WHITE PAPER

Payment Service Providers must get in Control

How PSPs overcome 5 AML compliance challenges

Eugène van Kampen - Senior Customer Advisor - SAS Institute
Imre Homoki - Financial Crime Advisor - Consortix

Contents

Billions of dollars are laundered by criminals every year. They are increasingly doing this with tricks to stay under the radar. To detect these types of practices as efficiently as possible and to avoid false positives, sky-high fines and reputation damage, payment service providers must continuously adapt their processes and work AMLD-compliant. Are you in control?

Of course, you want to make headlines because of your excellent service, innovative products, and customer experience, not because of the negative attention brought on by poor money laundering controls. Some payment service providers (PSP) have been the target of fines and enforcement actions that is detrimental to growth. Are you in compliance with the laws and regulations? Have you missed suspicious transactions or sanctioned entities?

AMLD5: More offenses punishable

To combat money laundering and terrorism financing, the European Union has set strict rules through the EU Anti-Money Laundering Directive (AMLD). These rules follow each other at a rapid pace and AMLD5[1] now ensures more harmonization within the EU and places even higher demands on organizations. The list of criminal offenses has been supplemented with, among other things, environmental offenses, and cybercrime.

Higher penalties for organizations and individuals

Moreover, AMLD5 does not only penalize companies, but also individuals. Persons with the power of representation, decision-making power or power of inspection may be prosecuted for lack of supervision or control. All maximum sentences are set at a minimum of four years, whereby temporary exclusion from, for example, commercial activities can be imposed. Organizations risk confiscation of commercial activities and judicial liquidation, among other things.

The challenges of finding suspicious activity

The tightened laws and regulations underline that PSPs must keep an extra close eye on the transactions they process for their merchant customers, as well as the customers of these merchants. For this, a risk-based approach is an essential part, as well as being able to focus first on those that pose the highest threats. PSPs are faced with 5 challenges in this regard.

1 AMLD5 is in place since January 2020 and AMLD6 is already planned for December 2021 with even tighter rules.

1. Development of a Risk Assessment Framework

To comply with the rules, PSPs – and financial institutions in general – must be able to verify identity of their customers, as well as identify and assess the risks of potential money laundering, terrorism financing and fraud by their customers. Eugène van Kampen, senior customer advisor at SAS Institute, is clear about the mission for PSPs. "This means ensuring that no sanctioned entities are accepted as customers during onboarding – including their ultimate beneficial owners – and a proper due diligence is executed for those that are accepted, to determine how closely they need to be monitored in the future. Furthermore, a proper risk assessment framework includes controls for transaction monitoring."

With today's tremendous data volumes, how do you know that a merchant is showing abnormal behavior, either compared to his own profile or to the profile of his peers? And how do you identify sus-picious behavior? And how do you find out if a merchant is listed as a politically exposed person (PEP), for whom close(r) monitoring is required? Imre Homoki, Financial Crime Advisor at Consortix, states, "A comprehensive and up to date risk assessment is therefore the very fundament of any AML/CTF program."

2. Do you know your customers and your customers' customers?

Compliance risk modelling looks more straightforward for retail banks than for PSPs: customers have only been able to open an account after having gone through an identification procedure. As a result, banks know their customers well and can keep profiles on them, so they can detect future deviating behavior.

This works differently at PSPs. They work with merchants who do business with private individuals and companies. These merchants do not investigate their customers for illegal financial activity. They typically do not have transaction monitoring or fraud detection software in place, to detect suspicious financial behavior. PSPs' view on these end customers is limited, but yet important.

Besides the fact that a PSP should be monitoring the merchant's behavior, it also needs to monitor the merchant's customers' behavior. But since they are not the PSP's customers, a pseudo-profile needs to be built for them. The fact that PSPs have end customer data from sometimes dozens of different merchants is a great advantage herein. This gives PSPs the ability to get a holistic view of end customers across all merchants. Not only can they create much granular profiles, it also provides extra insight into the total money flows.

As said, the first-line customers, i.e. the merchants themselves, are also important to monitor. According to Van Kampen this can also be challenging because it might not be immediately clear who the real beneficial owner behind the merchant is, the so-called ultimate beneficial owner (UBO). "The EU AMLD requires identifying those UBO's – possibly through entity resolution – to ensure they are not sanctioned as well and to determine if they are listed as PEP, because in that case close monitoring is required."

3. The right skills needed!

"You not only need financial crime domain experts, but data scientists as well to be able to design and implement appropriate risk models. But you're not the only one with this demand," says Van Kampen. Due to the global digital transformation, data scientists and related professions are in high demand and therefore scarce. That is why it is important that – when purchasing an anti-money laundering (AML) solution – the partner and the scarce knowledge do not disappear after implementation. Therefore, choose a partner who not only helps you with the start-up, but who also trains your employees so that you can maintain and develop models yourself, and that provides a flexible and configurable solution that is easy to use.

Having a good risk model is one thing, but ultimately it is always people who make the decision, the investigators. Therefore, it's of utmost importance that they can make quality decisions quickly through a user-friendly, intuitive solution that provides visualization of relationships, workflow, straight-through processing, rich information about the detected suspicious behavior or entity, and so on.

The decisions taken by the investigators are key for compliance with regulations. Their decisions determine which customers and behavior need be reported to the regulator and which merchants need to be offboarded. In addition, they are also crucial when it comes to an (automated) feedback loop, that allows for continuous improvement of the PSP's detection strategies.

4. Traditional transaction monitoring is inadequate

Traditionally, PSPs rely on rule-based transaction monitoring systems. The system notifies you when one or more threshold values are exceeded by a particular event, financial or non-financial. The problem with these systems is that with these rules you're looking for the expected behavior. But even though the expected financial crime behavior still occurs, criminals and terrorists are changing their methods to not being noticed and you need to be able to find the unknown. "Criminals will try as well to hide their identity, so if you're not able to resolve entities it will be difficult to get a holistic view on their behavior and criminal activity might stay undetected," warns Van Kampen

Another challenge might occur when no proper segmentation model for the PSP's customers is in place. In that case all customers will be monitored in an equal manner, i.e. by applying the same rules and thresholds, often resulting in a huge number of false positive alerts. Since, from a compliance perspective, they all need to be investigated, the cost of compliance will be higher than necessary. Homoki is clear about rule-based transaction monitoring systems. "These old-fashioned Transaction Monitoring Systems will no longer get the job done."

Finding an appropriate segmentation model and fine-tuning existing models is where the need for analytics comes in and with that the need for the good data-quality, but as well the right tools and skill sets. Having those available is strongly dependent on the maturity level of the organization for applying analytics in its processes, but without a doubt required for the future to pro-actively prevent financial crime instead of detecting it after it has happened.

5. Silos obscure insight

Efficient data collection and analysis is one of the pillars of a well-functioning AML / CFT[2] framework. However, still many PSPs work in silos, i.e. they are not combining data from different product and services or domains, resulting in inability getting a holistic view on their customers and customers' customers behavior. Criminals can be very inventive, are skilled and operate internationally in several domains at the same time. That is why it is important to be able to bring all data together and analyse coherently, and with that be able to prevent financial crime and provide the right intelligence to the regulators.

The award-winning AML solution from SAS®

To remain compliant and to avoid reputational loss and financial damage, it is important to bring not only your organization but also the technology to the highest level with SAS® Anti-Money Laundering. Not only has SAS® shown for years that it is the market leader in Data and Analytics. In addition, SAS® was awarded "AML Solution of the Year" at the Asia Risk Technology Awards 2020. SAS® brought financial institutions' model accuracy to more than 90%, reduced false positives by up to 80%, and improved suspicious activity report (SAR) conversion rate by 400%.

SAS® combines next-gen detection with a high-performance, cloud-based solution. SAS® provides rapid time to value, speeding up the time from data to decision. The SAS® Anti-Money Laundering solution is an integrated suite of state-of-the-art technology, that supports all steps to be and remain compliant with procedures and regulations. From screening organizations, people, transactions, and the news, to supporting a thorough customer onboarding, transaction monitoring and reporting process. The user-friendly self-service platform provides access to all relevant data and takes work off your hands thanks to robotic process automation, integrated case management workflows, alert hibernation, and automated alert prioritization.

Consortix: next level implementation

Do you also want to be in control as soon as possible? And have your customer due diligence, watchlist screening, transaction monitoring and compliance reporting process of the highest level within your organization? Then choose SAS® Anti-Money Laundering, implemented by the leading financial crime consultancy in Europe: Consortix. With Consortix you can rely on the combination of expertise in financial compliance, IT and data science capabilities, as well as their SAS® Anti-Money Laundering implementation experience.

Consortix has experience implementing Anti-Money Laundering, Customer Due Diligence and Watchlist Management solutions for over 10 years. Thanks to the in-depth knowledge in the field and the Consortix approach, you will be in control and stay in control.

Bio Eugène van Kampen - Senior Customer Advisor at SAS Institute

Eugène van Kampen is a senior customer advisor at SAS Institute for over 8 years and has more than 20 years of experience advising companies on how software solutions can help combatting fraud, money laundering and terrorism financing. Prior to SAS he worked for other software vendors providing solutions for combating fraud and financial crime too, as well as for operational risk (including compliance with the Sarbanes-Oxley Act).

Eugène holds a Master of Science degree from Twente University, The Netherlands, and is a Certified Anti-Money Laundering Specialist (CAMS) and Certified Global Sanctions Specialist at ACAMS.

Bio Imre Homoki - Financial Crime Advisor at Consortix

Imre Homoki has 15 years of experience in fighting Financial Crime. He held various positions in the Anti-Fraud and AML domains and gained extensive experience in building and maintaining effective Fraud and AML programs.

Imre joined Consortix Ltd. in 2020 as a Financial Crime Advisor where his main tasks include implementing industrial best practices and ensuring regulatory compliance throughout the full cycle of the implementations. He also provides miscellaneous advisory support in financial crimes matters.

He is a member of ACAMS, as a Certified Anti Money Laundering Specialist and Certified Global Sanctions Specialist, also a member of ACFE, as a Certified Fraud Examiner.

To contact your local SAS office, please visit: sas.com/belux