk Assessment (NRA), which can be used for a top-down sector analysis. If we receive, for example, multiple signals from our public partners about real estate risks, we can give more weight to real estate exposure, resulting in certain institutions receiving a higher risk score.

In the past, our emphasis when doing investigations was on the outcome of the Customer Due Diligence (CDD) or transaction monitoring processes as we recognised that processes were not appropriately established. Hence we looked at the client file, or at the alert handling. Taking this approach made it easier to demonstrate the inadequacies in the processes that would inevitably lead to shortcomings in the end product, a client file or review.

In the near future, we will also employ different types of assessments, such as

assessments related to the learning capacity within organisations. We aim to understand how findings identified by an institution have been addressed: What actions were taken? What discussions took place? What formed the basis for the decisions that were made? It is imperative that the discussions, underlying analyses, and judgment calls are transparent and well-documented. We don't expect institutions to be perfect, as long as they act upon errors and learn from the experience. We will be placing increased emphasis on this aspect in our supervisory efforts.


### **Future-proof FEC organization**

We will be needing KYC analysts in the future. Humans need to interpret the results generated by models. The nature of the work will, however, become more intellectually challenging and interesting. Therefore, it is imperative for analysts to keep expanding their skillset and learn to understand and interpret model outcomes. I observe that banks already employ highly skilled analysts, and like any other professional, they should continue to develop their skills and knowledge.

I also think that institutions need to take a more holistic approach towards client management.

This shift means reducing segregation between the view on their client from a credit risk, customer due diligence (CDD) and environmental, social and governance (ESG) perspective. All these elements are important for knowing your customer. A more holistic approach is relevant not only from a compliance perspective, but also from a commercial perspective.

Appointing a Chief Financial Economic Crime Officer (CFECO) at board level may be a good way to safeguard knowledge and experience at the board level – or sometimes even a necessity to set an organisation in motion.



However, regardless the function title, it is imperative to have sufficient knowledge and appetite within the board to maintain an adequate compliance culture in the long term. Institutions need to realise that financial economic crime prevention is a permanent commitment; a cost-benefit approach cannot prevail once regulatory oversight is no longer imminent. Our supervision will not stop and will also not become more lenient; we will, however, focus on the highest risks. The sector has woken up and it is our responsibility to keep them awake. I hope that the perception of exorbitant compliance costs changes, not due to the costs themselves which may or may not decline eventually, but because the added value is recognised.

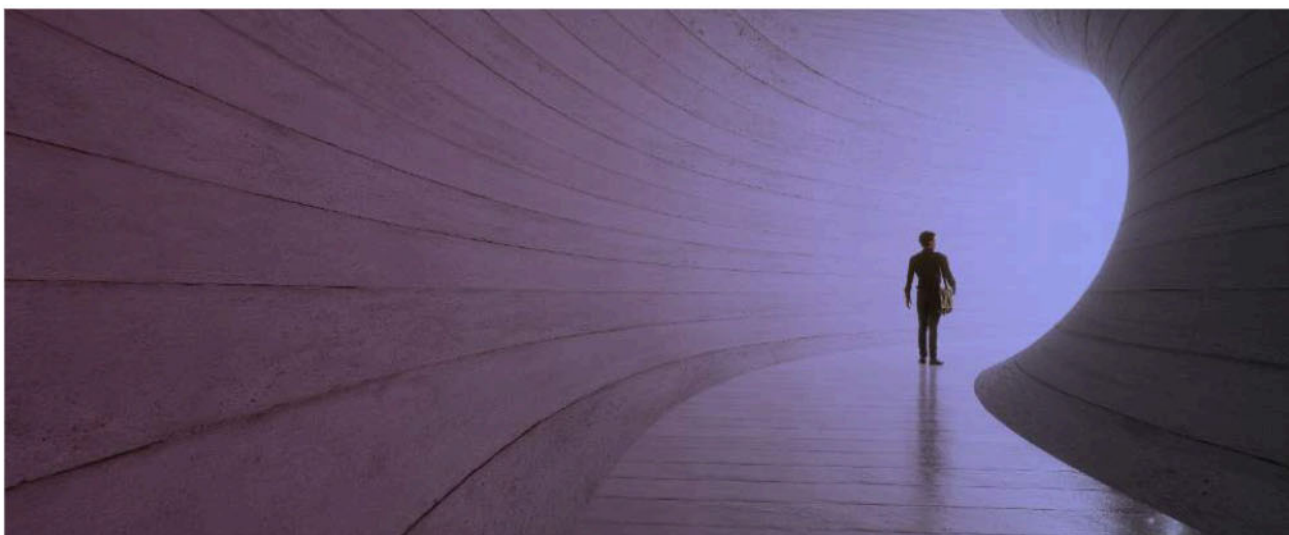
We need to step away from a culture driven by fear or an excessive focus on technical compliance, and move to a culture where we place trust in our own mature risk management frameworks. This requires a change in the system as a whole.

For institutions, this means improving risk analysis and testing using this as a basis for transaction monitoring and creating a feedback loop. Building trust through this process will enhance the overall approach.

Additionally, institutions need to have confidence that there is a knowledgeable supervisor who understands their processes and does not demand the impossible, while the institution itself is able to justify choices made in the process.

### **The case for change**

Enhancing collaboration and information sharing between public and private parties involved in financial economic crime is essential, and I am confident that we can achieve this in the near future while also upholding robust safeguards for data privacy. Access to more data enables us to distinguish between normal and abnormal patterns within a specific sector. It is important to note that improved data analysis results in higher-quality insights, ultimately leading to less intrusive client interactions. Increased international collaboration is important, given that criminal activities transcend national borders.



I am optimistic that within the supervisory realm, the Anti-Money Laundering Authority (AMLA) will function as a catalyst for positive change. Additionally, it will create more chances to exchange insights and knowledge gained.

The new EU anti-money laundering framework, with the AMLA, is intended to contribute to more harmonisation across the EU. This should reduce significant implementation differences, which is beneficial for institutions with cross-border operations, but also for tackling criminals operating beyond national borders. A risk, however, is that the European standardisation may enforce a more rule-based approach, while DNB is now transitioning towards a more risk-based approach. If we can demonstrate that our renewed focus is effective, we can promote it in Europe. We already see that some other European supervisors are taking a similar approach.

Institutions need to stay up to par with many new and changing regulations, which interact but do not seamlessly align. This requires a more holistic approach, moving away from silos and considering the interconnections of regulations. This principle applies not only to legislative and supervisory authorities but also to the institutions themselves.

### Threats and vulnerabilities

With opportunities come threats. Innovation is an opportunity for the financial sector, but also presents opportunities for criminals. In general, criminals are faster and better at optimising technological advancements. Anticipating new forms of criminal activity is challenging, particularly amidst remediation activities. Crime itself might not change significantly, criminals will always make money from drug trade and human trafficking. However, the dynamics of illegal money flows are evolving.



**Institutions need to take a more holistic approach towards client management. This shift means reducing segregation between the view on their client from a credit risk, customer due diligence (CDD) and environmental, social and governance (ESG) perspective.”**

Following the money has become increasingly complex due to the rapidly changing payment landscape, where a single payment passes through various entities, such as banks, payment institutions, electronic money institutions and crypto providers. The ability to trust other gatekeepers becomes more and more important, but is also dependent on political choices and striking the right balance between crime prevention and privacy.

### How to prepare

As a supervisor, I need to ascertain that institutions have a very clear understanding of the risks in their portfolio, as only this knowledge enables effective risk management. Institutions should possess in-depth insight into their portfolio and related risks, need to steer based on accurate information and be able to promptly respond to emerging risks.



# Tom van de Laar

**Head of Financial Crime Compliance – Rabobank**

Tom van de Laar joined Rabobank in 2017. He has fulfilled various roles in the field of AML. He is currently the Global Head of Financial Crime Compliance and Deputy Chief Compliance Officer (CCO) for Rabobank. Next to his role at Rabobank, Tom is a lecturer in Compliance and Integrity Management at the Vrije Universiteit Amsterdam (VU). Tom worked as attorney-at-law specialized in corporate criminal defence and compliance and as a consultant in governance, regulatory compliance and larger change and remediation efforts.



# Robin de Jongh

**Global Head of FEC CDD – Rabobank**

Robin de Jongh joined Rabobank in June 2023 as Global Head of Client Due Diligence. He is also a guest lecturer in Corporate Governance at the University of Amsterdam (UVA). Prior to his role at Rabobank, he worked at ABN AMRO for over 25 years, where his last role was Head of Detecting Financial Crime. He has been working in the field of AML since 2015.

### Personal motivation

**Robin:** The impact of many ugly things on the world, such as drugs, human trafficking, and terrorism, is enormous and fatal. People engage in these activities only to earn money. By working at a bank, I can make a significant contribution to eliminating these problems.

**Tom:** For me, it’s about doing the right thing. It’s in my nature to stand up for a certain view and advocate for it. I studied law and became a criminal defence attorney. As a lawyer, I was solving cases.

But in my current role, I can have a bigger impact with the team by contributing to solving the larger problems. What attracts me is finding solutions to systemic issues, looking at thinking errors and making things effective. What I like about combatting crime is that I can have a significant impact, as it deals with issues that are visible and tangible. I can contribute to solving bigger issues such as exploitation, drug trafficking, and oppression.

## Effective in preventing financial economic crime

**Robin:** I strongly believe that financial institutions should continue with their efforts to combat money laundering and other forms of financial economic crime. When looking back at the past years, much progress has already been made. I am aware of the prevailing criticism that the current system for combatting money laundering is costly yet largely ineffective, which was also the conclusion of an article published in *The Economist* in 2021\*. Furthermore, with information the police obtained through EncroChat (i.e. an encrypted messaging service used by criminals), the police has an abundance of data to analyse. Analysing this information is much more effective than analysing the numerous unusual transactions reported by the financial sector. That does not mean we should stop our efforts in the fight against financial economic crime.

Currently, we are looking at everything too broadly instead of focusing on what really matters. We should strive to maximise to a risk-based, effective and mature approach, leaving the period of enforcement actions behind. It is challenging to have a holistic and an in-depth view simultaneously. Additionally, I believe the authorities should adopt a pull approach, in which they request specific information from the financial sector, focusing on specific risks or cases.

**Tom:** The way we combat financial economic crime is an evolution rather than a revolution. While it is important to have the fundamentals in place ('basics in order'), we must also focus on advancing the maturity of our efforts to prevent financial crime. This next step requires courage. We must dare to choose where our focus lies so that we can determine where we can really make a difference.

We need to concentrate on the results, implying a focus on the effectiveness of our efforts in terms of preventing financial economic crime by good collaboration and the use of technology.



**We must dare to choose where our focus lies so that we can determine where we can really make a difference.”**

**Robin:** A few years ago, we were in a completely different phase. We were very much focused on rule-based compliance, despite the growing awareness that we were not really delivering a meaningful contribution to the prevention of money laundering. However, after we have the basics in order, we can become more mature.

Taking a step back and looking at the broader picture will enable us to evaluate how we can effectively contribute to the prevention of money laundering. Furthermore, there is also a shift taking place at the regulator: whereas in the past banks were strictly following DNB's approach on compliance with AML laws and regulations, DNB is now also closely following the approach taken by banks and the Dutch banking association (NVB).

**Tom:** The current danger is that we strive for perfection. But to take the next step, we also need to explore. As long as the exploration is done responsibly, with adequate safeguards and supported by reasoning, there should be space to do so.

\*'The war against money-laundering is being lost', 12 April 2021, *The Economist*.

## Courage and collaboration

**Tom:** I think that achieving a shift in our money laundering prevention efforts requires courage. For example, courage from the government to set priorities rather than focusing on many things at the same time with limited results. Priorities can be set through the NRAs for money laundering and terrorist financing, as well as through threat assessments performed by banks in collaboration with public parties and public-private partnerships such as Fintell Alliance. Priority setting by the US Financial Crimes Enforcement Network (FinCEN) can serve as an example. FinCEN defines its AML/CFT priorities at least once every four years pursuant to the US Anti-Money Laundering Act 2020.

**Robin:** It also requires courage from the supervisory and executive board members of banks to demonstrate patience and recognise that, despite pressure from various stakeholders such as regulators, clients, and the public, it takes time to establish the groundwork.

**Tom:** Specifically during times of polarization, it is crucial to maintain an ongoing dialogue between public and private parties, both at the national and EU levels. Rather than competing on the prevailing interest, privacy and money laundering prevention proponents should take a seat at the table together and integrate their frameworks. Sharing data in a responsible manner is essential in improving the effectiveness of our fight against financial economic crime. The Netherlands needs to advance further in this field. In comparison, the country is already more mature in the detection of fraud, by established fraud tracking registers (IVR/EVR).

**Robin:** I believe that there needs to be a dialogue to integrate privacy and anti-money laundering frameworks, instead of fighting each other on which interest takes precedence. While this may require significant effort, integration of these frameworks rather than taking a confrontational approach can result in a total solution. One practical example would be enabling the Dutch Data Protection Authority (DPA) to join the Board of the Financial Expertise Center (FEC).

Sustaining the dialogue between financial institutions and public institutions, including the FIU-NL, DNB, the Ministry of Justice and Security, and at the European level, is crucial. It is essential to keep the conversation going instead of adopting a confrontational attitude. I believe that collaboration, especially in terms of information flow, is extremely valuable. It is useful to share perspectives, and this could be proactively regulated between the public and private sectors. We can be formal and bureaucratic about it, but well-established cooperation will likely enhance the effectiveness of our financial crime prevention efforts.

## The future of the AML analyst

**Robin:** In the future, there will be fewer analysts with a higher level of expertise. They will be much more supported by technology. Information gathering will no longer be a part of their role, as information will be delivered to them in a structured way with preliminary analysis already completed. Automation, ML and AI will play a significant role in this transformation. I expect that the analysts of the future will need to have in-depth expertise and a critical mindset. Moreover, their expertise will expand to sanctions and transaction monitoring, as these domains will be increasingly integrated within the KYC/CDD process.

**Tom:** Analysts will continue to be a significant portion of the bank's workforce. There will not be an exclusive emphasis on financial economic crime, but the financial economic crime analyst's work will be integrated with, for example, ESG. The analyst will be supported by stronger technology to better process and interpret data that augments human decision-making. The work of the analyst will therefore become more rewarding, increasingly focusing on the most pertinent areas of financial crime risk.

### Preparing for the future

**Robin:** It is crucial to continue developing and improving the skills of those working in financial economic crime prevention, regardless of all the improvements that have already occurred in the past years.

**Tom:** We should continue with focusing on data quality, new technology and tooling, and our people. Hence, no new course is being set. At the same time, we should always be open to new risks and opportunities as they arise.

By combining these efforts and integrating solutions, we become more proactive and more effective.

**Robin:** Transaction monitoring will be more successful if it can be done across different banks, following the approach of Transaction Monitoring Netherlands (TMNL)\*\*. Technology, and specifically, privacy-enhancing techniques that are on the rise, will support the expansion of transaction monitoring. Furthermore, transaction monitoring is currently done retrospectively. However, I anticipate that for specific high-risk transactions, it will be conducted proactively in the future. Customers may be engaged in this process by banks requesting additional information or documentation from them before the transaction occurs. Prevention is always better than cure. Most importantly, if we want to prevent financial economic crime, we need to work together.

**Tom:** The system needs to change to enable more sharing between banks and public parties in a responsible manner. This could enrich data and provide better information. We need to shift our focus from predominantly legal compliance towards the overarching goal that we want to achieve (i.e. financial economic crime prevention). Making this shift requires collective courage.



\*\*TMNL (in Dutch: Transactie Monitoring Nederland) In TMNL, five Dutch banks bring together their transaction data on corporate customers with the objective of identifying unusual patterns in payment transactions that are not exposed when the banks monitor transactions individually. This approach enables money laundering networks and potential attempts in that regard to be identified and appropriate action to be taken.



# Hennie Verbeek-Kusters

Head of the Financial Intelligence Unit Netherlands

**Hennie Verbeek has served as head of the Financial Intelligence Unit the Netherlands ('FIU-NL') since 2008. Between 2017-2022, Hennie was Chair of the Egmont Group of FIUs, a global organisation that facilitates and prompts the exchange of information, knowledge, and cooperation amongst FIUs worldwide. Hennie also fulfilled several roles at the Dutch national police and the Dutch National Crime Squad.**

## Personal motivation

During my career at the Dutch police, I found that dismantling drug labs – or other illicit activities – was not that difficult, but I also experienced that it did not have the desired effect. Criminals would simply establish new labs in different locations. A far more effective, but also challenging, approach lies in the confiscation of illicit proceeds from these criminals. By disrupting their financial flows, we can more effectively combat organised crime. After all, these gains are often reinvested in the further professionalisation of criminal activities, which is prevented when their financial flows are disrupted.

Gaining insight into financial flows also offers valuable insight into the underlying offences. What personally motivates me the most is that, through my work, I contribute to crime prevention and – ultimately – a safer society.

## Enhancing the feedback loop

The main objective of the FIU-NL is to generate intelligence that is based on Unusual Transaction Reports received from gatekeepers. This intelligence is shared with security, intelligence and law enforcement agencies, such as the police, the Dutch Fiscal Information and Investigation Service (FIOD), the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). They are the parties that need to further investigate and gather evidence for use in courts. As FIU-NL, we may not always have insight into how our intelligence is used. This may be simply because there is no uninterrupted reporting line from gatekeeper to FIU-NL to law enforcement agencies, and therefore no subsequent return of information. Moreover, when the intelligence is used to build a criminal case, the Public Prosecution Service holds the authority to determine what information can be shared, when and with whom. Yet, we – police, FIOD, Public Prosecution Service and FIU-NL – are currently working together to improve the feedback loop.



We recognise that the obligations imposed on the private sector also require that we as public sector parties facilitate the private sector in enhancing their preventive frameworks. At the same time, law enforcement can focus on investigating the most serious crimes.

As FIU-NL, we were already committed to enhancing the feedback loop. The Financial Action Task Force (FATF) evaluation of the Netherlands, issued in 2022, has given further priority to this important topic.

### **The threat landscape**

I have noticed that different developments – or threats – are influencing the fight against financial economic crime. Firstly, there is increased polarisation on a global level and the involvement of state actors. For the FIU-NL specifically, this means that a big change in its landscape: whereas before FIU-NL could work together with virtually all FIUs around this world; in recent years this has become more difficult. For example, Russia's invasion of Ukraine resulted in the Russian FIU being suspended from the Egmont Group of FIUs. This means that Russia's large information position can no longer be leveraged by other FIUs. Conversely, other FIUs need to be mindful of 'hidden' Russian requests (i.e. Russians may seek information from FIUs that are not opposed to Russia, nor blacklisted, similar to the practice of sanctions evasion). Also, increased terrorist threat levels may change the flow of illicit funds. Secondly, organised crime is increasingly diversified. Criminal networks are no longer specialised in one type of crime; instead networks are connected through different types of crime. Drug crime, for example, can be connected with fraud, human trafficking, exploitation, and terrorist financing. As a consequence, law enforcement authorities can no longer specifically focus on one type of crime.

The third development concerns the pace of technological developments. New technologies enhance the ease and pace of financial transactions. The advance of AI benefits not only public and private authorities in their financial crime prevention efforts but is also (mis)used by criminals to commit their crimes.

### **Enhanced collaboration and information sharing in partnerships**

I believe that becoming more effective in the fight against financial economic crime and tackling the abovementioned threats requires increased public-private partnerships (PPPs) and private-private partnerships, as well as enhanced collaboration between different branches or departments within the same financial institution, and the use of smart technologies and IT solutions.

TMNL is a great example of a private-private partnership. Transaction data of corporate clients of different banks is shared in a safe, pseudonymised manner. This means that the transaction data is not retraceable to a specific entity. By combining data from different banks, TMNL is able to generate high-quality alerts. Conversely, when FIU-NL identifies a trend or phenomenon, TMNL can translate this into a specific search and provide us in return with additional insights. This generates higher-quality reports that the FIU-NL can analyse more effectively and, if needed, disseminate to law enforcement. To me, the Dutch Fintell Alliance\* is exemplary of a successful PPP.

\* Fintell Alliance is a PPP between FIU-NL and the four major banks: ABN AMRO, ING, Rabobank and Volksbank. Analysts and investigators from the respective organisations work at one location and share insights with each other. The partnership aims to achieve a more comprehensive view of criminal networks and their modus operandi.

In this alliance, participating banks report targeted Unusual Transaction Reports (based on a theme or specific topic) and the FIU-NL shares anonymised analyses with the participating banks, based on these and other reports.

This provides insight into certain phenomena, such as criminal ecosystems and the diversification of crimes within a criminal network, that would otherwise not be visible. Specific information stemming from the Serious Crime Task Force and the Terrorism Financing Task Force, is also fed into the Fintell Alliance. I hope that Fintell Alliance will expand to other sectors as well (e.g. accountancy, payment service providers), in addition to the banking industry.

The Dutch Fintell Alliance is seen as a front-runner for effective PPPs. Other nations look to it for inspiration to further professionalise their own partnerships. However, at the same time, the Dutch DPA is more restrictive on information sharing between public and private parties compared to other countries' DPAs. In other countries, DPAs actively participate in discussions to determine the conditions for data sharing, whereas to me it seems the Dutch DPA prefers to maintain a level of distance to avoid potential conflicts arising from its supervisory role.

### **Enhanced cooperation within financial institutions**

Besides the partnerships outlined above, an inward-looking approach towards enhanced cooperation can also strengthen financial institutions' financial economic crime prevention efforts. An example of enhanced cooperation within financial institutions can be found in the evolving role of compliance. Over the years, I have observed an increasing awareness of the importance of compliance, resulting in compliance being firmly embedded in the board room, as well as integrating compliance in the institution's vision and

strategy. With a clear vision and strategy on compliance, institutions are also increasingly able to step away from a 'tick-the-box' approach towards 'fit-for-purpose' compliance.



**We recognise that the obligations imposed on the private sector also require that we as public sector parties facilitate the private sector in enhancing their preventive frameworks.”**

### **The future of financial economic crime prevention**

I am positive about the developments in the financial economic crime domain in Europe. I believe that increased harmonisation, brought about by the EU AMLA and Regulation (AMLR), will also foster better cross-border collaboration. Currently, we are working on an upgrade of FIU.net. FIU.net is a platform used by FIUs from the EU Member States to standardise reporting formats and share intelligence, including pseudonymised matching of data from FIUs and, going forward, it should make joint analyses easier to organise.

I believe several initiatives will further evolve in the next decade and have an impact on the way we combat financial economic crime, such as the expansion of public-private and private-private partnerships (e.g. the expansion of the Dutch Fintell Alliance by including stakeholders from different sectors) and the exchange of employees between public and private parties (e.g. between FIU-NL and banks to improve the quality of reported alerts).



Additionally, I think there will be an increased focus on circumvention of sanctions in relation to illicit money flows as a result of increased polarisation. I also anticipate that there will be further integration of sustainability within the compliance and financial economic crime prevention domain. More risk-based, strategic discussions will take place on developments within certain companies (i.e. clients of the financial industry) and on financial integrity. The approach will be to look at the system as a whole, rather than just the transactions. Finally, technology will enhance the way in which the private and public sector can safely exchange information.



# Norbert Siegers

**Chief Executive Officer - TMNL**

**Norbert Siegers has served as the CEO at Transaction Monitoring Netherlands (TMNL) for the last four years. Before joining TMNL, Norbert was responsible for overseeing the development and innovation of digital channels at ABN AMRO. Norbert has a solid background in the intersection of technology, digital banking, data, payments, artificial intelligence, and the complex landscape of financial crime.**

### Personal motivation

My motivation for working in this field stems from my desire to solve complex problems with real impact. Four years ago, the field of financial crime compliance was relatively new to me. But the challenge of contributing to a topic that has such societal significance appeals to me; and TMNL is a great idea. Over time, as one delves deeper into this domain, it becomes apparent that the potential of making an impact in relation to financial crime is significant. Finding the right solution and supporters that can really change the system of tackling money laundering motivates me every day.



### A catalyst for change

At first sight, the fight against money laundering and terrorist financing is going well, if you look at the most recent assessment by the Financial Action Task Force (FATF), the global anti-money laundering organisation. Although there was still plenty of room for improvement, the Netherlands has made great progress. The FATF spoke of a robust system and praised the public/private partnership in which, according to the FATF, the Netherlands is leading. The Dutch Cabinet was very happy with that. So far so good.

But if you look at the results, for example, regarding taking money from criminals, they pale in comparison to the total amount of money that is laundered: around 300 million euros are taken from criminals annually compared to a total of tens of billions of euros in money laundering. To raise these millions, we are overhauling the entire system. Banks alone deploy 13,000 employees to prevent money laundering, which costs the banks 1.4 billion euros per year.

If you were to redesign the money laundering approach again from scratch today, you would not implement it as it is now. Coming up with an approach that is more effective than the current one is not that complicated, there are more than enough ideas. The trick is to say goodbye to the known and move towards something new, and that is the complicated part. Starting small and expanding is often the best route and can be a catalyst for far-reaching change.

## Perfect fit

Transaction Monitoring Netherlands fits perfectly into that approach. That is exactly how we started four years ago: a partnership of five banks to discover money laundering patterns of criminals who use multiple banks to launder money. Joint transaction monitoring makes the money laundering approach more effective, and we can look for significant money laundering practices in a more targeted manner. Because we see better what is wrong, we also see better what is right. Well-intentioned customers are therefore less inconvenienced by money laundering controls. We have successfully tested this on a small scale on the pseudonymised transactions of business customers.

For example, the money laundering scenarios that TMNL has tested in recent years have focused on human trafficking, VAT fraud and drugs, among other things. Our goal was to validate whether jointly monitoring transactions provides more meaningful signals than when a bank does this alone. The results have proven to be very valuable. This applies to both banks and investigative services. In three years, TMNL has returned more than 3,000 valuable signals to the banks, which allowed them to better investigate certain customers.

Banks were therefore able to submit better quality reports to the Financial Intelligence Unit (FIU). Banks are working increasingly intensively with the FIU, such as in the Fintel Alliance. Insights can be shared so that we can work together in a much more targeted manner.

TMNL has developed unique capabilities as a hub of the best FEC, Artificial Intelligence (AI), Data, and Technology knowledge in the financial industry. We have built trust through developing assured state-of-the-art technical

platforms and through strong controls on legal, security, and privacy risks, ensuring all we do is up to the highest standards and legal challenges. Thanks to the pseudonymisation of the transaction data, TMNL has no idea which customers are involved.

We understand that there is a delicate balance between privacy and anti-money laundering. That is not a mathematical formula; it is about proportionality. The new European legislation (AMLR) offers a solution to this and provides a clear framework for institutions to work together and tackle money laundering more effectively. We don't need to convince anyone that collaboration is key. You can never do it alone.

## Tipping point

The European Anti-Money Laundering Regulation (AMLR) represents a tipping point break in the trend. The central aim of the regulation is to better protect citizens and companies against financial crime that disrupts society. Therefore, the fight against money laundering and terrorist financing remains high on the political agenda. And it should be, if only you look at the devastating consequences of drug trafficking for Dutch society.

Although the new European money laundering regulation does not exactly fit what TMNL initially had in mind, it still offers good opportunities to have an impact. Let's look at what can be done in the future, considering the valuable results that TMNL has achieved so far.

Banks may continue to share data about customers who are at a higher risk of money laundering or customers about whom additional information needs to be collected to determine whether they pose a higher risk.

It is in line with the Dutch development in the coordination between banks and supervisors that we take a more risk-based approach to combatting money laundering and thus focus on the money laundering signals with the highest risk. At the same time, we must have the courage to no longer spend time on signals that do not undermine society. TMNL can make the money laundering approach easier for banks and customers. We can provide the tools that make it possible to tackle major criminals and spare small, bona fide customers.

### Harmonisation

The AMLR harmonises anti-money laundering legislation in the European Union. TMNL is pleased with the harmonisation of legislation because money laundering and terrorist financing are cross-border. The AMLR provides the necessary frameworks, and TMNL now knows broadly what it must comply with in 2027. With the AMLR, a balance has been found between the importance of privacy and the importance of tackling money laundering in the field of information sharing in partnerships – a major point of discussion in the Netherlands. That is an important gain.

The AMLR specifically leaves room for gatekeepers to collaborate with each other. This can be between banks but also together with notaries, for example. And that offers perspective for the future.

TMNL, its stakeholders and shareholders are currently carefully examining what the new European legislation means for TMNL's work and the possibilities that the new European anti-money laundering legislation will offer from July 2027. They will examine which of TMNL's services can contribute to a more effective joint approach to combatting money laundering and how the acquired knowledge,

experience and investments can be optimally used.

We have talked for a long time about an effective approach to money laundering; we just must do it now! We look forward to a future of working together in new, exciting ways and under a new legislative landscape.



**We must focus on money laundering signals with the highest risk ... and have the courage to no longer spend time on signals that do not undermine society."**



## Patrick Özer

**Partner Forensic Technology - KPMG**

**Patrick is a Partner at KPMG Netherlands and leads the Forensic Technology team. He is an experienced and data-driven forensic technology leader with more than 15 years of experience in preventing, detecting and responding to fraud, financial economic crime and other compliance incidents.**



## Jori van Schijndel

**Senior Manager Forensic Technology - KPMG**

**Jori is a Senior Manager at KPMG Netherlands and is part of the Forensic Technology team. He delivers data-driven and fact-based solutions around the core areas of financial economic crime technology, data analytics and e-discovery management to prevent, detect or respond to risks.**

### Personal motivation

**Patrick:** I grew up in a socio-economically challenged neighbourhood, where crime was highly visible. On various occasions, I have witnessed police raids uncovering criminal activities. In the neighbourhood, it was not uncommon that people would carry luxury goods and drive fancy cars, while they did not have a legitimate source of income. Driven by a feeling of injustice, I had always wanted to go into law enforcement, but eventually chose to study Artificial Intelligence (AI) because I was fascinated by what it can do.

Within KPMG, I now support organisations in their efforts to combat financial crime by applying my technical expertise within the compliance domain.

**Jori:** Already at a young age, I had a strong sense of justice. At school, I was always the one intervening in unfair situations or if someone was bullied, which occasionally got me into trouble. Initially, I wanted to study law, go into politics, and become a mayor so that I could help society. I chose IT, however, more specifically AI, because I found the legal and political reality too bounded and constrictive. To me, AI is unbounded in what it can do.

## The biggest contributor to a paradigm shift

**Patrick:** I see technology as the biggest contributor to a paradigm shift in financial crime compliance. By technology I mean the combination of the right tooling, new techniques, such as AI/ML, and the application of good quality data. Technology is able to detect risks and connect information far better than humans can. Still, its potential is sometimes held back by laws and regulations. Laws cannot keep pace with the developments in technology. Additionally, the process of implementing or amending laws and regulations can take years, leaving them already outmoded by technology upon their implementation.

**Jori:** Conversational AI and Generative AI, especially, will be at the centre of the paradigm shift towards more efficient and effective financial crime compliance. These technologies can more easily transform unstructured data into structured data, which will help automate the evaluation of unstructured data to assess if there is a risk. Using a chatbot-like interface, employees can evaluate risks based on information in the KYC file, instead of analysts having to manually search for the information.

## Ever-expanding role and responsibility of financial institutions (FIs)

**Jori:** Regulatory requirements and societal expectations on the role of in crime prevention are continuously expanding. At the same time, the mandate of financial institutions is becoming weaker due to legal limitations around, for example, data sharing, and oftentimes conflicting laws and regulations. The gap between expectations and mandate is too big for technology to close on its own. In my opinion, the central government should take more ownership in crime prevention and provide adequate means if they impose an

(originally) public task on private institutions.

The expectations financial institutions need to meet are almost unreasonable in light of the means they currently have at their disposal.

**Patrick:** Some of the governmental institutions have greater access to data and can better advise on how to tackle (organised) crime in the long term from a policy perspective. I think that they can more effectively use their authority to establish and execute a coordinated crime prevention strategy.



**Regulations are set up to protect a certain good, such as integrity of the financial system and data privacy, but in practice, they can also paralyse organisations and limit the benefits technology has to offer. ”**

## Threats to financial economic crime compliance

**Jori:** The (mis)use of Generative AI by criminals is certainly a big threat to financial crime compliance. Criminals do not have to abide by the same regulations as financial institutions. Through the use of new technology, it will become extremely easy to create fake documents. For example, false – but credible – identity documents can already be easily created via OnlyFake on the dark web. The current challenge with data quality might pale in comparison to the future predicament of distinguishing synthetic identities or fake personas from real ones.



**Patrick:** Regulations are set up to protect a certain good, such as integrity of the financial system and data privacy, but in practice, they can also paralyse organisations and limit the benefits technology has to offer.

**Jori:** Access to advanced IT systems and technology is also impacted by geopolitics. For example, US pressure has been reported to be the cause for ASML, a Dutch organisation, to halt its technology export to China. At the same time, Taiwanese multinational TSMC is responsible for producing 60% of the world's semiconductors and over 90% of the more advanced ones. Also, SoftBank recently issued a hundred billion dollar plan for an AI chip venture. Hence, countries and large conglomerates are trying to maintain, gain and direct control over (Gen)AI technology. Institutions should therefore evaluate potential geopolitical risks and take it into consideration when institutions outsource certain processes, particularly if these are outsourced cross-border.

**Patrick:** Catching criminals is always a cat-and-mouse game. It is extremely difficult for organisations to guard themselves against being (mis)used by criminals. A financial institution needs to think about all the forms in which criminals may abuse the system. This will cost a lot of (financial) resources, whereas a criminal only needs to find one.

### Privacy impact of AI models

**Jori:** My personal conviction is that privacy is impacted only if a human or conscious entity evaluates the information. (Non-conscious) AI models evaluating a large corpus of data and then providing humans only a very limited set of relevant data is, from my perspective, already privacy preserving.

Combining large-scale AI processing with an adequate framework to prevent or limit human access to data, could be a way forward to combining privacy with effective systems.


**Patrick:** I think we should try to differentiate between a system that contains personal data with restricted access enforced through technology, and one with unrestricted access granted to humans retrieving the same data. Of course, if data can be accessed with the help of technology, humans can potentially access it as well. In my opinion, we should explore data privacy enhancing technology to limit access to certain information, while benefiting in terms of crime prevention through data sharing initiatives (e.g. TMNL and KYC utilities). Ultimately, such initiatives have the potential to reduce the privacy impact for a larger group of people, as enhanced insights – obtained with the help of technology – will reduce the need for human intervention and customer outreach.



**(Non-conscious) AI models evaluating a large corpus of data and then providing humans only a very limited set of relevant data is, from my perspective, already privacy preserving.”**

### People and technology

**Patrick:** I think that the type of expertise needed to effectively combat financial crime will change in the next decade. For example, an AI model will be much better capable than humans of telling apart fake identity documents from real ones by evaluating specific data fields.



Financial institutions will need employees who have an understanding of the technology, as well as employees who are able to oversee more complex problems, and have the capability to consider new ways to identify and mitigate emerging risks.

**Jori:** I hope that there will be more collaboration between banks, and that banks will increasingly focus on their core competencies. This may result in more outsourcing arrangements, rather than banks building the technology in-house. Many banks are currently doing the same activities, such as building the same technology solutions, in isolation. Examples of effectively fighting crime occur when different police units or public authorities cooperate and connect the available information.

Criminals are becoming increasingly organised and diversified in their criminal activities (e.g. networks of criminals are involved in different types of crime, such as drug trade and human trafficking). This organisation and diversification makes it increasingly complex to effectively fight financial economic crime. Banks, together with public authorities, need to join forces rather than follow their own approach. On their own, banks will never have the best technology to safeguard the integrity of the financial system. Top-notch AI requires collaboration with companies such as Google and Amazon. By jointly developing technology and sharing it, individual institutions do not have to reinvent the wheel.

### **Public-private partnerships (PPPs)**

**Jori:** PPPs, especially within the context of thematic partnerships, can be very effective and efficient. Therefore, an increase in such partnerships might be worthwhile. In such partnerships, deep dives are performed on specific topics, such as agricultural risks, trade-based money laundering (TBML) and

second-hand car exports. At present, there are not a lot of partnerships dedicated to the sharing of technology, trained models, and data for the purpose of training models. Such partnerships are frequently hindered by, for example, legal limitations around data privacy.

Public parties, especially, possess a wealth of information that can be used for training models. The Financial Intelligence Unit (FIU), for example, has a database of transactions that are confirmed as (likely) suspicious transactions. While the FIU cannot disclose all these transactions to all banks, they might help banks with training AI models by running the following procedure. Banks develop models, the FIU trains the models using the data the FIU has, and the banks are only provided the trained model, and not the sensitive data.

**Patrick:** Explicit and specific information from public parties on money laundering methodologies can help to adopt a more targeted AML approach. I advocate for a hybrid approach which combines two complementary methodologies. Firstly, leveraging explicit examples sourced from verified intelligence provided by public parties enables financial institutions to enhance their investigation capabilities with precision. Secondly, the utilisation of theoretical assessments, such as identifying red flags or anomaly detection, facilitates the detection of emerging issues and trends. This dual strategy is poised to generate new Suspicious Activity Reports (SARs), thereby enriching the knowledge base of pertinent public parties. Consequently, this feedback loop allows for the extraction of practical, verified intelligence to further enhance investigative efforts.

## Next generation of KYC/CDD, transaction monitoring and sanctions screening

**Jori:** Different domains within financial institutions, such as KYC, TM and sanctions screening, but also credit and ESG risk, will become increasingly integrated from a data perspective. However, the follow-up of potential signals will be done in different teams, depending on the expertise required.

For sanctions screening, there are new regulations and developments (e.g. amendments to the Wire Transfer Regulation) that should facilitate increased transparency in payments by requiring additional information to be included in the payment message. The ISO 20022 standard will provide for richer data fields that can be used for screening. Banks should, however, have screening software in place that can also work with these additional data fields to reap the benefits of the additionally available information.

**Patrick:** KYC and TM processes are very siloed at the moment. Integration of these processes will offer a more holistic view. By adopting a perpetual KYC approach, institutions can conduct targeted reviews on the basis of trigger events. Additionally, technological advancements have made it possible that TM alert handling can be supported with instant background checks on the beneficiary of a flagged transaction, supporting the alert handler in their review process.

**Jori:** Data collection for KYC purposes can be made much easier with the help of technology. It is technically feasible to get a lot of information from the public web and open sources, but creating a database of information on the basis of public sources has been criticised by data privacy authorities.

Generative AI chatbots could be used for customer outreach, to collect information

during onboarding, but also when deviations occur outside expected patterns. This, however, requires societal acceptance that we will, with increasing frequency, interact with AIs instead of with humans. In a future scenario, an AI from a bank might directly interact with someone's personal AI assistant, reducing the burden on the human customer.



**Different domains within financial institutions, such as KYC, TM and sanctions screening, but also credit and ESG risk, will become increasingly integrated from a data perspective. ”**

**Patrick:** In the past, public registers were more widely available and contained more detailed information for the identification and verification of ownership. Access to public registers is increasingly being restricted by regulations. To create a more effective and efficient KYC process, I believe in a system in which clients upload their own information, which is then evaluated by one financial institution and, where possible, verified on the basis of access to public registers. Upon approval from the client, other organisations should then be able to access or use specific information for their KYC purposes as well, rather than redoing the entire KYC process. Such a system is already possible from a technology and process perspective, but the challenge lies in current legal limitations and societal acceptance of such a system. I see that there is also a lot of distrust towards public and private parties, which further limits the willingness of people to share information.

## Preparing for 2034

**Patrick:** The advancements in the financial crime compliance domain in the next decade will largely depend on what is feasible within the regulatory framework. Financial institutions should be agile enough to adequately implement changes in regulations across their institution and respond to the changing threat landscape, including new types of criminal behaviour. Technology implementations within financial institutions are complex and take a long time, while the speed of technological advancements is more rapid than ever before. Therefore, institutions should consider implementing modular systems, where one element can easily be replaced by another element, rather than ending up in a situation where the entire process needs to be redesigned.



**The advancements in the financial crime compliance domain in the next decade will largely depend on what is feasible within the regulatory framework. ”**



**Jori:** FIs should create a flexible IT architecture to keep pace with the speed of technological advancements. Most FIs have legacy systems and different systems that are used for the same or overlapping purposes, for example, as a result of past mergers and acquisitions, whereby old systems are maintained rather than integrated. FIs should invest in (human) expertise and technology, keeping in mind quality over quantity. I would rather have a limited number of highly skilled experts than a larger group of people with mediocre proficiency. Banks could consider attracting IT architects and IT developers from different sectors and disciplines, as they might be able to bring fresh perspectives.



# Tom Loonen

**Professor Financial Law and Integrity – VU Amsterdam**

**Tom Loonen has served as a professor of financial law & integrity at the VU for the past 10 years. He is one of the esteemed founders of the Certified KYC Expert Executive Education program at the VU. In addition to his academic role, he holds a position as an expert judge in the Enterprise Chamber of the High Court of Amsterdam and serves as special counsel at the international law firm Pinsent Masons Netherlands LLP.**

## **Personal motivation**

I began my career in the banking sector, where I gradually became involved in combatting financial economic crime. Later on, through my discussions with the National Police's Serious Crime Team, I learned about the impact money laundering has on our society and the undermining effect emanating from it. Organised crime is happening right in front of us. Think about tourist shops, such as 'rubber duck shops', occupying prime locations in Amsterdam with surely little ability to generate sufficient revenue to afford such a location. Our society, including our politicians, seems to more or less accept this situation under the belief that a free market economy should not be restricted. The prevailing attitude seems to be that society perceives no wrongdoing as long as there is no direct threat. It is disheartening to witness how we, as a society, turn a blind eye to organised crime. In this context, gatekeepers, public parties, and politicians play a crucial role that should not be underestimated.

## **Criticism of the current system**

In my opinion, every individual and organisation, both private and public, has a role to play in combatting financial economic crime. There has been increasing criticism against the government for not allocating sufficient resources to combatting money laundering. Both financial resources and human capital are lagging behind in the public sector, especially when compared to the private sector. This is a political choice. The central government should pick up its role in fighting financial economic crime. I believe that enhanced public-private and private-private partnerships, such as TMNL, are needed to improve the effectiveness of combatting financial economic crime. To this end, adequate public resources should be made available.

## **The future of the KYC analyst**

I anticipate a decline in the number of FTEs in the KYC domain, which I believe to be a positive trend. Costs have become too high. Banks are already taking steps to increase their efficiency and effectiveness, through the use of technology, rather than increasing manpower. Although the number of KYC analysts can likely be reduced, the quality of the analysts should be increased substantially. The KYC analyst of the future will be able to understand broader geopolitical developments and to approach KYC-related investigations strategically and holistically. Furthermore, with this enhanced understanding, they can better advise higher and middle management.

## From remediation to process improvement

It is important that banks transition from quick and reactive solutions towards more sustainable ones where compliance is more imbedded in the business processes. I have noticed that there is some resistance to implementing laws and regulations within banks, which is understandable given the ever-expanding scope, increased complexity and sometimes conflicting laws and regulations. Enforcement action is still one of the main drivers for regulatory change.

In recent years, there has been a heavy emphasis on remediation rather than improving entire processes. The latter also typically requires changes to IT systems and the organisational culture, as well as increased financial economic crime awareness and knowledge across all employees. Such knowledge should be extended to bankers rather than just KYC or Compliance personnel.

Improving entire processes requires a long-term vision and strategy for financial crime compliance and, in that vein, the role the institution wants to take in society. I believe financial institutions should transition from capitalistic thinking towards thinking about how they can add value to society.

They can make a difference, but it requires a conscious choice about their role in society and setting a strategy to live up to that role.

## Driving strategic change

Executive Board members should be able to exert an appropriate level of challenge, on their teams as well as on other Board members. Appointing a CFECO or CCO to the Board may demonstrate the importance of compliance, both internally and externally. However, the effectiveness of such appointments has not yet been proven. The officers should drive strategic change and take

a challenging role rather than operating in isolation and taking a 'tick-the-box' approach towards compliance.

## The role of clients

In my opinion, banking clients should be seen as essential stakeholders in the fight against financial economic crime. There is a large focus on the role of gatekeepers and the internal changes that they must make, while the role of clients in the fight against financial economic crime tends to be overlooked. To gain the trust and cooperation of clients, it is necessary to involve them in the understanding of why particular information is being gathered. Additionally, clients could be rewarded for providing information. Firstly, by making the process easier and more fun by – for example – incorporating elements of gamification. Secondly, by offering a small gift or discount in exchange for sharing information.

## The contribution of scientific research

With scientific research, extensive knowledge can be generated on effective strategies to combat financial crime. At the same time, it can provide constructive feedback and insights to improve the functioning of the financial crime prevention chain and introduce innovative and creative ideas for involving clients and client retention, for example, through gamification. I believe that AML processes can be enhanced by leveraging insights from different disciplines, such as legal, psychology and economy, but also marketing to enhance customer experience.



## Jaap van der Molen

Head of Detecting Financial Crime – ABN AMRO Bank

Jaap is ABN AMRO’s Group Head of Detecting Financial Crime. He previously worked as Global Head AML and Sanctions for ABN AMRO Bank and held high-level positions in the field of financial crime risk management at Standard Chartered Bank in both London and Singapore and ING Bank. In his work, Jaap is focused on delivering results as well as improving internal processes.



## Hanna Deleanu

AML Expert and Policy Developer – ABN AMRO Bank

Hanna is a subject matter expert on financial and economic crime, with a track record in designing and executing risk management strategies, policies and processes. Before joining ABN AMRO Bank, Hanna earned a PhD from Utrecht University for her research on the effectiveness of anti-money laundering policies in the EU.

### Personal motivation

**Hanna:** Combatting money laundering, terrorist financing and other forms of financial economic crime is important to me because I was born in a country that suffers from endemic corruption. Through my research, and as young citizen, I witnessed the toll corruption takes on individual citizens, society at large, the public good and, ultimately,

democracy. Corrupt funds are laundered through the financial sector. Thus, the more effective we become at identifying and isolating them, the more we ensure that crime does not pay and the more we support a fair democracy.

**Jaap:** Hanna's observation about financial crime and its impacts on society is true. As banks, we are creating barriers to criminal activity. My background as a macroeconomist drew me to international matters. After all, money laundering, sanctions evasion and their predicate crimes often transcend national borders. However, despite the inherently international nature of these crimes, efforts to combat them remain predominantly driven by national approaches and are often bound by borders. It is the dynamic interplay between these international crimes and national disparities that drives me in my work.

### The next big thing

**Jaap:** In the next 10 years, we will see a significant increase in public-private and private-private collaboration to enhance the fight against financial economic crime. For that to happen, we need the right framework for data sharing, and this is a big hurdle at the moment.

**Hanna:** sharing data in partnerships will play a huge role, and the success will exponentially increase by the use of AI.

**Jaap:** The success of AI is dependent on data. So I would start with data.

**Hanna:** Indeed. Hopefully, we will be able to benchmark better and distil and share good data sharing practices. We will be able to signal discrepancies way faster and will be more agile in taking action. The Public Prosecution Service should not need to fully replicate the banks' work to secure a conviction or a confiscation but should be able to directly use the suspicious activity reports (SARs) provided by the banks. If SARs will deliver more actionable intelligence and tell a strong risk story, they become more powerful inputs on which the other chain partners can build.

### Future workforce

**Jaap:** There will be a mix between systems and analysts. We will have analysts in 10 years, but they will be experts working on complex cases. They hardly occupy themselves with false positives anymore. They will be completing fewer but more complex cases due to elaborate and rich data and being connected to the data from the other banks. I imagine the scenario where it is allowed for one pool of analysts to be shared by all banks, not only to perform the risk detection but also the analysis of the risk.




**Analysts in 10 years will be completing fewer but more complex cases due to elaborate and rich data and being connected to the data from the other banks."**

**Hanna:** Indeed, in a future-proof financial economic crime organisation, expertise is going to be the basis – and will require the ability to make sense of the data, to use AI, and to really understand risk. This, together with high-quality data, will enable us to tell a compelling story about risk, its presence and its manifestation.

**Jaap:** AI can teach itself how things work and document it, based on data and information that is used to train and support these systems. Conclusions drawn by AI may be complex, and we should avoid a situation where we cannot reproduce the outcomes. At the same time, AI is not creative. Even Generative AI reuses the information we already know.





Therefore, the detection of new AML typologies and methods and responses thereto will remain complex and require an expert. For instance, AI may do some automatic outreach to the client, but eventually the institution having a relationship with the client would want to take some ownership there. I don't know if we even want third parties contacting clients from a commercial perspective.

**Hanna:** Analysts can be facilitated by AI to avoid doing menial tasks. And, as Jaap correctly points out, it would be great to achieve a scenario where analysts can collaborate across banks and public parties to holistically assess risk and generate actionable intelligence that is readily usable by the next person in the chain. Currently, there are too many silos and too many handovers, which results in a loss of speed and information.

### Emerging threats

**Jaap:** Over time, generations will become more digitally savvy. Older generations are now very vulnerable; but actually everyone can be fooled by AI, even younger people. AI makes it easy to pollute the truth. It is very simple nowadays to erase bad media coverage but also to pollute existing information with opposite information. Speaking of AI, our computers may also be 'learning' from this polluted information. If we start promoting conspiracies, then at some point a computer will think these are truths. With such use of (mis)information, generations can even forget events as large as 9/11. That worries me as an existential threat, so the question becomes: how do we protect the truth?

### Enhanced cooperation

**Hanna:** I hope that we will move to what DNB originally did well, and that is responsive regulation. Regulation that is not top-down but looks at participants in the industry and tries to co-create. We should understand that with

innovation, mistakes are inevitably made, and that making these mistakes transparent benefits us all if we learn from them as an industry. Having an open discussion, sharing best practices, collectively building and implementing guidelines will bring us towards a better and more standardised practice at a national and European level.

**Jaap:** We don't need more regulation, we need more cooperation. We need a much more thorough understanding of the things that are unusual, of typologies, and of when detection is effective in the eyes of the regulator and of the FIU, the police, the Public Prosecution Service, et cetera. Creating new regulation is not helpful, as the two-year drafting timelines often result in outdated rules. Criminals exploit this delay, rendering the regulation ineffective within six months. For enhanced cooperation between public and private parties, we need clear priority setting, feedback loops from the public sector to gatekeepers in the private sector and meaningful data sharing. A strengthened risk assessment that is tailored to the circumstances of respective gatekeepers will improve priority setting and steer us in the right direction for the next months and years.



**For enhanced cooperation between public and private parties, we need clear priority setting, feedback loops from the public sector to gatekeepers in the private sector and meaningful data sharing.”**

### Expansion of responsibility

**Jaap:** Banks with their central role in the economy continue to receive focus on what they do to support upholding of laws and regulations that apply to others. By virtue of processing payments and other transactions of their clients – who may be in breach of certain laws or regulations, which then may in turn constitute an economic crime – banks are considered to have a responsibility in this area.

For example, export controls but also the significant new sustainability regulations that apply to all companies. It is important to consider where banks can actually fulfil that supporting role credibly, based on information available to the bank, and where this becomes overly burdensome also to customers, e.g. due to additional KYC requirements, or duplicate with the role that other – public – institutions already have. For example, recruitment agencies are required by law to have a certificate which is aimed to prevent labour abuse. As banks, we check whether the recruitment agencies possess the right certificates. I am not disagreeing with the need for such regulation, but it is one other thing that is added to our internal checklist as part of the KYC process. We do this because we take our role in preventing such heinous crimes very seriously. But the field is quite

broad, and the impact of, for example, new ESG regulation such as Corporate Sustainability Reporting Directive is potentially that these checklists become longer, our KYC processes more complex, and the cost of doing business will increase as a result. At the same time, the drug-related organised crime situation in the Netherlands, criminal infiltration of the real economy, and underground banking are serious problems that require joint efforts and real focus. The real challenge remains to set priorities with the public sector (including the supervisor) and realise we cannot do everything.

### Increased effectiveness

In the next 10 years, we will be more effective and efficient in detecting and reporting financial economic crime by continued investment in systems and tooling. This will also allow us to keep costs in check, which is important for customers and shareholders. We will spend less time on tasks that do not add value, such as file administration, processing false positives and possibly certain true positives, and reporting will not require the involvement of an analyst.

Customer monitoring will include more than just monitoring transactions. We will be able to zoom into specific risk types, such as bribery, tax evasion, VAT fraud. Our output will have more actionable intelligence (e.g. 'I observe reuse of the same invoice number' rather than 'I have seen a cash transaction above EUR 10K').

## Enhanced customer experience

**Jaap:** Simplifying the KYC process will elevate the customer experience and make it more secure. This can be done by allowing banks access to relevant information from central repositories. To make this possible, the government should enable banks to utilise the Basisregistratie Personen (BRP ) and designate the Chamber of Commerce as the custodian of verified ownership data for companies.

## Purpose-driven change

**Jaap:** Five years ago, banks were thinking about how to deal with the Public Prosecution Service. They were under review by the regulator, and their purpose as gatekeepers was not fully crystallised. Fast-forward to the present, and there is an actual dialogue on the effectiveness with the different parties. We still have work to do to improve our AML frameworks and move to a situation of normalised supervision. But we are also having a more meaningful conversation with the public sector about priority setting, about

effectiveness, and about how to create an effective feedback loop. It would be great if we can continue this trend and add to this better technology, trust in the system and trust in each other.



**When everything is a priority, nothing is a priority. We cannot do everything and neither can the public authorities. So we need to make choices and set priorities together."**

To prepare for the future, banks and regulators should have open conversations on priorities. When everything is a priority, nothing is a priority. We cannot do everything and neither can the public authorities. So we need to make choices and set priorities together.





# Mark Lamers

Chief Executive Officer – Vartion

**Mark Lamers is the CEO of Vartion, a data analytics company that uses Artificial Intelligence (AI) and Machine Learning (ML) to develop its solutions for life sciences and finance (KYC/AML). Mark is well versed in both the technical and the managerial aspects of the finance industry. He has spent his entire career bridging the gap between business and technology, delivering solutions that meet the needs of both sides.**

## Personal motivation

What motivates me is finding solutions to very complex problems. The main goal in my work is to transform data into intelligence and optimise the process of doing so. This involves developing and applying advanced techniques for data analysis and decision support. Our company Vartion aims to find a balance between human and artificial intelligence in solving problems that matter to society. Vartion first developed Harvey, an AI-based solution that supports biomedical research. The founders were then approached by financial services company United, who believed Vartion's AI-driven search engine could also support them in regulatory compliance and the fight against financial and economic crime (FEC). The social relevance is obvious: I believe FEC should matter to everyone who values a fair, transparent, and secure world. So, with United as our launching customer, we created an AI-based compliance decision platform called Pascal. As developers

in the AI space, we also seek to understand the ethical, social, and legal implications of using AI for FEC prevention purposes.

## The paradigm shift

At present, financial institutions rely mainly on human labour to ensure regulatory compliance. With technology, however, they can reduce costs, speed up processes and minimise the risk of errors. Given the large volumes of data that require nuanced interpretation, adopting a nearly deterministic model could streamline the process. Using artificial intelligence, however, allows for even greater speed and precision, further lowering compliance-related expenses.

Meanwhile, more technologies are evolving that can transform the FEC effort. An example that lies at the heart of our solution Pascal is Entity Intelligence (EI). EI, a specialised area of AI, concentrates on gathering, analysing, and connecting data about entities from various sources. These entities can range from individuals and locations to organisations and transactions. EI aims to offer detailed and precise profiles of entities and map their interconnections. Information that other applications can use for various objectives, like transaction monitoring.

## Emerging threats and effective use of data

AI is making FEC more sophisticated, with criminals using artificial intelligence to automate their ransomware, phishing and identity theft schemes. No wonder, then, that financial institutions are turning to AI as well. They are using advanced analytics for early detection of unusual financial patterns. Big data supports them with extensive customer profiling and suspicious activity detection, while predictive modelling helps them to identify risk factors and anticipate threats. Besides protecting them against cyber threats, these technologies also help them to comply with anti-money laundering (AML) and know-your-customer (KYC) regulations. And they are key in monitoring transactions for suspicious activities, as required by regulators.

## AI Revolution

In the complex landscape of financial and economic crime prevention, AI is not just revolutionising the way institutions safeguard assets, it is also redefining the boundaries of what is possible in detecting and preventing financial crime. AI can analyse and interpret vast datasets with unprecedented speed and accuracy. Unlike traditional systems that rely on static rules or patterns, AI-driven tools adapt to and learn from new data, enabling them to identify sophisticated schemes and anomalies that would otherwise go unnoticed. Speaking from my own experience working on Pascal, we have developed AI models that can detect adverse media related to a person or organisation from over 700 million global media websites within seconds. We can instantly identify the network that this person or organisation is linked to. This dynamic approach makes it far easier for financial institutions to head off risks before they escalate into significant threats.

Meanwhile, AI is also entering the regulatory technology (RegTech) space. With Pascal, we have built advanced software to efficiently ensure compliance with regulations, reducing the risk of human error and the potential for oversight. This is particularly crucial in an era where regulatory demands are constantly evolving, requiring agility and precision in compliance processes.

## Preparing for 2034

Preparing for FEC prevention in 2034 requires a forward-looking and proactive approach along four lines: technological innovation, collaboration, compliance, and adaptability. Other necessary components of future financial crime prevention efforts are of course data privacy and sustainability. Given my own background, I am especially passionate about the need for technological innovation. And proud to be contributing to the FEC effort.



**Financial crime prevention efforts can benefit immensely from innovative AI-based technology, which can also help financial institutions stay compliant with regulatory requirements. Embracing AI, within ethical boundaries, is key for a resilient future.”**



# Laura van Geest

**Chair of the Executive Board – AFM**

**Laura joined the Dutch Authority for the Financial Markets (AFM) in February 2020 as Chair of the Executive Board. Her term was recently prolonged until February 2028. Since November 2020, she chairs the Dutch Financial Expertise Centre (FEC). The FEC is a Dutch collaborative effort between authorities with supervisory, monitoring, prosecution or investigative tasks aimed at strengthening the integrity in the financial sector. Prior to her role at the AFM, Laura held various management positions at the Ministry of Finance from 1990 to 2013. In 2013 she became the first female director of the Central Planning Bureau.**

### Personal motivation

The main theme throughout my career has been my passion for contributing to the public good. I have an intrinsic drive to address significant challenges, where solutions are not always present nor evident, and where diverse perspectives play a crucial role.

As Chair of the AFM, I have the privilege of playing an active role in the financial system. Through my role, I have the possibility to contribute to a sustainable financial system and the stability of the financial markets.

Being the grandchild of a policeman, I have had an affinity with investigating and detecting crimes from an early age. The FEC places an emphasis on countering financial and

subversive crimes, both of which present substantial threats to the economy and broader society. Another goal is the prevention and criminal prosecution of terrorist financing.

The FEC is a collaborative effort between multiple public partners with a common goal of effectively combating criminal activity\*. Each organisation approaches cases brought to the FEC from their own, unique perspective in light of their respective mandates. Together, the partners each add their piece to the overall puzzle. As criminals are not bound to mandates and borders, these puzzles can be very difficult to solve. When this does happen, the satisfaction lies in having pieced together the entire puzzle, having gained a clearer understanding of criminal methods, and having been able to act more effectively and efficiently in hampering criminal activities.

### The evolutionary journey of the FEC

Since its inception in 1999, the FEC has evolved from a partnership to exchange information into a forum to gain a broader perspective on various (criminal) phenomena, not only focusing on AML but also on CFT. A second important development during this period has been the broadening of the FEC cooperation through the establishment of partnerships with private sector entities, notably banks.

\*The FEC consist of seven partners: AFM, DNB, the Dutch Tax Administration, FIOD, FIU-NL, the Dutch Public Prosecution Service and the national police.

These PPPs have expanded the FEC's knowledge and expertise, leading to deeper insights and a wider network of collaborative partners. This has allowed the FEC to become more effective over time.

Within PPPs there has been a growing emphasis on thematic investigations to help the public and private sector to better identify risks. Successful collaboration resulted in tangible insights on, for example, trade-based money laundering (TBML). A FEC PPP thematic investigation on the automotive industry – conducted with Fintell Alliance – revealed that this industry does not rely heavily on cash, as initially expected by the stakeholders. This insight allowed the banks' KYC departments to break free from stereotypes. Through these collaborations with the private sector (the gatekeepers), we can respond more effectively as we learn from each other in terms of information, technology, and methodology.

In its mutual evaluation of The Netherlands\*\*, the FATF has noted the PPPs to be a 'key feature' of the Dutch AML/CFT system, with the FEC PPP as a strong forum to gather financial evidence, share best practices and discuss operational activities. I am proud that the FEC efforts are recognised internationally. Moving forward, it is the FEC's ambition to further expand and diversify its collaborative efforts with other stakeholders, both within and beyond the public sector.

### **A paradigm shift**

It is difficult to predict where we will be in ten years from now. I think that there are three developments that contribute to a fundamental change in our approach to fighting crime: internationalisation, digitalisation and the continuous shifts and rise of new threats to the integrity of the financial sector.

### *Internationalisation and changes in the geopolitical landscape*

The most crucial aspect for the coming years is the changing world, which forms the foundation for our work as regulators. As the world changes and becomes more internationalised, we see a rise in creativity, which is endless, especially when there are financial incentives involved. Thus, the challenge lies in constantly looking outward and adapting effectively to these changes, as I anticipate that internationalisation will increasingly impact our work in terms of what we do, how we do it, and where we do it. Criminal activities are already predominantly organised through international networks. As The Netherlands alone, we cannot solve this issue. Both as a regulator – AFM – and the FEC, we will need to consider the changes in the geopolitical landscape: things that used to be normal, may no longer be normal in the future.




**We will need to consider the changes in the geopolitical landscape: things that used to be normal, may no longer be normal in the future.”**

### *Digitalisation*

The world is also becoming increasingly digital. AFM is already shifting towards more data-driven supervision.

\*\*The FATF conducted its mutual evaluation of The Netherlands in 2022: <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-netherlands-2022.html> p. 5.



Simultaneously, digital crime is also on the rise, leading the FEC partners to examine different forms of criminal activities that arise in this realm. As a result of digitalisation, organisations must broaden their scope to address emerging issues, including the growing concern surrounding deep fakes and related phenomena. To effectively navigate these evolving challenges, organisations must adapt their methodologies to effectively combat digital crime, while upholding the principles of security and compliance.

#### *Shift and rise of new threats*

Finally, successes in safeguarding the integrity of the financial system in one place, will likely lead to a shift and the rise of threats elsewhere.

We have invested significant effort in combating money laundering, which has provided us with a decent understanding of illicit activities involving banks and cash transactions. I think that decentralised finance could soon become the new focus area from a financial crime perspective.

#### **Information sharing and privacy**

Data sharing brings opportunities, but there are also legal limitations. It is crucial to strike the right balance between privacy and fighting criminal activities. I believe that the Bill on the Data Processing by Partnerships Act (in Dutch: Wet gegevensverwerking door samenwerkingsverbanden, WGS), if approved, will advance information sharing with appropriate safeguards. Within the FEC, the public partners have already conducted thorough assessments into how and under which conditions information can be shared between the different FEC partners, in compliance with their respective mandates. The manner in which the FEC PPP operates could potentially inspire and guide other stakeholders in their own efforts to more

effectively combat financial crime. I believe that collaboration can really enhance the fight against financial crime and safeguard the integrity of the financial sector. TMNL is a great example of private-private cooperation with due consideration for privacy safeguards.

#### **Relevant AFM developments**

The AFM's supervisory role will soon be expanded to crypto-asset service providers under the Markets in Crypto-Assets Regulation (MiCAR). With the recent deals on the EU's AML Single Rulebook, it is also expected that the AFM's AML supervision – currently focused on the asset management sector and intermediaries in life insurances – will expand to other sectors. The parties that will be in scope of the EU Anti-Money Laundering Regulation and are expected to fall under the supervision of AFM, are crypto-asset service providers and crowdfunding platforms. At the AFM, we are working hard on implementing the actual MiCAR licensing regime whilst at the same time taking into account the risks of crypto-trading – for which we have issued multiple public warnings in the past. Collaboration with international peers will be key in managing the risks in the sector effectively. I also expect that with the ongoing geopolitical changes in the world, sanctions compliance will continue to grow in importance.

#### **Advice to compliance professionals**

Within both of my roles at the AFM and the FEC, I experience the importance of collaboration. In that context, I want to reiterate the African proverb “If you want to go fast, go alone, if you want to go far, go together”.





## Karlijn Jeurig-Koel

**Group director KYC & Financial Crime – Triodos Bank**

Karlijn has held the position of Group Director KYC & Financial Crime at Triodos Bank since 2021. With a master’s degree in criminology, she started her career as a Fraud Investigation Specialist at Ernst & Young. In 2012, she joined KPMG’s advisory practice, advising clients on matters of integrity and anti-money laundering compliance.



## Wibout de Klijne

**Director Compliance – Triodos Bank**

Wibout currently serves as the Director of Compliance at Triodos Bank and holds a non-executive Board Member position at Triodos UK. He started his professional career in 1997 as a security advisor at Rabobank. After serving roles as Head of Crisis Management & Fraud Investigation and Global Head of Compliance Surveillance & Investigations, he moved to Triodos Bank in 2019.

### Personal motivation

**Karlijn:** My purpose is to contribute to a more ethical society, which closely aligns with the mission of Triodos to ‘make money work for positive social, environmental and cultural change’. Financial economic crime is an abstract term, as it doesn’t directly address the underlying criminal activities, known as predicate offenses for money laundering.

**Wibout:** My purpose is to not only focus on technical compliance but also on effective compliance, ensuring that we align not just with the letter of the law but also its spirit. Criminals are innovative in finding new ways to commit their crimes. They often collaborate with one another and possess the resources necessary to perform their crimes; pursuing them is like a game of chess. Furthermore, I am enthusiastic about enhancing the effectiveness and efficiency of processes, an area we can and must improve.

## Changing our focus

**Wibout:** Criminals are always a step ahead, as they are not bound by the constraints of the law. Criminals can innovate faster with the advancement of new technologies, while public and private parties encounter legal barriers. Enhanced collaboration and sharing of information are important. However, even with these advancements, it is important to strike a balance between fighting crime and privacy rights. We should avoid granting unlimited power to public authorities to prevent the misuse of enforcement powers, as exemplified by the IRT affair in the 1990s\*.

Any detected unusual activity needs to be reported in the Netherlands. While the principle should be 'innocent until proven guilty', the monitoring and reporting process seems to suggest the opposite. Cases are sometimes left unaddressed by the public authorities due to a lack of capacity. This creates frustration and separation, whereas what is truly needed is enhanced collaboration. On the other hand, it is important to recognise that, like any other enterprise, public authorities must also make choices about the cases they pursue. I believe that there should be a more centralised strategy in the fight against financial economic crime, focusing on core crimes that need to be tackled rather than only the laundering process, as criminals will always find a way to conceal their illegal proceeds.

## From technical compliance to effective compliance

**Karlijn:** Both public and private parties should (re)consider their role and responsibility in detecting and reporting crimes. In recent years, there has been a significant focus on technical compliance, which resulted in financial institutions adopting a 'tick-the-box' approach towards compliance.

While this was necessary because of the immaturity of compliance organisations, drawbacks of this approach, such as de-risking and the exclusion of certain groups from the financial system, have also become apparent. Financial institutions should evaluate their approach towards customers and consider the risk of discriminatory practices.



**Financial institutions should evaluate their approach towards customers and consider the risk of discriminatory practices.”**

We need to question the fundamental reason for the existence of banks, as well as our investigative and supervisory authorities, while exploring ways to foster collaboration. Establishing common ground will enhance our effectiveness in the fight against crime. I also believe that investigative authorities would be more effective if they transition from a push to a pull approach, wherein banks investigate a certain modus operandi indicated by authorities. As part of this approach, authorities and banks work together in a concerted effort to detect new types of crime.

\*The IRT affair is a case in which the Dutch government was involved in the importation of drugs in its quest to dismantle criminal networks. However, its unconventional infiltration method resulted in the Dutch state facilitating large drug transports in the 1990s. See, for example, 'Parlementaire enquête oopporingsmethoden, IRT (1994-1996)', at Parlement.com.

In the future, advancements in data quality, technology and expertise will significantly enhance the effectiveness and efficiency of the KYC process, while bringing together expertise from various organisations will increase overall effectiveness. But also within organisations there is room for improvement by bringing knowledge together. Currently, KYC, screening, transaction monitoring, and reporting are too separated. Steps are taken to integrate them, and I anticipate this integration will accelerate in the near future.

**Wibout:** As banks, we will always be responsible for knowing our clients. This is not only important for anti-money laundering reasons but also for conduct reasons; i.e. do the products fit this customer, does our customer understand our products? Hence, if we want to work with shared KYC utilities, it will only be for retrieving verified data, not to lift the bank from its KYC responsibility. Not only banks need to enhance their data quality but also, for instance, Chambers of Commerce and the UBO Register.

Personally, I do not expect a major shift in effectiveness resulting from technology. AI will have an impact, but it will not radically change our way of working. Technology will enable us to work more efficiently, but it will not directly result in more criminals being caught. Criminals will find other ways to commit their crimes. There are even underground banking conferences where criminals exchange information on monitoring rules used by banks.

As of today, we have lost the fight against subversive crimes, and if we don't step up our game, the situation will worsen. We need more international cooperation and less bureaucracy between governments if we want to enhance the fight against subversive crimes.



**The added value of enhanced data quality and data sharing is that profiles of types of customers can be created.”**

### Data quality and data sharing

**Wibout:** The added value of enhanced data quality and data sharing is that profiles of types of customers can be created.

For example, data from the customs authorities can provide insights into the typical flow of goods within a specific industry. Data gathered by TMNL could be used for this same purpose within the boundaries of privacy legislation. Currently, we do not have an accurate benchmark of what is unusual and what is not, resulting in banks posing – unnecessary – questions to customers about transactions the bank cannot explain. With enhanced data insights, more accurate models can be developed. Although we can win a lot by using reference data, it is crucial to be mindful of potential privacy impacts and biases, as demonstrated in the Dutch childcare benefits scandal.

There were some calls to set up a centralised alert handling team for the Netherlands within Fintell Alliance and run within the already available mandates. I am in favour of these multi-bank transaction insights because it provides a more robust benchmark for distinguishing unusual from normal activities. Now we have to inquire with our customers since there is no alternative method to clarify the transaction. I do stress the importance of privacy as well. Using the mandates within the government with organisations of FIU, Police and FIOD should get the results we need.

## Organisation and workforce of the future

**Karlijn:** In the near future, we will be more focused on ongoing due diligence and less on periodic reviews. This will need to be enabled by regulatory changes following the AMLR. Transaction monitoring tools enable us to conduct ongoing due diligence, which requires reliance on transaction monitoring systems. Improved data quality and, subsequently, enhanced transaction monitoring will result in less alerts, yet at the same time, more complex alerts. I'm not confident that this will directly address capacity constraints, but I do believe enhanced analytical skills will be required to handle complex alerts. There will be more focus on alerts that matter.



**Transaction monitoring teams and KYC teams should increasingly operate as one team."**

**Wibout:** Transaction monitoring teams and KYC teams should increasingly operate as one team. Currently, there are too many handovers from one team to the other. Alerts requiring further investigation are handed over to KYC teams, as the transaction monitoring analyst does not have the skill set yet to obtain an adequate understanding of the client and the client's behaviour.

## A national crime prevention strategy

**Wibout:** As a country, as a government, our control of the fight against subversive crimes has slipped away. Within the governmental framework, utilising permit systems, strategically deploying the police, and exploring existing governmental powers offer

substantial possibilities. The organisation 'Human Rights in Finance' advocates for the government to leverage its current powers and concentrate on what is already possible. Rather than broadening the scope of the law to facilitate multi-bank transaction monitoring by overcoming existing privacy barriers, this organisation believes that the emphasis should be on maximising the potential within the existing framework. While I am of the opinion that implementing multi-bank transaction monitoring would reduce privacy concerns for a broader population, prompting a legal change for this purpose, I do agree that we can initiate improvements by better utilising existing powers. Collaboration should not solely target coordination among investigative and law enforcement authorities but should extend to other sections of the government as well. Currently, there is too much overlap or interference with each other's activities.

**Karlijn:** We need to appoint a national coordinator to detect crimes through analysing information available within financial institutions. The current approach is diffuse, makes no significant impact, and there is a tendency to point fingers at each other. The system is broken, not effective, and collateral damage is increasing. In a decade from now, this should look different.



**Wibout:** The way we work in the Netherlands is too fragmented, which leads me to believe that we must have had a high tolerance for money laundering; in a way, that is a government choice. It is imperative to establish a clear, national risk appetite for the country under the guidance of a national coordinator. If the risk appetite is low, it prompts the question of what measures are required to stay within the risk appetite limits. If we have zero tolerance for financial economic crime, we should also allocate adequate means to stay within the risk appetite. As a bank, we are also required to do this. While we may be shocked by subversive crimes, it is essential to recognise that these crimes are outcomes of choices. If these are outside the appetite, we should all take action. Merely pointing fingers at banks and modifying laws to enhance monitoring is not sufficient.

### Regulatory change

**Wibout:** There are more and more predicate offences for money laundering. ESG considerations will also increasingly be brought within the anti-money laundering framework. This also means that the facilitating role of banks is expanded since, in the end, there is a financial flow for virtually every activity. However, solely expanding the scope of laws and regulations in the fight against financial economic crime is likely to give similar outcomes as witnessed in the past years – a lot of effort with limited effectiveness.

Even without legislative changes, there is already an opportunity to proactively advance by enhancing collaboration with various organisations.

For instance, the Netherlands Labour Authority (NLA)\*\* possesses significant information, such as data on work permits or indicators of illegal workers residing at the same address.

Banks can play a more targeted supportive role in such cases. By seamlessly connecting data from diverse organisations, we can gain more precise insights and enhance overall effectiveness.

Presently, it seems that banks are required to obtain and document information and share it with the government to enable the government in its crime fighting efforts. The scope of the law is continuously expanded to increase information sharing, despite the abundance of existing information. Consider the numerous unusual transactions at FIU-NL that are never investigated. The current system seems too fragmented to effectively tackle financial economic crime.

### How to prepare for 2034

**Wibout:** I believe that truly understanding your client and your client's activities is crucial for banks both from a compliance and a commercial perspective. Furthermore, effective cooperation in the chain requires a common goal and respecting each other's efforts. For example, as a bank we need to monitor for signals of money laundering through tax evasion.

\*\*The NLA falls under the responsibility of the Ministry of Social Affairs and Employment and aims to ensure 'fair, healthy and safe working conditions and socio-economic security for everyone'. The NLA is, amongst others, responsible for detecting fraud, exploitation and organised crime within the chain of work and income and for supervising compliance with regulations concerning illegal employment.

In the Netherlands, so-called saldinisten withdrew large sums of cash in December only to redeposit the funds in January to avoid paying taxes on their savings\*\*\*. When we handed over transaction data of saldinisten to the Dutch Tax Administration, their initial response was that they wouldn't use the data. In their view, the relatively small amounts involved didn't justify the efforts needed to specifically address this type of tax evasion. Hence, banks are required to act upon such transactions, yet this same logic is not consistently applied to public authorities themselves. Examples such as these are detrimental to effective collaboration. We later established a very effective collaboration with the Tax Administration by engaging in joint discussions to outline our focus areas. Moreover, banks need to work in line with their mission, which will also enable them to define their approach towards compliance. When we, Triodos, act in accordance with our mission, we are very clear that we do not want our clients to avoid taxes.

**Karlijn:** KYC remains a central pillar in financial crime detection, also for the next decade. Data quality, technology and expertise are crucial for the future of compliance. Only with enhanced data quality, expertise to interpret the data and in-depth knowledge of criminal modus operandi transferred into effective detection rules and models, we can become more effective in detecting and reporting crimes. We need to step away from a siloed approach and integrate these three areas, i.e. data, technology and expertise. Effectiveness can be further enhanced by leveraging data and knowledge from different sources through effective partnerships.

**Wibout:** There are currently numerous new entrants in the financial market, for example, parties utilising blockchain and crypto technology, and this trend is expected to continue in the next decade. The authorities

have not yet fully understood or controlled these newcomers, such as blockchain and cryptocurrencies. However, delving into the dynamics of this chain is intriguing, specifically from an investigative perspective.



**Data quality, technology and expertise are crucial for the future of compliance. Only with enhanced data quality, expertise to interpret the data and in-depth knowledge of criminal modus operandi transferred into effective detection rules and models, we can become more effective in detecting and reporting crimes.”**

\*\*\* The tax authorities in the Netherlands use the account balance on 1 January to calculate the applicable tax.



## Anita van Dis

### Strategic Adviser – Public Prosecution Service

**Anita van Dis serves as a strategic adviser on criminal financial flows and as a coordinating officer in asset recovery at the Netherlands Public Prosecution Service. She is a seasoned public prosecutor, specialised in fraud and money laundering. Currently, her work involves policy and strategy development, primarily focusing on money laundering and confiscation of illicit assets.**

#### Personal motivation

Money laundering is a consequence of crime and inflicts harm on our society. It is, in my opinion, crucial to recognise that combatting money laundering is not just about addressing individual crimes but rather about tackling a larger and more pervasive problem. Furthermore, the fight against money laundering is constantly evolving. While the current focus mainly revolves around drug-related crime, there is a growing emphasis on responsible and ethical business practices, including those related to ESG concerns. At present, gathering evidence is difficult due to complex causal relationships, evolving public interests, and changing standards. However, new rules, on the topic of ESG for example, help us to identify the entire chain of beneficiaries of illicit activities. Such a development truly motivates me in my work.

#### The importance and the downside of AML compliance

I would like to start with explaining what we know about how criminal money, which is earned through, for example, fraud and drug-related crimes, circulates in the criminal world. Where money flows stemming from fraud usually occur electronically, money flows stemming from drug-related crimes often are in cash and – increasingly – in cryptocurrency. Still, it is rare to find significant amounts of criminal cash flowing directly into legitimate businesses. A large portion of the drugs money stays underground and is used for payment of new deliveries. Another portion is funnelled to regions abroad, like the Middle East, where it either remains or where underground banking systems facilitate its movement. Once integrated into underground banking systems, the cash is often utilised in TBML schemes. Further down the line, the funds are invested in legitimate business and ultimately make their way back to the criminals here in the Netherlands. It is also important to acknowledge that both drug and fraud criminals apply fraud techniques to hide the beneficial owner and/or source of proceeds when utilising the legitimate financial system and investing their proceeds in legitimate businesses. As a result, it becomes difficult for gatekeepers to detect connections with criminal conduct, resulting in fewer SARs. While we possess information about the flow into the underground banking system and have an understanding of TBML schemes, details of investment flows are generally less clear.

By this stage, the link between criminal activities and the funds has often vanished. AML compliance measures and information on unusual transactions from the private sector are essential to bridge this intelligence gap. This makes private sector efforts crucial for effectively combatting money laundering and preserving the integrity of our financial systems.

While AML legislation is crucial for combatting money laundering, it does come with its downsides. An example of this is the impact of the legislation on developing countries seeking to enter the global financial markets. These countries often suffer from corruption and are considered to be of higher risk, also because of their heavy reliance on cash transactions. Because of limited financial resources, they might also not be able to comply with standards set by international organisations such as the FATF. As a result, certain countries and sectors may be excluded by the financial sectors of more developed countries.

It is important to recognise that banks have been designated as gatekeepers with specific obligations in preventing money laundering. Holding them accountable through proper enforcement can serve to firmly establish their legal and societal responsibility, to ensure compliance and to combat illicit financial activities. Given their role and responsibility, I do not view the sanctioning of non-compliance with AML/CFT regulations as a means of criminalising them and/or an ineffective use of public resources.

### **Current issues within the AML system**

To me, there are various obstacles that hinder the fight against money laundering. A first obstacle is the lack of adequate international cooperation. We, as public prosecutors, face challenges in evidencing money laundering cases. While we can easily identify compliance deficiencies in financial

institutions, establishing concrete evidence on a money launderer is difficult as we are often confronted with intelligence gaps. The changing geopolitical landscape increasingly limits cooperation with counterparties from certain jurisdictions, such as Russia and China. Misalignment between legislation of countries complicates international collaboration even further. Finally, capacity problems in certain countries lead to a prioritisation of court applications, with a preference for addressing violent offences over money laundering. FIUs and private parties often do have the necessary information but cannot or do not share it.



**The changing geopolitical landscape increasingly limits cooperation with counterparties from certain jurisdictions**

A second obstacle is the current privacy legislation. This legislation, including the strict interpretation by the Dutch DPA, hinders the effective exchange of valuable information between public and private parties. I also experience that important public parties with a role in crime prevention, such as municipalities, can be hesitant to share information.

Even when permitted, they do not share information since the strict and resource-intensive compliance requirements do not align with their capacity. Furthermore, unlike gatekeepers, they have no reporting obligation, nor a right to report to the FIU. This prevents the efficient exchange of important information and impacts the effectiveness of the fight against crime.



## The importance of PPPs

The programme Ketenvesterking ('chain enhancement') is important as it helps us visualise the reporting chain – i.e. the links between the parties in the preventive and repressive AML policy – and improve collaboration from reporting to investigation stages. Information sharing plays a vital role in this regard, and the Serious Crime Taskforce, as a PPP under the Financial Expertise Centre, facilitates this process. However, the aforementioned stance from the Dutch DPA is not helpful. It is unfortunate that despite having all the necessary intelligence within the AML chain of public and private parties, we are hardly able to connect the dots.

Another unfortunate aspect is the lack of an effective feedback loop within the reporting chain. As shown in the annual report of the FIU, over 70% of the suspicious transactions reports received by the Public Prosecution Service are connected to existing investigations. An improved feedback loop could enhance the effectiveness of the reporting chain. In my opinion, the prosecution of banks has not disrupted the relationship between the sector and the OM.

To the contrary, I would say, as it has provided a renewed impetus to PPPs. In my experience, banks have demonstrated enthusiasm and a clear willingness to collaborate actively in the fight against money laundering. Banks also want to improve the effectiveness of their AML programmes.

## The imbalance between the public and private sector

I agree that the balance between the public and private sector is not always optimal. The (increasing) legislation places a significant burden on private parties, requiring substantial investments from them.

At the same time, developments and investments within the public sector have been limited. This creates an imbalance between both sectors. I believe it is evident that the public sector needs to improve its efforts. Public parties that have a role in combatting subversive crime should actively take on their role. A national strategy for combatting money laundering could assist these public parties in integrating this task efficiently into their work and allocating adequate resources to it.





The Ketenvesterking programme plays a crucial role in this regard, as it demonstrates the efforts currently being made within the public sector. Next to this programme, the Public Prosecution Service, together with investigative authorities and the FIU-NL, has drawn up a joint strategic programme to tackle criminal money flows. This programme includes seven lines of action for the coming years, such as obtaining a shared intelligence position regarding criminal money flows for law enforcement, collaboration with both private parties and international partners, and enhancing the effectiveness of gatekeepers and supervision of gatekeepers.

In addition to this, there should be a more balanced focus of supervision that goes beyond mainly targeting the banking sector. Currently, there is significant societal pressure on banks, which can sometimes overshadow other potential areas of concern. I strongly believe that sectors such as real estate and investment funds should also undergo stricter supervision.

### **The paradigm shift**

Over the past decade, there has been a significant shift in the perception of AML efforts. The pressure from society has intensified, largely fuelled by events such as the Panama Papers. This has prompted a change in how AML compliance is viewed. Where it used to be mainly considered an obligation, it is now recognised – especially by major banks – as something that is actually important. Furthermore, a global convergence has taken place in legislation, and we have also observed a significant increase in the number of gatekeepers, primarily driven by the emergence of new forms of financial services, such as cryptocurrencies. I believe that in the next ten years the implementation of ESG and environmental regulations will especially change the FEC compliance landscape.

As a side-effect, these rules will produce evidence for money laundering cases, particularly when it comes to issues such as modern slavery (i.e. a predicate offence for money laundering) in production processes or environmental damage caused by certain products. The private sector will have a clear(er) picture on the production processes and, as part of their gatekeeper role, will provide intelligence to investigative authorities for further follow-up. The Public Prosecution Service can utilise this intelligence in their analyses. I believe that the ESG regulations themselves will not create new criminal offences, but they will expand the duty of care resting upon financial institutions and their board members. Moreover, when building a criminal case, non-compliance with such regulations can be used to evidence the 'knowledge' element (i.e. knowledge of the underlying offence, which may be required for a money laundering conviction).

A second important development in the fight against money laundering is the European Directive on non-conviction-based confiscation, and subsequent implementation in national law. This allows public prosecutors to confiscate assets without first having to obtain a criminal conviction. In these situations the burden of proof about the (legitimate) origin of assets will be on the suspect instead of the prosecutor. This is a really important tool to disrupt criminal operations.

History has shown that criminals will eventually be caught. Both public and private parties will continuously develop new methods to trace criminal activity and illegal proceeds, often in ways that criminals had not yet anticipated during the commission of their crimes. Criminals should thus be aware that they can never escape detection.



### **Future readiness of the Public Prosecution Service**

Criminal organisations are becoming increasingly sophisticated and specialised in, for example, money laundering. Therefore, to ensure our readiness for the future, our focus in the fight against money laundering is continuously expanding beyond the mere confiscation of illegal proceeds, to also disrupt criminal revenue models, but also to continue with our focus on gatekeepers of the financial sector. In this regard, we are actively innovating in digital investigations. This process includes investigating and analysing digital information to trace and reconstruct activities or events that have occurred on digital devices or networks, as well as efforts to identify illicit flows through the use of

cryptocurrencies. Besides, we are gaining more and more understanding and insights into the entire money laundering chain. This is achieved through the initiation of various strategic programs on areas such as TBML and underground banking.

Furthermore, we are continually improving our international cooperation. Even if challenges arise from the Dutch DPA, which I am optimistic will not persist, we remain committed to finding alternative approaches to foster innovation and cooperation. Importantly, the upcoming EU legislation makes positive strides in this regard.



# Timothy Goodrick

Director – KPMG Australia

**Timothy Goodrick is Director in KPMG Australia’s financial crime practice, specialised in leading projects to design and implement effective systems to combat financial crime, with a focus on financial crime transformation. Throughout his career, Tim has worked in both public and private sectors, and his work included leading Australia’s AML/CTF strategy in government, working extensively with FATF and FATF-Style Regional Bodies members, and supporting financial institutions in financial crime transformation.**

## Personal motivation

I get to contribute to something that is not just good for our clients but also good for society and communities as a whole. For me, working in the field of financial crime is more than just a compliance challenge. It is a challenge to better detect, prevent and deter financial crime as a whole, and this is what motivates me.

In my work, I aim to take a holistic approach towards designing and implementing more effective and sustainable financial crime programmes that align to the regulatory requirements. I often see that regulatory frameworks are blamed for being inefficient and ineffective in financial crime prevention. While laws can certainly be improved, in many cases the problem lies with ineffective or inefficient implementation. Institutions should focus on the risk-based approach by first understanding the risks they face and then

interpreting laws in such a way that the risk is adequately addressed.

## The system is not broken, but can be improved

There is an ongoing discussion on the effectiveness of the financial crime prevention regime. We must be conscious of the displacement effect: when one way is blocked, criminals will find another way to launder their proceeds of crime. However, we have to recognise the progress that we have made; it is only two decades ago that banking clients could still use anonymous and numbered accounts.

Completely throwing out the system is not the answer. The system is not perfect, but as a global community, made up of government authorities and the private sector, efforts are being made to improve the effectiveness of the regime and these efforts need to continue. Take transaction monitoring as an example – major improvements need to be made and are being made, as the current state of high false-positive rates, often well above 90%, is not sustainable.

## The next big thing

In the short term, we will see more integrated teams and more integrated solutions across the bank. We are seeing a greater focus on financial crime, including at the C-suite level. We will also see incremental improvements in the short term as processes and systems evolve to be more effective and efficient.

In ten years’ time, CDD and transaction monitoring systems and processes will be radically different.

The current onboarding processes often contain manual aspects, which are difficult to manage and result in poor customer experience. Monitoring of the customer lifecycle will not be the same. I expect that basic customer risk scoring models will be replaced by advanced models, which will introduce behavioural factors and may vary among different customer segments. There will be a convergence of CDD with transaction monitoring, in which customer risk assessments become more dynamic with the use of transaction information.

Straight Through Processing, especially for retail clients, will improve. It may, however, also introduce a new challenge of effectively mitigating fraud risks. The onboarding for non-individual/institutional customers will be more complex. However, improvements will be made through the ingestion of information from third-party data sources, which will make it possible to identify beneficial owners and ownership structures, and monitoring changes in these, on an ongoing basis.



**I expect that basic customer risk scoring models will be replaced by advanced models, which will introduce behavioural factors and may vary among different customer segments. "**

Furthermore, the method of information gathering from clients is expected to evolve with the use of more interactive portals that include tailored information and document requests, leading to an enhanced customer

experience. As a result, the onboarding process will become significantly faster in the near future. When we consider transaction monitoring, the rule-based engines for detecting suspicious transactions will be increasingly substituted with advanced models based on AI/ML techniques. This is coming much faster than anticipated. During our interviews with global thought leaders two to three years ago, this was seen by many as something that is yet to come\*. We are, however, already seeing this in place, as complex transaction monitoring systems are already augmenting standard detection systems and will be taking over elements. Using AI/ML can help looking beyond behaviour, but also helps to predict suspicious behaviour we have not seen yet.

The other major advance that we see is rapidly taking place, is using a transaction monitoring copilot to increase the effectiveness of transaction monitoring investigations while significantly reducing resources.

The transaction monitoring copilot has the capability to ingest all relevant case information (customer, transaction and third-party information), perform an initial analysis and generate a narrative. GenAI is already being used for developing narratives and case notes, which will be reviewed by an analyst. This transformation will significantly reduce alert-handling times. We are already seeing some of these advancements, and in the next ten years, this will be the norm.

### **The importance of risk assessments**

I believe that an accurate understanding of risks can enhance the fight against financial crime. To increase this understanding, it is imperative to use relevant and up-to-date data, rather than data that is several years old.

\* [Financial Crime – A Paradigm Shift \(kpmg.com\)](https://www.kpmg.com/au/issuesandinsights/articlespublications/financial-crime-a-paradigm-shift)

Using near-time data to assess risks and, more specifically, changes in risks, and directly feeding it into the risk assessment, will significantly improve institutions' understanding of risks.

Additionally, institutions should improve the way they use the risk assessment. I have seen a number of good risk assessments, but often they are done to tick a regulatory box rather than for the purpose of actually driving the institution's AML programme. Institutions should have the end goal in mind from the start of the risk assessment process and ensure that the work does not end once the risk assessment itself is done. They should also be able to demonstrate the risk assessment has been used to drive the financial crime programme under the risk-based approach.



### Breaking through silos

Having the first and second line working together instead of in silos is a big challenge. Financial Crime Operations within the first line is often not given due weight, or sometimes not even a seat at the table where key decisions are made. This is despite the size of

such teams and the value they add given their expertise on the ground.

First line and second line teams need to work closely together with clear feedback loops. When this goes wrong and teams work in silos, we often see either accountability gaps or duplication of effort – both are poor outcomes.

The starting point is setting a clear three lines of responsibility, and maintaining this over time by evaluating and ensuring that it remains fit for purpose.

### Workforce of the future

I believe that the main change in the financial crime workforce will be in operations, with a key change in the content of the work. Analysts will be spending more time analysing data rather than collating data. This will drive process efficiencies and lead to better outcomes, both from a financial crime perspective – as time can be spent on actual investigation – and from an employee perspective. Offshoring activities to reduce cost base will continue to play a role for large institutions, which increases the importance of having the right governance and oversight in place.

### Roadblocks for change

Institutions face significant challenges to find the right pathway to transform their financial crime technology. Legacy systems are difficult to replace, and institutions are faced with complex choices, such as building an own transaction monitoring platform, buying off the shelf, or partnering with another entity. There are good and bad examples for these different options. However, this is not a reason not to start now by setting and agreeing to the 'north star' and defining a strategy on how to get there.

This technology strategy should include incremental value throughout the project, rather than waiting 5+ years to see any benefit. It should also align with an institution's data strategy, which allows an institution to take tactical action where necessary, while remaining conscious of the bigger picture and avoid constant 'firefighting'.

Part of the challenge is engaging with the regulators to push the boundaries. There are regulators that encourage innovation and changes, but there is also a global propensity to fall back on what is familiar. For example, institutions believe that they will not get into trouble with the regulator for using an off-the-shelf transaction monitoring platform. Going down a different path with AI/ML is not without challenges from a cost perspective, but the upside is so significant that with the right controls in place, it is a risk worth taking. Engaging with the regulator early is a critical step while then keeping them informed along the journey.

### Preparing for 2034

I believe financial institutions should focus on:

1. Recognising the important role of financial crime operations teams and giving them a seat at the table when driving change in the institution.
2. Setting the future strategy for TM by identifying where they want to be in ten years' time from a process, technology and data perspective, and designing a path to get there with incremental benefits;
3. Innovating customer due diligence at onboarding and on an ongoing basis, to reduce manual processing, improving handling times and improving customer experience.

It is time to start now, as changes are coming much faster than anyone has anticipated!



**Institutions should be able to demonstrate the risk assessment has been used to drive the financial crime programme under the risk-based approach."**

# Idzard van Eeghen



Advisor to the board of bunq

**Idzard Van Eeghen has a diverse work experience, spanning different companies and roles. Idzard has been with bunq since May 2018, consecutively fulfilling the role of Chief Finance and Risk Officer (CFRO) and CFO. Currently, he is working as advisor to the board of bunq, the second-largest neobank in Europe. He also serves as non-executive board member of the Norinchukin Bank Europe, Stichting Impact Matters and Handelshuis Van Eeghen & Co.**

## Landmark ruling in the bunq appeal against DNB

In October 2022, the Trade and Industry Appeals Tribunal (CBB) in the Netherlands ruled in favour of bunq in its case against the DNB. Rather than applying a rule-based approach, bunq used an AI-driven risk-based approach to detect financial economic crime risks. The CBB ruled that there was insufficient evidence to support several instances of non-compliance alleged by DNB. However, some other instances of non-compliance were, according to CBB, adequately substantiated by DNB. This landmark case marked a turning point in DNB's approach and paved the way for more innovative and effective methods of complying with anti-money laundering laws. A month before the ruling, DNB had already released a report titled 'From Recovery to Balance', promulgating a more risk-based approach, using technological innovations to combat financial economic crime. In his capacity as CFRO, Idzard led the case of bunq against DNB.

## Personal motivation

Detecting financial economic crime serves a common good, but also helps to build a sustainable business. It is a costly affair to have fraudulent customers. If you can mitigate that, it should help to run your business more efficiently. What I like about bunq is its user-centricity, coupled with its focus on financial economic crime. The traditional system is very risk-averse at the cost of user-friendliness, whereas the user should come first and the financial economic crime regulations should be designed in such a way that they do not hinder serving users well. There have been many court cases where banks have been reprimanded for not acting in the best interest of their clients.

## Client-centricity

bunq combines user-friendliness and doing the right thing – making sure that the rules are applied in such a way that we also help more vulnerable user groups. While many banks promote a customer-first approach, the mindset at bunq is really different compared to other banks. At bunq, if a new proposition is introduced, the first question is always: 'How does it benefit our users?' Anti-money laundering laws dictate what institutions 'have to do'. bunq follows the law, while at the same time asking itself how effective compliance can be achieved in a user-friendly way. For example, we do not want to pose questions to our users when the outcome does not make a difference in detecting fraud.



Asking questions is unavoidable to get to know your user better, but it has limited usefulness for detecting fraud, and we rather focus on making our user's lives easier.

In general, I believe that, when investigating customers, one should keep in mind that customers who have been with a bank for many years and have not displayed unusual behaviour will not all of a sudden become a fraudster. Fraudsters typically do not wait for years to become a fraudster. Hence, in a risk-based system long-time customers should be approached with some consideration.



**To keep up with changing regulatory requirements and emerging threats, it is crucial to have skilled IT personnel, proficient coders, and systems that can be rapidly adapted. "**

### Trends in financial crime compliance

There are several trends within the financial economic crime domain that, in my opinion, will shape the future of compliance, including the following:

- Increased harmonisation of AML legislation in the EU. Full harmonisation remains a work in progress, but I believe that applying the same standards across the EU will contribute to more efficiency for banks.
- Transitioning from rule-based ('tick-the-box') towards a more effective compliance framework. The impact of a rule-based approach became apparent in the past years (e.g. certain groups of high-risk

customers, such as sex workers, were categorically excluded by some banks). DNB and financial institutions are already engaged in discussions on how to move to a more risk-based approach.

- The balance between privacy and the prevention and detection of financial crimes may shift towards detection of crimes. Presently, privacy is sometimes seen as an impediment to fostering more efficient collaboration between banks and authorities in combating financial economic crime. I believe, however, that the public may be willing to sacrifice some aspects of privacy if it contributes to the fight against serious crimes. I also believe that, in view of the ever-expanding range of information that banks need to obtain from their customers, it should be clearly defined upfront what the purpose is of collecting the information and what will be done with the information. For example, in the ESG domain, banks are supposed to get increasingly more information about the social, governance and climate impact of their clients. What if forced labour in our user's supply chain is detected, should this be reported to public authorities, and what will they do with this information?
- Criminals exploiting new technologies pose a challenge. There is a permanent battle between fraudsters and banks. Banks should adopt innovative technologies and formulate financial economic crime strategies to proactively mitigate potential emerging technology risks. While ML and AI help banks to detect fraudsters, criminals also leverage these technologies, as seen in instances such as deep fakes. This is not just a bank thing, but everyone has to contribute: police, retailers, etcetera.

- The use of ML for monitoring transactions will continue to increase, but this can be seen as a natural progression of the model itself – the longer it is deployed, the better it performs. This is more of a trend rather than a paradigm shift. Notwithstanding the increased use of models, I anticipate that human oversight will remain important. Also, for larger customers served by relationship managers, one would hope that these managers know their customers well enough to pick up suspicious signals that models cannot see.

### Future-proof financial economic crime organisation

To keep up with changing regulatory requirements and emerging threats, it is crucial to have skilled IT personnel, proficient coders, and systems that can be rapidly adapted. Adaptability and agility are essential to ensure a swift response to changing requirements and emerging threats.

I anticipate that there will be fewer, yet better-trained analysts in the future. The qualities of future analysts are, for example:

- strong analytical capabilities to detect anomalies;
- sound judgement to recognise patterns and make informed decisions, including when to blow the whistle and when not to;
- ability to quickly grasp and stay up to par with new information, such as the latest fraud trends and techniques;
- a comprehensive understanding of customer behaviour, be it a company or an individual, and the ability to discern whether it aligns with the customer's profile.

Financial institutions and regulators should focus more on catching the 'big fish', i.e. high-impact fraudsters, such as those evading sanctions, rather than small-scale fraudsters.

This requires well-trained, smart analysts who closely collaborate with relationship managers to form an accurate and comprehensive understanding of the customer.

### Increasing effectiveness

Apart from the financial economic crime domain, institutions need to stay up to par with ever-expanding rulebooks on all kinds of topics, creating pressure for financial institutions. Adding to this pressure, supervisors, for a long time, adopted a rule-based approach towards compliance, rather than a focus on the effectiveness of the measure. It is easier to supervise whether checklists have been followed than looking at the effectiveness of the entire framework, which can have multiple dimensions, such as effectively detecting fraudsters and user-friendliness.

The focus should be on the overarching goal of the law, i.e. the prevention of financial economic crime.

To me, this is an 'outcome-based approach', enabling regulators to provide guidance and oversight based on the desired (high-level) outcome.

Recently, there appears to be a shift towards a more open dialogue between DNB and the banking industry regarding a risk-based approach and a focus on enhancing effectiveness of financial economic crime prevention measures. There is a growing recognition of the current imbalance in the number of employees dedicated to fighting crime between public parties and banks. I believe that supervisors should have a deep understanding of what truly matters for the overall health of banks and distinguish between key priorities and minor details. While addressing details remains important, it should not overshadow the bigger picture.

I think that both the financial institutions and regulators should have teams with a balanced mix of skilled professionals, with a greater emphasis on crime fighters rather than solely legal experts.

The primary motivation of crime fighters is to catch criminals, whereas legal professionals may have different motivations centred around following rules, procedures and completing checklists. A diverse workforce can contribute to more balanced decision-making which will, in the end, increase effectiveness.

### Information sharing

I believe that information sharing between financial institutions, for example, information about known fraudsters, can enhance the fight against financial economic crime. In my opinion, the government has an important role to facilitate this process. However, collaboration should have clear goals and be judged on its effectiveness, or else it becomes another source for bureaucracy.

A dilemma revolves around how to act upon information about known (past) fraudsters: deny them access to a bank account or not? Since everybody needs a bank account, they could be offered ring-fenced accounts with only limited payment opportunities, enhanced monitoring and, as a consequence, slower service. Clear guidance from the authorities on this issue would be welcome. Another key question revolves around how much privacy we are willing to compromise to enable information sharing for enhanced effectiveness in the fight against financial economic crime.

### Prepare for the next ten years

Institutions should transition from a rule-based approach towards an approach that is focused



**Institutions should transition from a rule-based approach towards an approach that is focused on effectiveness of the financial economic crime prevention measures; this is what I call an 'outcome-based approach.'**

on effectiveness of the financial economic crime prevention measures; this is what I call an 'outcome-based approach'. The current reality is, however, that many financial institutions are in the process of repairing their processes and gaps taking a 'check-box approach'. To some extent this is unavoidable as gaps should be addressed.

On the other hand, steps are already taken to move towards a more outcome-based approach, with DNB and Dutch banks having identified high-risk industries and determining the necessary checks to be carried out when opening accounts and thus preventing entire groups from being excluded from the banking system. I expect that this outcome-focused agenda will likely extend over the next five years. I also believe that institutions should focus on emerging risks, such as new forms of fraud, e.g. through the use of technology. Finally, I believe we can enhance effectiveness through increased international harmonisation and information sharing. This requires agreement across jurisdictions and the collaboration between all stakeholders: authorities, retailers, businesses, and banks.



# Wim Huisman

Professor Criminology – VU Amsterdam

**Wim Huisman is Professor of Criminology and the Head of the VU School of Criminology. Wim Huisman is founder and board member of the European Working Group on Organisational Crime (EUROC) of the European Society of Criminology and a past president of the Division of White-Collar and Corporate Crime of the American Society of Criminology. The research focus of Wim Huisman is on the field of white-collar crime, corporate crime, and organised crime, including research on effectiveness of AML regulation and financial crime compliance.**

### Personal motivation

As an academic, I have been studying white-collar crime for almost thirty years now. I am intrigued by this type of crime. Two to three decades ago, there was a lot of concern about 'ordinary' street crime, but not so much interest in white-collar crime. Our understanding of crime primarily focused on street crime, and explanations for this type of crime were found in the characteristics and background of the offender, such as broken families, low levels of education, poverty and proneness to addiction. This knowledge didn't fit with white-collar crime, which interested me. Why would a white-collar offender, often a successful businessperson or corporate executive, commit a crime?

Another fascination is that street crime genuinely feels like crime due to direct victimisation and obvious criminal acts. In

contrast, white-collar crime is often committed in the context of legitimate business and economic activities, which brings a challenge in exposing the crime. My motivation is to find out what drives a white-collar offender and why white-collar crimes qualify as actual. The main purpose of criminal justice is to differentiate the black from the white, the good from the bad. But white-collar crime is mostly about shades of grey. Criminalised non-compliance in business operations often does not stem from commissions ("you shall not murder", implying a deliberate action to commit the crime) but from omissions ("you have to identify your customer", meaning that by refraining from taking action you commit a crime). This calls for other types of explanations, in which not only individual traits, but also organisational dynamics play a role.

### The next big thing

The biggest contributor in the next ten years to fight financial crime will be AI. I expect an arms race between the regulator and the offender. Regulators have already started to use AI in monitoring compliance. Private parties, or gatekeepers, are increasingly viewed as 'co-regulators', and increasingly apply AI in this role.

On the offender-side, there is an increase in the use of (generative) AI, such as for creating fake news, fake data, CEO fraud and so on, and this is expected to amplify in the future. Trading algorithms have already committed market manipulation. I believe that this dynamic is shaping a future where regulatory algorithms will compete with offender algorithms.

Financial institutions are gatekeepers of the financial sector, and if they do not comply with the law, they will shift from being the problem solver to the problem itself, from being a 'partner in the fight against crime' to a (corporate) criminal. AI will play a role in this, since the various roles, responsibilities and tasks that are now executed by humans, will shift to AI. The trend of attributing regulatory responsibilities to gatekeepers in various domains of financial crime (money laundering, bribery, ESG, etc.), entails that these gatekeepers will be the frontrunners in developing and using regulatory AI. If financial institutions and regulators won't take pre-emptive action against the use of AI by offenders, awareness will only come when it is too late. That's the story of history.

### **A futureproof financial economic crime organisation**

In a futureproof financial economic crime organisation, I expect that employees will mostly be guiding the systems driven by AI. Instructing and understanding AI, requires a high level of knowledge and employees with more diverse backgrounds. The field of financial crime compliance was initially dominated by lawyers; with the shift of 'compliance 1.0' (rules and regulations) to 'compliance 2.0' (culture and conduct) this moved to behavioural scientists, and now we see the influx of data scientists.

I believe that the financial sector is leading in the transition towards a new organisational culture. Other industries – such as law firms – are lagging behind, as we have seen in recent scandals.

This is surprising, considering the level of expertise on compliance in this sector. Two to three decades ago, organisational cultures in the financial sector were more homogeneous, as everything was business-oriented.



**Research on motivations for AML compliance, indicates that the motivation is primarily extrinsic. Compliance is driven by a desire to avoid liability."**

Currently, one-third of bank employees is engaged in combating financial economic crime, which must have an impact on the organisational culture, becoming more compliance-oriented and risk averse.

I hold both positive and negative expectations about the organisational (compliance) culture:

- A positive aspect is the increasing cultural heterogeneity within banks. The ING case (please note: the 'Houston case', in which ING accepted a EUR 775 million settlement of the Dutch Public Prosecution Service for violations of the Dutch Money Laundering and Terrorist Financing (Prevention) Act – Wwft) shows that non-compliance was caused by prioritising business over compliance, indicating that the power balance was not right. The case demonstrates the need for change, emphasising the significance of the 'tone at the top' and board responsibility for compliance. Rabobank – which is currently under criminal investigation – and Volksbank have appointed a CFECO as a board member, someone focused on compliance rather than business. From a cynical view, this may be perceived as symbolic, but in a more optimistic view, such a board position may impact the tone at the top regarding financial crime compliance. This shows the positive potential regarding cultural change

- On the negative side, research on motivations for AML compliance, indicates that the motivation is primarily extrinsic. Compliance is driven by a desire to avoid liability. This is a barrier for cultural change, as compliance remains predominantly business-oriented, centred around preventing penalties and costs. Previous cases of appointing a CCO on the board after a major financial crime scandal showed that some of these new CCOs perceived preventing corporate liability as their main responsibility, instead of achieving actual compliance.



**A method proven to be more effective, involves analysing compliance trends over time (i.e. longitudinal analysis)."**

Another interesting development is that compliance is becoming a risky job. For deterrence reasons, the emphasis of punishing non-compliance by regulators and law enforcement agencies has shifted to individual executives instead of companies alone. Initially, CEOs were prosecuted and even jailed for non-compliance.

Now that companies have started appointing persons responsible for financial economic crime compliance within the board, the personal liability for non-compliance may shift from the CEO to this person, thereby becoming what is called in criminological literature 'the vice-president responsible for going to jail'. This is already happening in the US. With persons responsible for financial economic crime compliance within the board, it is even more apparent who will be held liable in case of serious non-compliance.

The Wwft even includes a requirement to appoint a board member who is responsible for ensuring compliance with this law. This personal liability of compliance officers may be seen as a dark side of this development.

### Emerging threats

I believe that climate change is an emerging threat for the financial sector, which is illustrated within the ESG development. Besides the devastating effects climate change has on the environment and humanity, ESG legislation has a tangible impact for financial institutions.

Legislation creates new responsibilities, but also new crime. For example, financial misreporting would not exist without reporting requirements. New legislation leads to crime in three ways:

1. By not complying with new legislation you break the law.
2. Corporations will try to find loopholes.
3. Compliance has a price-increasing effect; the law is aimed at protecting certain interests, such as sustainability, and as a consequence of complying with legal requirements, products or services become more expensive. This creates an incentive for fraud, i.e. by offering a service for the premium price, while actually producing or executing it in a substandard, non-sustainable and therefore illegitimate way.

## Evolving regulation

Regulation evolves by creating circles or layers of regulation. The first layer is the actual crime that causes harm: the things you should not do. Such as committing fraud. The second layer is secondary (derivative) legislation: legislation to prevent breaking the first layer, such as a positive obligation to prevent fraud, by putting in place compliance management systems. Not complying with this second layer of regulation is criminalised by itself, as is shown by the example of AML legislation. A third layer is currently also being created: by trying to solve issues that gatekeepers are struggling with, regulators issue guidance to fill in open norms.

This guidance is normally a soft law instrument without legally binding force, but becomes a type of regulation itself when soft law compliance is expected by regulators, such as the DNB Guidance on the SIRA. Finally, regulated companies develop their own tools, and once regulators are positive about these tools and make those tools mandatory, this creates a fourth layer.

This entire system is called the 'regulatory creep' – creating layer after layer of regulation. Initially, only the breach of the first layer was seen as crime. However, also the breach of the subsequent layers of regulation are criminalised. Instead of preventing the real crime, for which this regulatory system was designed, financial economic crime regulation mostly produces new, corporate, crime when gatekeepers do not sufficiently comply.

## The future of collaboration and information sharing

I believe that information sharing between private parties, as well as between private parties and the government, will increase. The pressure towards more public-private collaboration is stronger than the pressure against such collaboration.

The opposing force is distrust, as well as privacy regulations, but I expect this will be resolved in the future as the push towards increased collaboration to fight financial crime is simply stronger. Working together, which is also proposed in the Dutch Bill 'Plan van aanpak witwassen', is in my opinion the only solution to tackle the problem of displacement. I firmly believe that collaboration is the only way to address these issues.

The dual position of the regulator towards the gatekeeper is a struggle. On the one hand the regulator is partner in the collaboration, but on the other hand the regulator can be the 'police officer' if the gatekeeper is not doing the job good enough. As a gatekeeper, how can you trust a governmental partner in sharing information, when this partner may use this information to punish you? This is something new. We do not know yet how this is going to work out. Just like we would not have foreseen ten years ago that banks – and even their CEOs – would be criminally prosecuted for not fulfilling their financial crime compliance tasks.



**This is a limitation in ML as well: in relying on past data, it tends to focus on the high-risk group, finding non-compliance within this group again, but potentially overlooking issues in other groups.”**

## Longitudinal patterns within compliance

Regulators have the ambition to work risk-based and data-driven. However, this is not what they are currently actually doing. At this moment, there seems to be a gap between the desire to work data-driven and the ability to do so. Because of this, they are also not able to work risk-based. There are multiple barriers that withhold regulators from working data-driven: people, expertise (also relating to AI), funding and the fact that regulators generate their own data, but do not manage this in a way that allows proper predictive analysis.

Predicting the future is about understanding the past. To pursue a risk-based approach, regulators commonly rely on typologies, but these are often static and rooted in subjective assessments of a company's risk level. A method proven to be more effective, involves analysing compliance trends over time (i.e. longitudinal analysis). A study within the chemical industry I was involved in revealed the importance of such a longitudinal analysis; companies deemed as low risk in the past transitioned to higher risk, due to shifting compliance behaviours over the years. And vice versa. There may be various factors driving these various trajectories in compliance. A risk-based approach therefore requires a more dynamic view on corporate compliance.

The majority of regulatory capacity is allocated to a select few gatekeepers, which can be perceived as high risk. This creates a confirmation bias. The chemical industry study illustrates that low-risk companies can transform into high-risk entities, a shift undetected by the current regulatory approach within the financial sector. This is a limitation in ML as well: in relying on past data, it tends to focus on the high-risk group, finding non-compliance within this group again, but potentially overlooking issues in other groups.



**The majority of regulatory capacity is allocated to a select few gatekeepers, which can be perceived as high risk. This creates a confirmation bias."**

Academic research revealed changing compliance patterns, but the underlying factors driving them are not yet clear. Sanctions might influence these patterns, but other elements, such as board changes, could also play a role. To gain insights into future compliance and non-compliance, a deeper understanding of past compliance patterns is essential. By discerning the drivers behind these patterns, we can make informed predictions about potential instances of non-compliance.

## The (in)effectiveness of AML measures

As also mentioned by other scholars and professionals – for instance my good colleague Mike Levi in KPMG Australia's report 'Financial Crime: A Paradigm Shift' – quality of data remains a major handicap in achieving data ambitions. Next to this, the imbalance between the public and private sector needs to change. The government is demanding a lot from the private sector, but we do not know whether the measures they impose are indeed effective (even though we know that they cost a lot of money). Providing feedback is crucial for enhancing effectiveness. The FIU should provide feedback on unusual transaction patterns, enabling gatekeepers to understand why they are doing what they are doing, and how they can improve that. This should not change in ten years, but tomorrow. The problem, however, is the capacity at the FIU.



I also believe that changing the unbalance in capacity even just a bit, can have a major impact. Bank employees could perhaps even contribute to the FIU's investigative work. In return, this hands-on experience will empower bank employees to produce higher quality unusual transaction reports. This cross-collaboration fosters effective PPPs.

AML measures are sometimes presented as a cure to everything. A recent article suggests that AML measures can be used to combat ESG non-compliance. This implies that, for instance, selling clothes linked to child labour, which should or could have been known by performing due diligence activities, can lead to a prosecution for money laundering. I find this approach too far-fetched at this moment, considering the uncertainties about the effectiveness of AML measures.

It is governmental policy, that all crime prevention and intervention should be 'evidence-based' (or at least 'evidence-informed'): based on or informed by sound academic knowledge on the potential effectiveness of the measures and interventions. This should also apply to the effectiveness of AML measures. However, the risk indicators utilised by AML experts, such as those identified in the NRA, are to a large extent not evidence-based. To improve the predictive value of money laundering risk indicators that gatekeepers need to work with – and therefore the evidence base of the whole AML system – a lot more scientific research needs to be done.

## Preparing for 2034

There's room for improvement, although steps forward have been made. Financial institutions should question the regulators as well, like bunq has done by being so brave as to face the regulator in court, arguing that mandatory AML procedures were not effective. Not out of commercial interest, but out of a genuine interest to understand the effectiveness of their AML efforts. This isn't about avoiding compliance, but about a call to action for the government. Currently, gatekeepers are used as guinea pigs, as it is unclear whether the government's AML approach is effective. The government can and should do a better job in ensuring that what it is asking from gatekeepers is worthwhile. Quoting Mike Levi once more: gatekeepers should not be required to spend large sums on activities that have no clear benefit. Moreover, for gatekeepers to enhance their role, they must have an intrinsic motivation to effectively combat crime. This intrinsic motivation is currently lacking.



**To gain insights into future compliance and non-compliance, a deeper understanding of past compliance patterns is essential.”**



# Andrea Wiegman

## Trendwatcher – FIOD

**Andrea Wiegman is trend researcher and foresight expert at FIOD. Andrea identifies future trends by exploring risks and opportunities to prevent financial economic crime. She has developed a social intelligence trend watch tool for financial investigation in PPPs. In her daily work, Andrea dives into trends and rising topics related to (tax) fraud, money laundering, corruption and cybercrime. Andrea is currently conducting PhD research into her methodology in trend research and exploring the future.**

### Personal motivation

As a historian, I have always been interested in changes and trends from the past compared to the present. The world is constantly evolving, and new solutions and innovations keep emerging. When it comes to new ideas, I enjoy delving into history, as past and future are inherently intertwined. In my daily work, I set a vision for the future. I speak with different experts and carefully listen to what's being said between the lines, to what's mentioned, but not extensively discussed. I don't predict the future, I explore the future. My background as historian enables me to look beyond various subjects and understand that everything is interconnected.

In my opinion, our financial crime prevention approach is too fragmented, leading to unnecessary duplication of efforts. The available workforce capacity needs to be reimaged and effectively allocated. Bringing

people from diverse backgrounds together reduces the risk of tunnel vision in financial crime prevention. I want to foster increased cooperation between the public and private sector, and also between different jurisdictions. My main motivation is contributing, through my work, to a greater good, to a safer society.

### The paradigm shift

I anticipate that the paradigm shift will come from new technologies, AI and quantum computing. These new technologies will alter the approach on combatting financial crime entirely. In order to remain future-proof, organisations need to invest in technology, need to be prepared to work with quantum technology and understand how AI works. In a quantum world, one particle can be either A or B, depending on the context or perspective. This is a new and disruptive concept and completely different from the clear data world as we know it at present. Therefore, we need to learn how to deal with information, knowledge and data, as well as with fake information, fake data, fake identities and everything in-between. Quantum computing will provide a technical solution for data sharing, since it will enable us to work with smaller datasets to provide insights. I expect that we will find a solution for current data sharing limitations and inefficiencies, when dealing with anonymised data and smaller sets of data, which could hinder us from obtaining a comprehensive view and drawing conclusive insights. I believe, however, that we need to adapt to working with data limitations.

Our tendency is to draw conclusions only once we have the entire picture, but we need to explore the potential of drawing informed conclusions even when faced with incomplete information.

### Financial crime risk

I think that new risks for financial crime will emerge within the workplace. There is an increasingly diffuse boundary between legal and illegal behaviour as a result of complex and sometimes even conflicting laws and regulations. Loopholes within the law will be exploited by professionals who may display unethical, yet lawful behaviour (i.e. 'awful but lawful'). For me, white collar crime includes crime within all kinds of companies and the digital world. The challenge is to identify when certain activities or products should fall within the scope of supervisory powers. Nowadays a wide range of (non-financial) products and digital assets can be seen as 'money' and used in the money laundering cycle.

Globalisation also contributes to a more diffuse approach to combat financial crime. Globalisation and the speed of sharing information also enable criminals to have more knowledge of ways to launder money or commit other crimes. In addition, due to globalisation, the rise or influence of (new) very rich non-democratic societies is felt on a global scale. Cultural differences also bring about differences in our perception of criminal behaviour and the definition of compliance (e.g. in some parts of the world, bribery is widely accepted as a standard part of doing business). And dirty money will always find its way, also in more democratic countries. Therefore, I strongly believe that increased collaboration among international gatekeepers will become more and more important.

The current way of analysing integrity risks, such as money laundering, primarily focuses

on the identification of risks, sometimes even via a questionnaire. In my view, emphasis should be placed on opportunities to identify new avenues for enhancing the effectiveness of financial crime detection. Questionnaires will not provide detailed insights into trends. If we want to explore new trends, we need to engage in organisation-wide discussions and foster collaboration across departments, and possibly extend cooperation to different institutions. The dynamics of group interactions can give us new insights.



**Our financial crime prevention approach is too fragmented, bringing people from diverse backgrounds together reduces the risk of tunnel vision in financial crime prevention."**

### Regulatory change

AML/CFT laws and regulations should continuously evolve. Yet, I believe there is even more to win by, more specifically, tackling corruption. The numerous subtle forms of corruption pose a challenge, but there is also a significant opportunity, as much wrongdoing originates from corrupt practices.

New laws will be implemented following the impact AI has on society and will introduce new ways how societies interact with each other, as well as opportunities for new forms of criminal behaviour. Sanction laws are continuously changing, without maintaining a clear focus on the laws already implemented. We are lagging behind in re-using valuable elements of these laws before implementing new regulations.



**The complexity that comes with new technologies has to be accepted and we, as a society, need to learn how to work with these complexities.”**

### Data, technology and multi-disciplinary collaboration

As I previously emphasized, data and technology will be major enablers in combatting financial crime. In particular, AI and quantum computing will change the way how financial crime is currently detected and will require a new way of approaching data and information. The introduction of new technologies does not form a risk per se. The real danger arises with the use of these new technologies. For example, the rise of fake identities and fake news generated by AI. The complexity that comes with new technologies has to be accepted and we, as a society, need to learn how to work with these complexities.

I identify the following challenges in the field of financial crime prevention that must be addressed over the next decade:

- Organisational systems are (too) outdated to fully make use of new technologies. Major organisations, both public and private, are stuck within a legacy structure hampering an effective response to new trends.
- Our public institutions (laws, regulations, supervision) are too slow to adapt to the dynamic world we currently live in. Laws and regulations are already outdated by the time they are implemented.
- There is not enough knowledge regarding

the use of new technologies. For example, also with the use of AI, people tend to focus on answers we already know. This behaviour is associated with confirmation bias, a well-recognised tendency in society to overly rely on known information while neglecting the significance of unknown information. We may perceive AI as less reliable when it presents new or unexpected answers, despite the potential added value that such responses may offer.

- Public and private parties operate within a fragmented financial crime prevention landscape, which results in inefficiencies in sharing valuable data and information. The amount of hand-overs in the process results in a loss of information. As an illustration, consider the game of one person whispering a story to another as a way of passing on a narrative. As the story circulates through different individuals, the final person often recounts a different story than the story conveyed by the first person.
- Across public and private parties, there is a clear lack of discussion on long-term strategies in light of emerging technologies.

Every risk brings along an opportunity. I believe that we can overcome these challenges with enhanced, multi-disciplinary collaboration. Effective collaboration is a profession in and of itself, which may even require new forms of leadership.



## Financial crime compliance capabilities

In my opinion, there are different opportunities to enhance financial crime compliance capabilities. First and foremost, I believe we need to work more in multi-disciplinary and dynamic teams. Many changes are coming our way at the same time, such as quantum technology, AI, international crises, geopolitical threats, etc. We are unable to oversee the entire field, which emphasizes the need for increased collaboration. Legal and finance people have led the current compliance efforts, but they are not trained in the dynamics of change. We need to work with people who are not like us, who do not understand us. We need to learn how to trust different approaches to look at a complex issue.

When it comes to new technologies, there is currently an over-reliance on experts with a beta background. Overreliance on experts with the same background creates a risk of tunnel vision. The impact of AI and other new technologies needs to be understood by a wide group of people. I strongly believe that value can be added by also relying on experts with an alpha background, such as storytellers to explain the context behind the technology. It is not about who knows the truth; rather, it is about navigating the unknown.

Detecting emerging trends in financial crime requires an understanding of criminal networks. I believe that crime scripting is an essential tool to understand criminals. Crime scripting places the offence at the forefront and is a step-by-step narrative of the process an offender follows when committing a crime. Again, the process of crime scripting requires multidisciplinary and diverse teams focusing on uncovering unknown aspects rather than seeking confirmation of what is already known.

I emphasise the need for more strategic discussions on the use of new technologies. There is not enough discussion on addressing questions such as 'what's beyond the horizon?'. We need to embrace complexity and learn how to deal with it.



**I strongly believe that value can be added by also relying on experts with an alpha background, such as storytellers to explain the context behind the technology.”**



## How KPMG can help

KPMG leads the way in providing expertise and tools to help set you up for success:

- Support with establishing a policy house
- Monitor and assess the progress and quality of your remediation program
- Support with designing, executing or validating your SIRA
- Regulatory lineage to implement, monitor and demonstrate compliance with significant amounts of legislation
- Develop your FEC strategy and target operating model
- Develop and execute a technology strategy and operating model
- Aid in digitalisation of integrity risk management, AML and sanctions compliance programs
- Implement our global KYC Managed Services solution
- Conduct maturity assessments of your financial crime compliance processes
- Support with measuring and enhancing your organisation's risk culture
- Evaluate regulatory compliance and identify areas for enhancement through quality assurance or internal auditing procedures
- Validate your FEC models
- Act as interim compliance officer
- Support with establishing regulatory-compliant data analysis ecosystems

## Acknowledgements

This report was very much a team effort. We would like to extend our thanks to Kay de Vries, Eric Schneider, Niels Nederpelt, Yael de Vries and Naz Akyüzol.

# Contact

**Leen Groen**

**Partner**

**Risk & Regulatory | Forensic, Integrity and Compliance**

T: +31 20 656 7618 | M +31 6 5393 8480

E: Groen.Leen@kpmg.nl

**Evelyn Bell**

**Director**

**Risk & Regulatory | Forensic, Integrity and Compliance**

T: +31 20 656 4070 | M +31 6 1927 8758

E: Bell.Evelyn@kpmg.nl

**Patrick Özer**

**Partner**

**Risk & Regulatory | Forensic Technology**

T: +31 20 656 8207 | M +31 6 2269 4146

E: Özer.Patrick@kpmg.nl

**Erwin Mol**

**Partner**

**Risk & Regulatory | Governance, Risk & Compliance Services**

T: +31 20 656 7498 | M +31 6 5275 5920

E: Mol.Erwin@kpmg.nl

**Melissa van den Broek**

**Senior manager**

**Risk & Regulatory | Forensic, Integrity and Compliance**

T: +31 10 453 4427 | M +31 6 5714 6541

E: VandenBroek.Melissa@kpmg.nl

**Jori van Schijndel**

**Senior manager**

**Risk & Regulatory | Forensic Technology**

T: +31 20 656 8563 | M +31 6 5314 8020

E: VanSchijndel.Jori@kpmg.nl

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



The information contained in this document is of a general nature and is not intended to address the circumstances or needs of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. Some or all the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

© 2024 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.