# SUMMARY
# LEADERS IN FINANCE AML EVENT 2024


**WRITTEN BY: DIJANA NURKIĆ, SENIOR CDD/KYC SPECIALIST**

**REVIEWED BY: MAARTEN BOLK, COO, LEADERS IN FINANCE EVENTS**

On the 3rd of October, the fourth edition of the Leaders in Finance AML Netherlands Event was held. An event that connects professionals from the AML ecosystem with each other. More than 70 organisations were represented and both national and international participants and speakers were present. These financial crime fighters came together at Fort Voordorp, in order to learn, share knowledge, network and to form or deepen relationships between different players within the AML domain.

In the previous editions, almost every stakeholder within the domain was represented. However, previous editions did not have the Dutch Data Protection Authority or a convicted professional enabler of financial crime. This edition had, along with the 'regular' stakeholders, both! The event had different keynotes and Q&A's, a banking panel and different Ask Me Anything sessions. The common thread during this event was looking to the future, collaboration, good data, data sharing, and AI.

## Opening

### Irene Rompa, Moderator

In her opening words moderator Irene Rompa mentioned that she reached out to some of the participants of the event in order to determine what is top of mind in this community right now. One of the things that kept coming up in the conversations was the joined anti-money laundering initiative Transaction Monitoring NL (TMNL) being dismantled, because it conflicts with European legislation. Another hot topic was the sentencing of the former CEO of Swedbank (Bonnesen). She was sentenced to 15 months in prison over her handling of anti-money laundering protocols. Others who are working at financial institutions are preparing for the new European Anti-Money Laundering Autority (AMLA) that will begin operations in 2027. Then, the new Anti-Money Laundering Regulation (AMLR) will also come into effect. Yet another topic is last week's news about the House of Representative in the Netherlands approving a bill to ban cash payments above €3000. In general, all the conversations Irene had mentioned how methods of money laundering and terrorist financing are constantly evolving and how new technologies are making things more complex.

## Keynote and Q&A

### Philippe Vollot, Managing Board Member & Chief Financial Economic Crime Officer, Rabobank

Philippe first wanted to talk about a couple of things that are close to his heart. One of those things is a public-private partnership. He says that it's important for him to be careful how to define a public-private partnership. In some countries he has seen meetings between effective regulators, banking associations, financial institutions and law enforcement. During the meeting all parties agree that they should be better at fighting financial crime and afterwards they agree to meet each other in two months. But unfortunately, nothing happens. In some other countries, Philippe has seen the beginning of a real public-private partnership that's really effective. The different actors have a common view of how to fight financial crime and they are going to start to try finding ways to effectively share information.

According to Philippe, this is the future. We need to think about the entire value-chain of fighting financial crime. You can have a bank with thousands of people working in this field and with the right systems and controls implemented, but if the FIU does not have enough capacity to look at all these alerts and to move them to skilled police officers who in turn move this to prosecutors to prosecute the criminal, then your ultimate goal is not reached. Philippe was quite pleased with the recent statement of the Dutch Cabinet. It was about effectivity, public-private partnership and that

they are going to try to push the capacity of key actors to share information and patterns. He was also pleased with the statement, because it gives hope for reducing the drug production problem in the Netherlands. But we need to make sure that the partnership will have tangible results in time of prosecution.

Another topic Philippe wanted to talk about is TMNL. It's quite devastating according to Philippe, that TMNL got dismantled. When Philippe started his current job at the Rabobank, he was enthusiastic to be in the Netherlands and he thought this country was well advanced in having the TMNL solution. Philippe said that TMNL does work. He has seen it work. We are allowed to share some data about high risk clients, but Philippe says that this might not be of a lot of use, because a professional money launderer won't be flagged as a high risk in the bank systems. The very talented money launderers, will come in as low risk clients. What TMNL  has shown in terms of working, is that for the low risk clients who are under the radar, it has generated certain alerts. They had several cases of a very small company running a perfectly acceptable business, a small cash deposit every month and everything lined up with the activity of the business. However, TMNL picked up that there was some activity at other banks and it generated an alert. Which Philippe believes would be useful for the FIU. It's sad according to Philippe and he was even in Brussels to plea about the importance of TMNL and that the data is anonymised, but he crashed into the wall of data privacy. The data privacy took over the debate compared to financial crime.

The third topic is really one that is popular in the Netherlands: unusual transaction versus suspicious transactions. Philippe believes we should move to suspicious transactions, which is what this country will do. He does believe that the FIU in this country is doing a great job, but at the same time the FIU in this country got 2 million unusual transactions in 2022, while the FIU in France got 160.000 transactions being reported and Germany got 230.000. Philippe wants to be effective and he politely disagrees with people who state that we need to report the unusual transactions. In order to be more effective, he will have to be better in his job, he needs his analysts to do a better job. It's not that he needs more people, but better people. It's also about improving the effectiveness of the whole system. And that is possible, because we in the Netherlands have a regulator that is sophisticated. He feels that they speak the same language when it comes to TM, CDD, etc. He has a lot op hope for the Netherlands. It's too bad TMNL crashed, but we have sophisticated regulators, FIU tries to do well and all stakeholders within this domain try to be effective. With the new Cabinet's statement there is hope that it will become more effective and the bad guys will be actually put in jail.

The fourth point is something that is not talked about often. It's communication with customers. Philippe says that the bank is not a law enforcement agency, but a bank, which is a profitable organisation. The bank wants to do business with it's customers and also prevent criminals to

launder money or misuse the financial system. We need not forget that 99% of the customers are good customers. Sometimes we forget to explain to them properly why we're doing things. There will always be customers who will complain or find the process difficult, but banks have a duty to society and to fight financial crime. It's about how you do this and how you explain it to the customers. Explain to them that we want to protect them.

Philippe often gets asked what he thinks about remediation and what can make remediation fail or be successful. Philippe has a lot of experience with remediation. The first rule, according to him is to surround yourself with people smarter than you. If you don't have the talent, then don't even think about remediating the bank. The second rule is not to focus on a lot of things at the same time. Focus on the two or three things that are making the regulators extremely unhappy and where tangible progress can made be upon. Showing tangible progress is important for the stakeholders. Another rule is to get the budget. It's important to fight for the money. Money can bring in big talents and you need to pay people to do a great job for you. You need to have your management understanding that it is going to cost a lot of money and then after that by levering technology it will reduce the costs of the business as usual. Last but not least, focus on quality. Do this during the remediation, but also after the remediation is done. The first thing that Philippe did at Rabobank when he joined after he brought a talented team in, is to focus on quality. He looked at the first line monitoring and KPI's and saw that they weren't good. There was not even a point to start if the bank doesn't have the right process to assess the quality of what the analysts do. Are alerts properly reviewed? Is the classification (low, medium, high) good enough? So that was the first thing he did, setting up a team to have proper quality assessment. The second thing he did was the SIRA process. He looked at what he wanted to actually achieve. He wants to understand the financial risk exposure of the bank. What is the intrinsic risk, what are the mitigation actions, what is the residual risk? So they first solved the SIRA process. It is important to keep in mind to be decisive, to keep things simple and to have discipline.

Philippe has worked in a lot of countries. The thing that most surprised him about the CDD ecosystem when he came to work in the Netherlands was the filing of unusual transactions. That was really different than what he has heard in the rest of Europe. Another thing that surprised him was that top bankers in this country were under criminal investigation. There is no board member who is willingly trying to do money laundering. In holding board members responsible, you're actually creating some fear in people. So every complex situation will be pushed into a committee, because people are afraid to make a mistake and to be held responsible. People were concerned in terms of liability. It kind of created a trauma under professionals. They reduced now, two years later, 70% of the cases going to a committee. According to Philippe, banks have responsibility and banks should be sanctioned when they don't do what has to ben done, but he would rather see more money launders in newspapers than bankers.

One question from the audience is where we could get the data we need for our work from, keeping all those restrictions and privacy around data in mind. Philippe says your data needs to be in order. You can have all the tools and AI in place, but if you're not looking at the correct data you will get nowhere. He says that we need to keep open minded. There was a statement from the Cabinet that they are trying to find ways for financial institutions to share data. In other countries Philippe has also seen that in a public-private partnership law enforcement has shared patterns with the bank. No sharing of names, of course. But in another country law enforcement gives the bank a call and says to check a Swift payment between country X and country Z, after time Y. It was really precise. So sharing patterns could be the way forward.

Criminals are quicker than us. They of course have no budget constrains or supervisory board. So we have to be as pro-active as we can to identify a potential threat and effectively using the new technologies and the new regulatory framework to our advantage. When Philippe just arrived at Rabobank, he said he had no interest in AI. That was because the foundation of the FEC domain there was not in order. He first needed to get the right people and the right processes, because it would be ineffective to plug AI on something that isn't clean. Later on, of course, AI and machine learning came more into play and six months ago he and the management team even created an innovation lab. Philippe has a lot of hope in the new technology. He states that he is not reducing costs by doing this, he is reducing the operational risk by effectively having less reliance on the analyst and more on the system. So Rabobank is using it more as guiding and helping the analyst to focus more on the key risk.

Philippe is now at the middle of his management board mandate. What he wants to achieve in the remainder of his mandate, is operational effectiveness. Closing the remediation programme internally, validating what they did and having DNB be happy with what Rabobank did. He wants to move to business as usual and adding a sustainable process. Agile enough to integrate new regulatory requirements and keeping the quality. After remediation, keep fighting for the budget. Because you need to implement that sustainability and optimalisation. Senior management needs to understand what the risks are of reducing the budget. Compliance is good for business. What is wrong if a bank knows perfectly well who their customer is? If you know your customer well, you can send them the right product, at the right time, in the right way. There is nothing wrong with that and financial crime should not be isolated from the overall banking value chain. You need to get information effectively about the client for business reasons, for financial crime reasons and for sustainability reasons. Reducing the budget immensely will lead your key people to leave and your quality to deteriorate. You need money to do proper compliance and compliance is good for the business.

## Banking panel

- **Robin de Jongh, Global Head of Client Due Diligence, Rabobank**
- **Karim Tadjer, Global Head Financial Crime and Fraud Prevention, ING**
- **Helène Erftemeijer, Sector Coordinator AML/CFT & Subversive Crime, NVB**
- **Jeffrey Voors, Global Head of AML, CFT & Sanctions, ABN AMRO Bank N.V.**
- **Karin de Jong, Partner, Head of Forensic & Financial Crime NL, Deloitte**

During the session the panellists were looking ahead to the AMLA, AMLR, Article 75 and the importance of regulatory relations. It's going to be a new field on the European level. In the summer of 2025 the AMLA will take seat in Frankfurt, there will be a European single rulebook, a directive is coming and harmonisation is going on. Can we keep track? There is also some worry in the market. The risk-based approach has been evolving in the last couple of years in the Netherlands. But does the new AMLA mean that we are back to square one?

The panellists agree that we are not going back to square one. There are still a lot of things to analyse and to understand. The regulation that has been put out can be read, but there are still many questions about what is exactly meant. That will be worked out in the regulatory technical standards. This will be done by the AMLA, but the AMLA is still not here. In Frankfurt there will be something set up in 2025 with 400 people, but who are those people? Are they only coming from supervisors? There is still much unknown. However, we need to take this (AMLA) as an opportunity and a way forward, not as a step back. The intent of the AMLA is a good one and it is to accelerate fighting financial crime and to accelerate partnerships and cooperation. As an industry, we need to work together to find a way to set the tone.

According to the panellists we can and should contribute in how to operationalise this. There are however also a few worries when talking about a rulebook and us wanting to work risk-based. There is risk-based room in AMLR, but it's not easy to get from rule to risk-based. And if we do the work risk-based, we need risk-based supervision. Otherwise, it's not going to work. How are we going to get there? The new AMLR will come in a few years, but if we need to comply with the changes that we see in the AMLR (like adding additional data points), there might not be enough time to do so. There needs to be clarity on some things, but some of the regulatory technical guidance is not planned until 2026. So what can we do now? We can look at our policies and procedures and look for gaps between what's there at this moment and what needs to be there with the new AMLR. There still needs to be a lot of adjustment to systems, data and the management of our data. That's a lot of work and it can't wait. We know the basics of what needs to be done and we can do that now in order to prepare for the AMLR.

Harmonisation across Europe is important. Each country will have their own views and standards that they bring to the table. We have to be careful that we don't end up stacking all the good things different countries bring, because we will end up with a whole stack of requirements. So basically, it should be done as a risk-based approach. Overall the panellist agree that it's quality over quantity. Because resources are deplete, we might want to allocate our resources to the higher risks and dare to dial down on the low risks. The panellists state that they do see (within their banks) that this shift is already happening and that one of the elements why this shift is occurring, is because they don't want to treat all their customers as criminals. When it comes to harmonisation (when AMLA has taken seat), regulators should also have an understanding of the diverse market of the European countries and an understanding of some of the localities. The first couple of years there needs to be an understanding  from the regulators of what's happening in the markets. AMLA should not be fully centrally lead from the first day on, but slowly more and more in harmonisation. So it would be good to have a diverse AMLA staff.

Article 75 is probably the most mentioned article from the AMLR. An important element in that article is the high-risk definition and what it actually is. If you know something as being high risk, then there is no use going further into that. You should get things on the table you don't know. So the hiding lower risk. So it would be good to know what law-enforcement and prosecutors see as higher risk. It's not just the gatekeepers who know what is higher risk in the Netherlands.

Moving from unusual to suspicious transactions can make the industry stronger. It will have quite some impact on our work, because we have been working in the current way (reporting unusual transactions) for a relatively long time. So we will need some time to learn and accommodate. By looking at suspicious transactions instead of unusual transactions, some unnecessary outreach might be prevented. Moving to suspicious transaction will bring more responsibility to the bank. Filing unusual transactions is based on an analysis, but filing suspicious transactions is based on an investigation. What also makes it a bit more difficult, is that there is no free sharing of information in Europe and so determining what is suspicious might be harder (than in the US, where there is almost free sharing of information). If we move to filing suspicious transactions, we need better analyses, better systems and better people. So there is some work that has to be done, but ultimately it will increase the effectivity within the chain. One thing that might happen when we go from filing unusual transactions to suspicious transactions is that society might expect that banks will only ask questions when transactions are suspicious. So people might think that they will not get questions anymore about source of wealth etc. It's interesting to see how different the facts are if we move from unusual to suspicious transactions.

In preparation of the new AMLR, the NVB and the banks have done an analysis together on what CDD, monitoring and reporting requirements are in the AMLR and they have compared that to what is currently in the Wwft. They looked if there is a difference and if so, how impactful that difference will be. They've also had a discussion with the Ministry of Finance and the supervisor about the main concerns and on where the unclarities are.

Steffie Schwillens of the DNB says that she hopes that we trust that regulators are not purposely trying to make life difficult or ineffective. That's not what they are trying to do and it's also not want AMLA is trying to do. She thinks we all need to work together to see what is necessary to take us to the next level and that AMLA will take us to the next level. It might be with some setbacks, but large institutions (like the banks) know how to deal with that. Try to be smart. Steffie understands the worries and concerns, but she feels we have to act from confidence and guts. We need to be smart and work together with other countries that might be more influential. We came a long way the last couple of years and she has seen the discussion changing in those years. She hopes that they as a supervisor have been able to fulfil a useful role in the whole process. She thinks we should continue from confidence. If you tell a good story and you have your house in order, you can sit down with regulators and talk to them.

## Ask Me Anything - Risks and Opportunities of GenAi in AML

- **Steffie Schwillens, Head of Financial Crime Supervision focused on the banking sector, DNB**
- **Johannes Lont, Senior Manager Financial Crime, Zanders**

Before interviewing Steffie, Johannes first gave a short presentation about GenAI and the potential and risks of GenAI within AML and financial economic crime. We all talk about GenAI, but it's good to set the scene of what GenAI really is. GenAI is about content generation. This content can be text, image, audio or video. GenAI is also about machine learning. The third important item about GenAI is the interactive capability. A popular example of that is ChatGPT.

So why is GenAI relevant for FEC and AML? Well, look at the three items just discussed in this text. Content generation (as in generating a summary or report) is matching with FEC, because the FEC domain is text heavy. Secondly, FEC is really labour intensive and if you can make use of machines, it makes the work less intensive. The third thing is that the work is quite complex. If you really want to prevent financial economic crime, you have to be smart, there are a lot of policies, it's complex work – so the interactive capabilities of GenAI might help out and make things a bit easier. So GenAI can help by making summaries, assist with a search on policy documents, generate automatic reports and act as customer service bots that answer the questions of

customers (and explain to them why we are asking certain questions).
Of course there are also risks involved with the use of GenAI. One of them is biased responses. That's harmful content or content that's not in line with the regulatory point of view. What can we do about this? We need to make sure that the thing we ask to the chatbot and also the outcome are well managed and only presented if it's within the right boundaries. Another risk is hallucinations. Maybe you have experienced this while working with ChatGPT. Sometimes things are generated that are absolutely not true. So make sure that the grounding is correct. This means that the data needs to be sound. We as professionals in the AML domain need to think about how we manage GenAI, the opportunities and risks. Criminals can also employ GenAI.

- Steffie says that the Dutch Central Bank (DNB) also makes use of GenAI and that she thinks that for a supervisor, they are pretty far advanced. They are experimenting a lot with GenAI and type of solutions. Like every organisation, they have to deal with security issues and privacy and that's why they tend to be a bit careful with the use of GenAI. However, they are piloting Copilot. They have also build a ChatDNB tool. In comparison to ChatGPT, the ChatDNB is really basic. Within their work they also have to deal with really lengthy regulations and Steffie says that Copilot can help with that.

- GenAI has different potential gains. Steffie thinks that the whole AML field is looking for efficiency gains. Some things banks are doing now (during the remediation) are not sustainable for the future. So things need to be done in a more efficient manner. That doesn't always mean that it's going to cost less, but you might use less people and more time of your people to do the complicated stuff (i.e. real risk-assessments). GenAI might help translate outcomes to basic client files. In order for this to work, we have to keep thinking (and keep the risk of hallucinations in mind) and not get lazy. Otherwise you might get dangerous outcomes.

- We are in a GenAI phase where we can get different responses to the same question. Steffie uses the question (in a chatbot) 'Is this answer correct?' to check. Sometimes the chatbot says that the answer is not correct and it then gives a different answer. Analysts need to be trained how to deal with these tools in a mature manner. The professionals in the AML field are dealing with important stuff and they need to be audible. In the end, an analyst needs to reconcile why he/she came to a conclusion. One can't just simply copy and paste the first outcome a chatbot gives (without checking it) and go on to the next question. So this awareness needs to be created and analysts need to be trained in using and dealing with these chatbots.

- What does Steffie think are the most important characteristics in terms of leadership to make it through this next phase in AML? She thinks one of those characteristics is having guts. GenAI doesn't have guts. It only puts out information it has picked up somewhere. Leaders need to

have guts and confidence, in order to make choices. GenAI can help us do more in less time and analyse big amounts of data, but we always have to remain making choices. That's why you need leadership. Leaders need to steer the group and decide what the biggest risks are, what the focus should be on and what not to focus on. Another characteristic is that leaders should also learn from their mistakes. Mistakes are going to happen, either with GenAI or without GenAI. The industry and the supervisors need to accept that and also build on those mistakes. Never waste a good crisis.

- There will be some changes in the regulatory landscape when it comes to AI, because of the AI Act. There is still unclarity about how the supervision will be done. Steffie is relatively happy that Europe is way ahead with the AI Act. Europe can be an example for other continents. Supervisors will also have to learn a lot on this topic, together with the sector. Supervisors will also make mistakes and adjustments are needed. It's a balancing act. The sector also needs to have guts and tell the supervisors when they are not right and the sector needs to challenge the supervisor. That will create a conversation, which will become more and more important.

## Ask Me Anything - Developments in AML Screening and Monitoring

- **Robert van Haersma Buma, Lead Business Development Payments, Digital Identity Services & Open Banking, Rabobank**
- **Krik Gunning, Co-founder & CEO, Fourthline**

Fourthline is a regulated KYC FinTech that offers one solution that helps companies be compliant on the one hand and to fight financial crime on the other. In June of this year, Rabobank and Fourthline entered a partnership. One of the main themes Rabobank and Fourthline touched upon when they started their partnership, was trust.

- With the help of GenAI financial institutions are aligning more with the expectations of regulators. Most banks in Europe have upped their game when it comes to being a gatekeeper, especially with the onboarding of new clients. One thing regulators are more and more asking for, is knowing/checking not only who the account holder is, but also who the account user is. With GenAI, these things can be found out. It is important to have an audit trail. A lot of banks historically have relied on tools like Face-ID on your phone. But those tools don't give you an audit trail. European regulators are increasingly asking financial institutions to make sure that they can proof with an audit trail that it was really the account holder that was using the account.

- It's great to fight financial crime, but that's only a small percentage of the existing clients a bank has. With new clients, it's also only going to be a small percentage (doing financial crime). Should we also think about the approximately 98% of bona fide clients who also have to go through the KYC process and educate them on why we're doing it? Of course it's because banks want to comply with the requirements of the regulators, but what should be more important is to allow the end-customers to basically learn self-defence. Banks can present a client with the tools and establish a ground truth of who the client is (like biometrics and where the client resides) and what a normal transaction pattern is. That means that banks can also give a client the weapons to prevent their identity being abused, their account being accessed or their savings being stolen. That's according to Krik what it should be about: guiding your users how to retain trust.

- A lot of financial institutions underestimate the value that they created with the massive investments over the past years. The four largest banks of the Netherlands spent 1.1 million on KYC and they have told the DNB that it's not sustainable. However, the technology and the knowledge that's being brought up is relevant in a ton of other sectors as well. Financial crime is not just about the drug criminals trying to launder the money, but it's also about other types of financial crime that effect other sectors. The technology and experience that the banks have gained, can be extremely helpful for other variables and companies.

- Trust is one of the largest assets for Rabobank. Trust has been build (traditionally) between Rabobank and the customers by conversing processes to adhere to KYC/AML requirements. Regardless the hassle, the intent of these processes is to establish a high level of trust. Trust between the bank and the customers. And trust between Rabobank and the regulator. Rabobank wants to minimise the 'hassle' around this, but still maintain the high level of detail and trust. A lot of energy and time has been put into optimizing and automizing the processes and Rabobank saw that customers also have a similar need. That's why Rabobank made the Rabo Identity Services available for customers as of 2015. It's a service that makes digital identification, verification and onboarding journeys available for customers and it has the level of trust that is expected from a large bank. However, ease of use is also becoming more relevant for customers. Rabobank thinks that collaboration and cooperation is necessary to bring customers the best products. By combining the bank's extensive experience in the field and the technology that a company as Fourthline provides, Rabobank enables the customers to optimize their digital onboarding journeys with trust, ease of use and flexibility, while at the same time fraud and crime is prevented.

- According to Krik it's time for a bit of optimism. There is more that financial institutions can do with everything that has already been done within the organisations. In terms of technology and

in terms of the track record and experience they already have. He encourages the audience in the room to use it for the broader society, not just the financial system. Robert believes that being successful in this field requires to get the data in a way that is easy for the customers.

## Speech

### ▸ Marnix Enthoven, Senior inspector system supervision, Dutch Data Protection Authority

The DPA is the independent regulator in the Netherlands that monitors our fundamental right of protection of personal data. Financial institutions need to safeguard the financial sector, but also safeguard the data of their customers. It can be difficult to balance data protection and AML efforts. Information is power and financial institutions have a great deal of information, so they have power over people. Data protection legislation has the aim to empower people. The GDPR aims to do this by setting a framework of principles that organisations have to adhere to. You have to ensure lawful, fair and transparent processing of the data. The data has to be accurate and just the minimum amount of data that is needed has to be collected. Institutions also need to ensure that the data is properly secured. Also, financial institutions need to be accountable to the people what they are doing. To help people make sure that organisations collecting their data actually do this, there are some individual rights granted to people.

Privacy and data protection are recognised globally as a fundamental right. The GDPR is an expansion of that. The GDPR places stringent obligations on financial institutions. That's because financial data is such a sensitive category. Transaction history can reveal a great deal about you, for example where you live, where you travel, your medical history and what your political affiliations are. Data protection laws give individuals more control over their personal data. These laws obviously exist because misuse or mishandling of data can have serious consequences (like identity theft or discrimination).

Most financial crime fighters hear about (or even see) the extremes of crime in their field (like human trafficking or prevention of terrorist attacks) and this might give them a certain view of the population they are dealing with. Luckily, as also mentioned a view times in the previous sessions during this day, the vast majority of the customers are no criminals and they also have no criminal intent at all. Recently, the NVB started a campaign to raise more awareness on fraud. Some people don't know they are doing 'bad' things and people also sometimes unknowingly make mistakes. There are a couple of examples in the Netherlands in which the latter group has been harshly treated because of that. Marnix suggests to look into those examples and what went wrong, to learn from it, because you should always presume innocence. The customers are probably not the next Al Capone and that's why they should also not be treated like that.

The DPA does understand that financial institutions are increasingly tasked with ensuring compliance both with AML legislation and data protection legislation. This might compose a challenge. The AML regime is filled with frameworks from the FATF and over the last thirty years of AML legislation, data protection and privacy have not been on the forefront of those recommendations. This is problematic according to Marnix.

DPA is still assessing the changes of the new AML package, but they have already seen that data protection has a more central role. One of the key elements from the new AML regulation is the data sharing partnership. The DPA and other European counterparts/European data protection boards have had strong opinions about the new rules regarding the broad sharing of data. The new AML package has to live up to the standards and has to be interpreted accordingly. For the partnership in data sharing it is important that the partners commit to the data protection principles. The obliged data protection impact assessments that have to be done, have to be up to date every time and be thorough.

This is only applicable when it comes to personal data. Marnix thinks that a lot of the partnerships that will evolve, don't need to have personal data, but can go of the information about (for example) modus operandi. When personal data is processed, the GDPR is applicable and all the previous mentioned principles (like fair and transparent processing) need to be ensured. The roles and responsibilities of all the partners in the partnership should be well established and communicated to the outside world. So for example, which party is controller?

The current system of a lot of formal or informal partnerships is not transparent enough. The sharing of data in partnerships must lead to fair outcomes. A fair processing means that it may not lead to unfair outcomes. A few reports earlier this year from the DNB, NVB and the Ministry of Finance as well as some judgments from the Human Rights College have posed significant problems with regard to direct and indirect (and perceived) discrimination. That was for individual organisation. Marnix thinks that these risks are multiplied in partnerships. A partnership should have all the technical organisational measures in place to prevent, detect and mitigate discrimination and other violations of human rights violations. Especially when AI systems are used.

Once personal data has been collected for AML purposes, it should not be reused for other purposes, like marketing. This otherwise violates the GDPR, unless explicit consent is given. The data received through a partnership may only be used for the purposes of the partnership. The GDPR grants an individual the rights to know what data is being collected about them and how it's being used. However, AML laws sometimes grant confidentiality, especially when it comes to

suspicious activity reports. This creates a potential conflict between the transparency obligation of the GDPR and the AML confidentiality rule. The DPA is under the impression that financial institutions now are applying these confidentiality rules too strictly. People must need to know why they are treated the way they are. The challenge is to find a way to balance these two legal frameworks in a manner that ensures the effectiveness of the AML efforts and that respects the individual rights and freedoms. In Marnix' opinion, this is not impossible to achieve. Financial institutions must ensure that they have the appropriate and technical organisational measures in place to protect the data they collect.

Encryption, anonymisation and other security measures are essential in reducing risks. We must ask ourselves the question: what is effective? What is proportionate and what is necessary? Are there less intrusive means possible? Do we have fair and transparent outcomes? As it seems, the interplay between AML and data protection is delicate. Financial institutions have big tasks on their hands with this. Lastly, Marnix states that it sometimes might seem to conflict and that there are clear boundaries, but it's not possible to achieve. The DPA will try to take a more proactive approach (when it comes to the new AML package) within the AML field in the next couple of years.

## Ask me anything - Upskilling the AML professional

### ▸ Annee Spijkervet, VP of Financial Services & Tech, Lepaya

Annee states that there is a lot of change happening in the finance industry. When there is a lot of change, whether it's tech change or change because of market needs, people tend to feel uncertainty. The result of feeling uncertain, is disengagement with the job or feeling unsafe about the job. As leaders it is important to guide teams through the change. A soft skill that might help with this, is feedback. It's important to provide feedback to people, to make sure that they are resilient and that you help them navigate through these changes. Take for instance the increase of AI. AI might help people reduce the level of operations that they are running, but it also means that people might need to be upskilled to other roles in the organisation. The nature of the role that people are doing today, will change. Soft skills play an important role in this.

There is urgency in upskilling people in the AML field. That's because a lot of people are being hired/working in the AML space. All the things that have to be done in order to comply with what the regulators are asking for means that you need to have skilled people. New workers in this field need to be onboarding as quickly as possible and leaders should help them with this by giving feedback, coaching and transferring certain knowledge to them. In finance (and especially AML) so many things are rapidly happening.

Annee thinks that there are certain traits that are important for leaders and employees in this field to develop. Critical decision making is one of them. AI and other tools can help us to reduce the operational workload, but there still needs to be a person to decide whether something is a suspicious case or not. Analytical thinking is another important trait. Communication skills/ storytelling are/is also important. You need to get your message across and you also don't want to get a bad reputation because you said something that you didn't want to say.

How to make sure you can make a behavioural change when you have been to a workshop or training? One way is to practice with what you have learned multiple times, so it's integrated in your daily job. It requires a muscle-brain memory. Practice makes perfect. This is also the case for soft skills. You can use technology to give a push and make sure that you practice the learned thing a couple of times. This should go together with reflecting on how did it go and what you are going to do different next time. But you could also make an agreement with your colleague. Your colleague will remind you to keep practicing the new skill. If you're a leader, make sure that if you provide your employees with a training, to also have certain accountability partners across the organisation to remind your people of integrating the skills. Make sure that you as a leader are part of their developmental journey.

Development tends to play a role in people hopping around jobs (job hopping). People tend to look for other opportunities if they don't feel or don't see there is an actual progression that they have within their role. As a leader you need to stretch people in their current role. So you need to challenge them to grow beyond what they're currently doing in their role. It's not that people are impatient, they're just eager to learn. And that's why they hop around. Sometimes leaders don't do enough to address that appetite.

When it comes to upskilling in the soft skills area, you need to have a foundation of certain skills. When it comes to more specific jobs, those require more specific skills. For analytical skills, there is a foundation needed. Once you grow in a more analytical job, you do need more specialised skills to excel within the job. With the support of technology, people might become more specialised, because other tasks will be taken over by AI.

AI is reshaping the financial industry. Leaders need certain skills to stay ahead of that transformation. One of those skills is agility, because of all the changes that are happening. Leaders should also be good at prioritizing. Thirty years ago people had an interaction with a 100-150 different people in a professional setting throughout a year. That has now tripled. The number of interactions has grown massively. This in turn means that you need to have different skills to interact with all these different people to get your message across. So you need to be much stronger in your communication skills.

Nowadays, people are so busy with their jobs, how does a learning environment be fostered then? Annee states that as a leader, you need to lead by example. What you see from research is that people don't get promoted because they are the best at their job, they get promoted because they display the skills that stand out. In business you need certain skills if you want to perform or over-perform yourself. As a leader you also need to motivate your people to invest in those skills. Those skills are transferable. A lot of people have been hired within the AML domain. What happens to those people when in a few years less analysts are needed? With those skills, the people can be staffed in another job. So it's good to invest in people and their skills.

Despite everything that is happening, human intelligence will be very important to guide yourself, your team and your organisation through change. A lot of guts are needed for the future and people might have some uncertainty. But there will always be uncertainty. So let's make sure to upskill people to face this uncertainty and to do what is needed to create impact.

## Keynote and Q&A

### ▸ Jonathan Gilbert PhD, Financial Crime Consultant & Lecturer in Law, University of the West of England

Jonathan Gilbert went from working at a UK law firm to being sentenced to twelve years in prison for his role in a multi-million-pound mortgage and bank fraud conspiracy. The trial judge stated that his breach of trust was as bad as it could get. During his six years in prison Jonathan turned to education. For himself and for other prisoners. He tutored fellow prisoners, he obtained a Master's degree in Counter-Fraud and Counter-Corruption Studies and has earned his PhD. Now he is the Global Head of Learning & Development at IN8 and he's a lecturer at the University of the West of England. Jonathan also uses his experience and what he went through for the good, by giving financial institutions insight into the facilitation role of key professional agents in property related financial crime. During his keynote Jonathan explains how he went from turning a blind eye from what his client was doing to being actively complicit in the offending.

- A professional enabler is someone who intentionally uses their professional status, knowledge and know-how to manipulate an otherwise legitimate transactional process of activity that facilitates financial crime on behalf of their clients and/or other connected parties.

- The convenient definition of mortgage fraud is the obtaining of mortgage advances on properties by making fraudulent statements.

In 1999 and 2000, initially everything was fine. He had a good portfolio, his practice was squeaky-clean at that time and someone from his network referred pilot Mark Entwistle to Jonathan. Jonathan and Entwistle became friends as well as business acquaintances. Entwistle had some properties and wanted to use Jonathan to obtain more. The partner's from his firm were actually really impressed that Jonathan gained Entwistle as a client.

Initially it was fine, but Entwistle was testing his luck a bit. There was one property they were trying to purchase and Entwistle called Jonathan and asked him to fax someone that they have 100.000 in the client account. Jonathan said that they don't have that, but Entwistle stated that if they do get the property, they can turn it into three or four apartments and that it's a good opportunity for them. Jonathan went through with it. More dishonesty developed over time and Entwistle kept pushing and pushing. Everything got bigger and bigger and they took out multiple bogus mortgages on strangers' homes. So Jonathan went from turning a blind eye to what Entwistle was doing to active complicity. What he and Entwistle and some others were doing, was fraud-for-profit. That is (according to the FBI) the misuse of the mortgage lending process to steal cash and equity from lenders or homeowners. Initially they took the mortgage advances to get big, so they were the biggest property developers in the South of England. As time went by, Entwistle took that money for himself and he also had some gambling problems. The money wasn't going into the business model and that's why everything came crashing down.

Judge Beddoe indicated that Jonathan's breach of trust was really bad and that Entwistle could have achieved almost nothing of what he did without Jonathan's active complicity. And that's correct, because Jonathan was that gatekeeper. A typical mortgage fraud involves multiple professional enablers. You have the broker, maybe even the estate-agent. Then you got the mortgage broker who falsifies bank statements or inflates the income. You may have an accountant who can make accountants to show that the applicant is worth more. A valuer can also be involved. A complicit valuer can uplift your property in value, so you get more money of the banks. Lastly, you have the solicitor at the end. That was Jonathan. He was that gatekeeper. Entwistle and Jonathan both got fourteen years, which is the maximum you can get in the UK for fraud. Jonathan pleaded guilty, so two years were taken off of his sentence. The broker had five years and the accountant had three years. Entwistle's best friend was acquitted, because they used him as a straw person when Entwistle's credit started to run dry. The bank manager from the Royal Bank of Scotland was acquitted on a bribery charge.

In 2009 everything came crashing down. The financial crisis expedited that, because there was no money in the system anymore and they had a huge debt pile. Straight away, the civil lawyers were all over them. They shut everything down and Jonathan was also bankrupted. The following year, the police came to his door. For Jonathan, this was actually a relieve. He knew that is was

coming. He was on bail for four years. The trial started in 2014. He went to jail that year and came out in 2020 (so he eventually served six years). Today he still has to deal with the probation officer/ probation services. As a matter of fact, he had to ask permission to the probation services to attend the Leaders in Finance AML Event.

Jonathan was hit with the civil lawyers, the regulators, the bankruptcy and being called a criminal. There was also the collateral damage, like public shaming. He has children and a wife. This all had an impact on his wife and family. It's also the impact and the breach of trust with his colleagues, his partners and his staff. Jonathan is living with that guilt and shame. And also there is the post-conviction. He is still under the control of the probation service. It has been really impactful and it will affect him for his entire life. So why did he do it then?

The key variables are opportunity, distal pressures, rationalisation and workplace socialisation. Jonathan worked at a smaller practice where he was tasked with getting the work in, like a hunter and gatherer. From the beginning there was not a lot of control. Throughout the years Jonathan felt there was some ethical slippage, where he was turning a blind eye to certain things. There was a workplace socialisation. He thinks that if he went to a bigger firm were there is a proper supervision, oversight and management that he would not have gone so far with it and not had the opportunity to do so. That's why compliance and oversight is so important. Jonathan had experience and he knew the system. He knew that he could complete a mortgage and that banks would maybe come after six months and ask were their security is. Jonathan hoped that by that time it would pay off from something bigger down the road. He thought he could play the system. He was also in charge of his own office, so if a letter from the bank came in, it would come to him and not anyone else. So there was a lack of supervision. And at that time the regulators were reactive and not pro-active like today.

Mortgage fraud is easy in a market where there is lots of mortgage and lots of competition between lenders and a lot of due diligence is missed. Jonathan tried to rationalise everything away and used denial tactics on himself, like 'it will be repaid when the new apartments are sold, we're just taking the profit now.'

Then there was also the pressure that got to him. The so-called Boom strain. The client has fraudulent intent to expand their property portfolio. This strain is transferred to the professional enabler to attain clients goals (i.e. asking the solicitor whether he would send a letter to X). The solicitor-enabler facilitates fraud to relieve client pressure. The latter also includes an autonomous strain. At that time Jonathan had just divorced his first wife and Entwistle stated that if Jonathan did something (like send a letter with a false statement) then he would pay for his kitchen. So he was getting all these extra things of him and Jonathan became reliant on Entwistle to finish the

the kitchen or to pay off a credit card. They needed each other. Eventually, this went into the Bust strain. The client (Entwistle in this case) is pressurised to meet loan repayments (increased audit checks due to default). The strain is transferred to the professional-enabler who is already link into the fraud (Jonathan) to recycle fraudulent debt to avoid detection. The solicitor-enabler facilitates fraud to relieve client's strain and to avoid detection, leading to entrenchment. Jonathan became really entrenched.

Jonathan also has ten tips for us:

**1. We are out there:** professionals are commonly used to facilitate economic crime.

**2. The importance of being earnest:** don't take a professional's position at face value if you suspect serious wrong-doing. Don't place large firms on pedestals.

**3. Gut-instinct:** rely on it. Speak to your colleagues about it.

**4. The invisible supervisor:** think how an entity is being supervised.

**5. Be a criminal for a day:** I suspect this is happening, what would I do if I was person X?

**6. Beware of suspect professionals:** they might engage or be friendly in order to get more days in which they can try to do something/come up with a lie.

**7. Pressure cooker:** put very strict timescales on a professional and request evidence.

**8. Cut all angles.**

**9. Don't fear the horse bolting:** if you missed something, don't fear it, shut it down.

**10. Beat the shredder:** carefully preserve a paper trail.

When asked if he thinks he would still be doing this if he hadn't got caught, Jonathan says that he would not. It really took a toll on his health. He advises professionals who find themselves on the same slippery slope to connect to people around them and find the guts to own up as quickly as possible.

**For information on the next edition, Leaders in Finance AML Event 2025, see here:**

- **https://www.leadersinfinance.nl/aml-nl-event-2025-1/**