Introduction

Both the crimes of money laundering (hereinafter: ML) and financing terrorism (hereinafter: FT)\(^2\) have their specificity. In particular, it appears in the multitude of ‘transactional activities’ undertaken between the source of funds (assets) and their intended use (demonstration) or investment (multiplying). Convergence in the field of ML and FT occurs especially when the reason for the mechanisms of camouflage of funds intended for terrorist activities is a prohibited act, which is a source of assets for their further criminal use (criminal consumption). In the case of money laundering, this is an obvious source of funds – a prohibited act, which is to be legalised in further proceedings, \textit{i.e.} to make it appear that their origin is not contrary to the law. Transactional activities should fall within the scope of the objective side of the act, such as the activities of receiving, possessing, using, transferring or exporting abroad, hiding, transferring or converting illegally obtained assets (money laundering). And in the case of terrorism financing, collecting, transmitting, making available or offering or covering costs. This state of affairs means that perpetrators use a wide range of chains of connections between obligated institutions and unsupervised entities for ML and FT, connecting them through various types of transactions, which are intended to facilitate the blurring of the source of funds and their destination. Thus, chains of connections are created that must be identified for the purposes of assessing criminal activities and their legal classification in the proceedings. Therefore, as part of counteracting ML/FT, there is a double process: declassification – not recognising ap-

\(^1\) Maciej Aleksander Kędzierski — doctor of law, legal advisor, lecturer in postgraduate studies at the Kozmiński University in Warsaw. 
Contact the author via the editorial office.

\(^2\) English acronym meaning: Anti-Money Laundering/Counter Financing of Terrorism.
parent processes as reflecting real events, and classifying the instrumental treatment of these ‘events’ as specifically defined crimes (especially under Articles 165a and 299 of the Penal Code). The criminal method of layering (ML) or building artificially multiplied links in the supply chain (FT) serves to consciously complicate ML/FT practices vertically and horizontally. Taking into account the tactical patterns used by the perpetrators, it is not necessarily possible for a single institution to be able to identify individual links or some logical sequence of them (using the assessment of the event as a preceding and subsequent link) arranged in the scheme of the chain of the procedure (a chain diagram too short to identify). Therefore, establishing patterns of actual chains of criminal transactions, which also have evidentiary or analytical value for the process, is very difficult and sometimes effective only at the level of the financial intelligence unit (hereinafter referred to as: FIU) or in the confrontation of financial information with information obtained through operational activities – reconnaissance. From the perspective of a single bank, as an obligated institution, it is sometimes not possible to notice a number of circumstances beyond a given bank. Only after receiving information from a larger number of banks (but also from other types of obligated institutions) is it possible to identify patterns of certain behaviours and dependencies between transactions that may indicate the criminal nature of the conduct. Taking these considerations into account, there is a constant search for mechanisms that can identify criminal chains of transactional links as quickly and broadly as possible for the purposes of counteracting money laundering and terrorism financing. In 2017, a report prepared by EUROPOL (the European Union Agency for the Cooperation of Law Enforcement Authorities) indicated that only 10% of reported suspicious transactions (Suspicious Transaction Reporting, hereinafter referred to as: STR) are further investigated after their collection, and this the status has not changed since 2006. Together, banks and MSBs (payment service providers) are the source of the majority of STRs sent to FIUs (financial intelligence units). However, reporting on terrorism financing accounted for less than 1% of the reports received by the FIU in 2013–2014. The use of cash is, however, the most important reason for reporting entities to inform FIUs about their suspicions.

The countermeasure mechanism in the AML/CFT system involves primarily creating knowledge about the threat in obligated institutions through risk assessment and appropriate adjustment of financial security measures. As a result of obtaining extended knowledge based on the identification, verification and monitoring of the client/transaction, as a result of detecting suspicious circumstances, information is further transferred – in the form of a report – to the financial intelligence unit. These reports

---

3 Penalisation in the Polish Penal Code (Ustawa z 6 czerwca 1997 - Kodeks karny, DzU, 2022, items 1138, 1726, 1855, 2339, 2600; DzU, 2023, items 289, 403, 818, 852, 1234, 1834) in the cited articles on terrorism financing and money laundering, respectively.

are the SAR (Suspicious Activity Report) and STR. The reports in question are the result of the recognition and analysis of identified events/circumstances that could be associated with money laundering or terrorist financing. They are transmitted by a single, individual obligated institution to the national financial intelligence unit. The reports become a source of knowledge and the basis for further analysis in the unit. As a result of collecting more extensive knowledge about the procedure, the information may be subsequently forwarded in the form of a notification about a suspicion of committing a crime to the prosecutor’s office. For many years, SARs have been subject to assessment of their reliability and usefulness in the fight against money laundering and terrorism financing. New solutions are also being sought to enable the transmission of these reports – not only with the knowledge of a single obligated institution, but also from a number of institutions, in one report, when the perpetrator’s activity concerned more than one of them. Moreover, ways are being sought to obtain the most effective possible picture of how a crime is created based on the mutual relations of the perpetrators, acting to the detriment of several obligated institutions, and by monitoring related transactions. It is important to obtain as wide a trace of the criminal chain as possible when the practice is based on relationships with various obligated institutions. So far, the main burden of such activities has been focused on the analysis of the financial intelligence unit, whose executive instruments were dedicated to cooperation with various obligated institutions. These activities were undertaken, as it were, secondary to the findings made by the obligated institutions based on primary, basic sources of information generated within the institution itself. Over time, noticing the systemic deficiencies in question, the obligated institutions themselves began to create mechanisms for building a common SAR (as a result of the knowledge of many obligated institutions), so that their value better approximates knowledge about criminal practices and their patterns. This means going ‘forward’ in terms of SAR content construction. The common SAR is, in principle, primarily a document (an extensive report) intended to inform the financial intelligence unit about the arrangements made in the obligated institution regarding the demonstrated circumstances of linking events, clients, transactions with suspicion of money laundering or terrorist financing involving more than one obligated institution. In particular, this should apply to the situation when a given obligated institution is aware that another institution has also fallen victim to the same or similar fraud, ML/FT practice or other type of crime, which affects the identification of both the original, basic prohibited act and the identification of the chain of legalisation of the funds obtained in this way, or transferring them to terrorist beneficiaries. The connecting element may be the client’s person (natural or legal), the procedure mechanism, the submission of the same documents, the country of origin or the beneficiary of the funds, etc.

Often, the effect of such conduct is referred to as ‘bulk SAR’ or ‘collective SAR’. It appears that it is also possible to use the term ‘common SAR’ or the popular British term ‘Super SAR’.
The Polish Act on countering money laundering and terrorism financing\textsuperscript{6} states that the basis for submitting a SAR is Art. 74 (indirectly also Article 41 section 2) of the P.P.P.F.T. Act. Pursuant to its content, the obligated institution shall notify the Inspector General of circumstances that may indicate a suspicion of committing the crime of money laundering or terrorism financing. The notification is submitted immediately, but no later than within 2 business days from the date of confirmation of the suspicion by the obligated institution. The notification shall include: identification data referred to in Art. 36 Section 1 of the P.P.P.F.T. Act, the client of the obligated institution submitting the notification, the identification data referred to in Art. 36 Section 1 of the P.P.P.F.T. Act, natural persons, legal persons and organisational units without legal personality who are not clients of the obligated institution providing the notification, the type and amount of property values and the place of their storage, the number of the account kept for the client of the obligated institution providing the notification, marked with the IBAN identifier or an identifier containing the country code and account number in the case of accounts not marked with an IBAN, the information referred to in Art. 72 section 6 of the P.P.P.F.T. Act, in relation to transactions or attempts to conduct them, indication of the country of the European Economic Area with which the transaction is related, if it was carried out as part of cross-border activity, information held about the identified risk of money laundering or terrorist financing and the prohibited act, including from which the property values may originate and the justification for forwarding the notification. In accordance with the assumptions of the drafter, the provision of Art. 74 Section 1 [of the P.P.P.F.T. Act] ‘provides for a departure from the necessity of a transaction whose circumstances indicate that it may be related to money laundering or terrorism financing, the so-called suspicious transaction, as a necessary condition for the materialisation of the reporting obligation (suspicious transaction report). Information about identified circumstances that are not necessarily related to a specific transaction is reported (suspicious activity report). The adopted solution seems to sanction the current practice of obligated institutions in terms of transferring the so-called descriptive notifications, and to take into account recommendations formulated for the Polish system for countering money laundering and terrorism financing during its evaluation conducted by the Moneyval Committee\textsuperscript{7}. As a consequence of its findings, the obligated institution may submit a report to the FIU, invoking Art. 74 Section 1 or Art. 86 Section 1 of the P.P.P.F.T. Act, depending on the status of the arrangements made. Specification of the behaviour, customer and identification of reasonable suspicion regarding the transaction

\begin{footnotesize}
\textsuperscript{6} Ustawa z 1 marca 2018 o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU, 2023, items 1124, 1285, 1723, 1843); hereinafter referred to as: the P.P.P.F.T. Act.

\end{footnotesize}
enables the provision of information pursuant to Art. 86 Section 1 of the P.P.P.F.T. Act. In the future, if supra-institutional reports are to be built, they should be focused on both the ability to identify suspicious circumstances and reasonable suspicions regarding accounts and transactions.

**The idea of building a ‘Super SAR’**

The basic motive for building ‘Super SARs’ (super-institutional reports, Super Suspicious Activity Reports) is greater exchange of information between reporting entities, which is the key to ensuring a more comprehensive view of suspicious incidents in which many people are involved or various banks are obligated institutions. This approach is justified in several respects. It is related to the fact that ML/FT perpetrators use various types of financial institutions in their criminal tactics, both in terms of subjectivity, the scope of services provided, but also in terms of geography and time non-parallelism (or identity). Another issue is that criminal activities are based on a network of personal and organisational connections, both in the field of organised criminal groups and terrorist organisations. Therefore, here too, there is a differentiation in terms of the subjects – contractors and objects – of institutions used to achieve a criminal goal, legalise funds or provide them to terrorist beneficiaries. Financial institutions may have difficulty identifying or detecting potential criminal activity on their own. While criminal networks deliberately conceal money laundering patterns by using multiple accounts at multiple financial institutions (and often in different jurisdictions), a given institution typically sees only a fraction of a transaction, network or trend, and most countries prohibit the exchange of information between an institution’s financial partners in connection with risk or suspicion of financial crime. Another argument in favour of cooperation and wider verification (supplementation) of information is that a single obligated institution, even the most organisationally and structurally developed, will always have a limited scope for perceiving signals about events that indicate suspicion related to ML/FT. This limited field of perception is primarily related to the specialised, own substantive scope related to the products and services provided. In the case of certain types of crimes, *e.g.* tax crimes, it is necessary to apply cross-checks, therefore, obligated institutions, especially those providing financial services to business entities, may, as part of the indicated cooperation, provide knowledge about the economic connections of clients involved in tax crimes (this is an additional advantage not only for countering ML/FT, but also initiating penal and fiscal inspections). Cashless transactions are also becoming increasingly popular, which is reflected in the history of accounts kept. Moreover, the specificity of the ‘legalisation’ of funds is largely based on the need to leave numerous ‘traces’ in the mechanisms of non-cash transactions related to servicing the accounts of entities participating in criminal activities. This argumentation, given as an example, already indicates the need for positive cooperation in terms of
combining facts, events, and building an 'extended' transaction trace, network connections and compiling complementary information content with knowledge as broad as possible and armed with elements and evidence of perpetration and suspicions regarding circumstances that may indicate the client’s involvement in money laundering or terrorist financing.

The same applies to specific transactions (suspicious) or funds placed in a bank account. As a consequence, it is possible, in the event of suspicions of committing financial crimes (but also ML/FT), to submit one joint notification (report) with other obligated institutions as participants of the AML/CFT system. The approach, focused on a supra-individual common SAR, brings closer the recognition and analysis of ML/FT signs based on searching for traces of the organisation of criminal activity, rather than identifying it with a specific event and a specific type of product offered by a given (unidirectionally profiled) obligated institution. This is a different paradigm than the current one of looking at the SAR only through its own scope of substantive performance, in favour of a broad perspective of identifying the practice in various areas related to the service provided by the obligated institutions. To build such ‘Super SARs’, it is possible to use a wide range of business profiles of broadly defined (also in the Polish Act) obligated institutions. However, the impetus for such action may come from the initiative of both the obligated institution itself and the financial intelligence unit. If it is possible to implement projects, as in the first case, the financial intelligence unit should be at least notified about such an initiative and its implementation, and in addition, the regulations should provide it with a supervisory status or the possibility of discontinuing this cooperation at any time for a justified reason. Given the rather domestically assessed effect of introducing ‘Super SARs’, it is also worth mentioning the possibility of applying them in international relations. Here, the possible positive effect should be taken into account in the face of the significant internationalisation of money laundering and terrorism financing. Looking at this problem from the point of view of financial intelligence units, both the FATF (Financial Action Task Force\(^8\)) and EU documents have for many years placed an emphasis on motivating and observing broad cooperation between national financial intelligence units. The argument about the internationality of the practice of ML/FT is often cited in this context. Creating a transnational alliance of obligated institutions could help in the fight against crime both at the base level (as prohibited acts generating criminal profits) and at the level of mobilising these funds for the purpose of their apparent legalisation or to be provided to terrorist beneficiaries of terrorist activities. Another argument in favour of building a ‘Super SAR’ is that, as part of this cooperation, obligated institutions will be able to better understand, identify and assess risk, especially in the field of institutional risk. This approach should strengthen risk assessment, especially carried out by smaller obligated institutions, and

---

\(^8\) Anti-Money Laundering Task Force – an intergovernmental organisation established in 1989 on the initiative of the G7 group of countries to develop a global policy to combat money laundering.
reverse the trend related to derisking, or debanking, which is also used in the AML/CFT area.

So far, the methods of ‘checking the threat’ related to a client or a transaction have been limited to the following activities: a system that usually requires the cooperation of at least two different intra-bank teams and imposes restrictions on the type of information that can be exchanged, based on configuring encrypted e-mail messages or just a phone call. These systems, although verifiable in reality, had side effects, such as slowing down the settlement of transactions between customers and generating high operational costs. Moreover, these activities were carried out as a subjective initiation, and not as one of the basic elements requiring verification. Moreover, solving problems related to data privacy (protection of the secrecy of financial information) should improve the monitoring of suspicious transactions and enable the exchange of information both between regulatory authorities and the obligated institutions themselves.

One of the basic elements of building the ‘Super SAR’ is to create legal possibilities to provide information to other entities in order to supplement the initial material constituting the starting knowledge for further analyses. The American PATRIOT Act (hereinafter referred to as: Patriot Act)\(^9\) was, among other things, intended to enable a broader exchange of information between law enforcement, regulators and financial institutions regarding AML risk. Notably, Section 314(a) of the Patriot Act and its implementing regulations (Section 314(a)) allow federal, state, local, and EU law enforcement agencies to contact U.S. financial institutions through the U.S. Department of the Treasury’s Crimes Enforcement Service, FinCEN (Financial Crimes Enforcement Network), to locate accounts and transactions of persons who may be involved in terrorism or money laundering. Section 314(b) of the Patriot Act and its implementing regulations (section 314(b)) provided financial institutions with a limited, secure ability to share information with each other to better identify and report potential money laundering and terrorist activities.\(^{10}\) However, a U.S. financial institution may not share a SAR Suspicious Activity Report or disclose information about the existence of such a report (SAR Information) with third parties, including non-U.S. affiliates. Therefore, in order to create more extensive reports, both in terms of subject matter, it is necessary to introduce appropriate regulations enabling the ‘sharing’ – between authorised entities – of knowledge in the area of information generated in the field of AML/CFT.

Joint monitoring of transactions is not only the responsibility of banks, but also of other institutions. The inquiry is not related to transactions but to due diligence towards specific customers. The main dilemma here

is the difficulty of determining how many entities, apart from the first applicant institution, also have a similar problem with this client and the possibility of differences in the assessment of the risk level between clients of individual institutions to which this ‘collective’ operation of the system may apply. It seems that the common SAR will continue to strive to achieve an ‘extended transaction footprint’, which means that banks and payment entities, as before, will be the most interested and involved in the AML/CFT system, and it is they who will most often take the initiative to launch the common SAR procedures. It should be noted that, by servicing financial settlements, banks are often able to partially monitor the activity of other entities in the AML/CFT system. However, creating a common SAR should help in determining the actual mechanisms of ‘laundering’, ‘investing’ and ‘transferring’ funds, which should not only be associated with tracking ‘criminal profits’, but rather the means used by the perpetrators. This has to do with the specificity of both ML and FT. In both cases, criminally managed funds may be mixed with legally obtained funds, which makes it difficult to identify the funds originally marked with criminal activity and to identify the criminal practice of using them.

‘Super SAR’ in British legal solutions

In the United Kingdom, under the Proceeds of Crime Act 2002 (POCA)\textsuperscript{11} and the Terrorism Act 2000,\textsuperscript{12} persons in the regulated sector are obliged to submit a SAR in relation to information that comes to their attention in the course of their business if they know, suspect, or have reasonable grounds to know or suspect that a person has attempted or is engaged in money laundering or terrorist financing.\textsuperscript{13} These provisions allow banks and other companies in the regulated sector to exchange information with each other on a voluntary basis in connection with the suspicion that a person is involved in money laundering, the suspicion that a person is involved in committing a terrorist financing offence or in connection with the identification of terrorists’ property or its movement or use. The idea to create the ‘Super SAR’ mechanism in the UK arose from the success of the Joint Money Laundering Intelligence Taskforce (JMLIT) – a partnership between law enforcement agencies and financial institutions.

The British Criminal Finances Act of 2017 (hereinafter referred to as: CFA)\textsuperscript{14} brought significant changes to the system for reporting suspicions of money laundering, introducing a new countermeasure instrument in

\textsuperscript{13} The Criminal Financing Act 2017 (CFA) introduced new sections 339ZB−339ZG into the Proceeds of Crime Act 2002 (POCA) and new sections 21CA–21CF into the Terrorism Act 2000.
the form of the ‘Super SAR’. The very adoption of the Act and the preparation of legal solutions therein were preceded by the preparation of the government’s ‘Action Plan for Counteracting Money Laundering and Terrorism Financing’ in April 2016. It presents proposals to reform the SAR system and improve the exchange of information both between law enforcement agencies and the private sector and within the private sector by introducing ‘legal information exchange ports’. The plan was to build on the work done by the Joint Intelligence Task Force on Money Laundering (a pilot set up in February 2015 as part of the Serious and Organised Crime Financial Sector Forum), which involved the National Crime Agency (hereinafter referred to as: NCA) and representatives of the financial sector. The system enables regulated sector entities to voluntarily share information with other regulated sector entities for the purpose of submitting a common SAR. The ‘Super SAR’ aims to condense information from various sources to produce a higher quality report. The ‘Super SAR’ mechanism is also intended to fulfil the reporting obligations of entities – obligated institutions – and eliminates the need for many such entities to submit SARs in the same case. In addition to the Act, the UK Home Office has published a circular providing further guidance on the exchange of information between banks and other financial institutions in accordance with the CFA. Pursuant to the Act, information may be made available either on the initiative of regulated entities or at the request of the competent national authority. The Act sets out the conditions under which such exchange of information may take place, including the provision of the required notification to an authorised officer of the competent national authority. The notification is treated as meeting the requirements for disclosure of information on suspected money laundering in accordance with Art. 330 and 331 POCA. The Act provides that a disclosure of information made in good faith by a regulated entity will not violate any obligation of confidentiality owed to the person making the disclosure or any other limitations on the disclosure of information. Providing information under the provisions is completely voluntary and at will. A member of a regulated sector also has the right to refuse such disclosure. Members of the regulated industry should consider whether they are required to submit SARs individually or take advantage of the information exchange provisions. What is important is the so-called submitting a request for disclosure. A request for disclosure may only be made by an authorised

---


official of a national authority or by a regulated sector entity. The recipient of the disclosure request must also be an entity conducting business in the regulated sector. Requests for disclosure must include the following elements: a statement that the request is made in connection with suspicion of money laundering by a person and an indication of the suspected person (if known), a description of the information requested from the recipient, and an indication of the person or persons to whom disclosure of the information is requested. In addition, where a disclosure request is made by a requesting entity in a regulated sector rather than by a competent national authority, it must also include a statement stating that the person is suspected of engaged in money laundering and other information that the person making the disclosure request considers deemed appropriate to enable the recipient to determine whether the requested information should be disclosed. Where an applicant submits a request for disclosure, he or she must also make a notification to the NCA (National Crime Agency), which acts as the Financial Intelligence Unit (FIU). Such notification relieves the requesting entity from its disclosure obligations under Section 330 and its designated officer obligations under S331 POCA (Section 331). At the same time, the required notification to the NCA must: state that a disclosure request has been made; specify the entity to which the disclosure request was directed; identify any persons (if known) suspected of engaging in money laundering in connection with the disclosure request; provide any other information that would be required to be disclosed to the competent national authority when submitting a traditional SAR, in particular the information on which such knowledge or suspicion is based, and the location of the money laundered property (if known).

Once a disclosure request is received, the recipient has the option and at the same time the dilemma of whether to disclose the information because the system is voluntary, not mandatory. The service recipient may disclose information if the following conditions specified in the regulations are met. Condition 1 – The recipient is an entity conducting business in a regulated sector, the information on which the disclosure is based reached the recipient in the course of conducting this regulated activity and the person (or persons) to whom the information is to be disclosed is also an entity conducting business in the regulated sector (regulated entity). Condition 2 – An authorised officer of the NCA has requested disclosure from the recipient or the person to whom the information is to be disclosed (or at least one of them) has requested it from the recipient. Condition 3 – Before the recipient makes the disclosure, the required notice, as indicated above, will be given to the competent national authority. Condition 4 – The recipient must be satisfied that the disclosure will or is likely to assist in establishing any matter relating to the suspicion that the person is engaged in money laundering. Disclosure may not include information obtained from a UK law enforcement authority unless that authority consents to such disclosure. Once a recipient has disclosed information in response to a disclosure request, the recipient and the requesting entity may elect to prepare a joint disclosure report (i.e., a ‘Super SAR’). The
joint disclosure report includes: a notification to an authorised officer of the NCA, a joint determination made by the recipient and the requesting entity to provide the information (as defined above and potentially with other entities to which the recipient has disclosed the information), and an indication that the joint information, after disclosure by the recipient to the requestor, will be sent before the expiry of the ‘applicable deadline’ as drafted, i.e. before the expiry of: (1) the deadline set by the competent national authority, if requested; or (2) 84 days from the date on which the required notification was made to the appropriate national authority. The report should meet the following content requirements: (a) include an explanation of the extent to which there are still grounds to suspect that the person has been involved in money laundering; (b) contain information identifying that person; c) determining the basis for suspicion; d) and provide any other relevant information on the matter.

As indicated, although the Act gives regulated entities the opportunity to submit an application for access to information, it does not impose such an obligation. Without a mandatory filing, it is difficult to predict how proactive regulated entities will be in requesting information from each other rather than simply filing a traditional SAR. The ability to share information and submit joint reports can be extremely useful for some entities if their interests are aligned but may prove problematic if entities disagree about whether to file a SAR. The provisions have been assessed as complex and user-unfriendly, and there are concerns that the exchange of information under the new system may impact data protection.

Polish legal solutions ensuring improvement of SAR quality

The Polish legislator indicated that obligated institutions included in the group and their branches and subsidiaries with the majority share of these institutions having their registered office in a third country introduce a group procedure for counteracting ML/FT in order to comply with the obligations imposed on the group and its entities – obligations specified in the provisions on counteracting money laundering and terrorism financing. The group procedure defines the rules for the exchange and protection of information provided for the purposes of performing obligations in the field of counteracting ML/FT between individual entities

---

18 Harris D, Birch A, op. cit.
included in the group (Article 51 Sections 1 and 2 of the P.P.P.F.T. Act). A group procedure should be created when the group includes at least one obligated institution and at least one entity – another obligated institution or an entity conducting activities corresponding to the activities of obligated entities defined in EU (European Union) regulations. The group procedure should also be created when the obligated institution has established a branch in a third country. As indicated by the General Inspector for Financial Information (hereinafter referred to as: GIIF\textsuperscript{21}), referring to the explanatory note to FATF Recommendation No. 19 – mandatory provisions regarding the exchange of information (between group entities) should include provisions ensuring confidentiality and preventing information leakage.\textsuperscript{22} The exchange of information in a group is therefore a special case of possible exchange of information between the obligated institutions that are part of the group, taking into account the conditions specified by law.

Moreover, in order to counteract ML/FT, clearing houses established pursuant to Art. 67 of the Act of August 29, 1997 – Banking Law\textsuperscript{23} and institutions established on the basis of Art. 105 Section 4 of this Act, provide the GIIF [GIFI], at its request, with the information and documents covered by the request. Requests, information and documents may be transmitted using an IT system. The house with the indicated status is the National Clearing House (hereinafter: KIR S.A.).\textsuperscript{24} At the same time, it should be noted that obligated institutions may use the services of a third party when applying the financial security measures referred to in Art. 34 Section 1 points 1–3 of the P.P.P.F.T. Act, provided that this entity immediately provides, at the request of the obligated institution, the necessary information and documents regarding the financial security measures applied, including copies of documents obtained during the application of financial security measures consisting in the identification of the client and the actual beneficiary, and verifying their identity, in particular using electronic identification means and trust services enabling electronic identification within the meaning of Regulation 910/2014.\textsuperscript{25} Additionally, at

\textsuperscript{21} The name General Inspector of Financial Information – in English, it allows the use of the abbreviation: GIFI.


\textsuperscript{23} Ustawa z 29 sierpnia 1997 - Prawo bankowe (DzU, 2022, items 2324, 2339, 2640, 2707; DzU, 2023, items 180, 825, 996, 1059, 1394, 1407); hereinafter referred to as: the Banking Law.

\textsuperscript{24} National Clearing House S.A. – infrastructure institution of the Polish banking sector, operating pursuant to Art. 67 of the Banking Law.

the request of the GIIF, the obligated institution shall immediately provide or make available the information or documents in its possession, necessary to carry out the tasks of the GIIF specified in the Act, including those relating to: 1) customers, 2) transactions carried out, in the scope of data specified in Art. 72 Section 6 of the P.P.P.F.T. Act, 3) the type and amount of property values and the place of their storage, 4) the application of the financial security measure referred to in Art. 34 Section 1 point 4 of the P.P.P.F.T. Act; 5) IP addresses from which the connection to the IT system of the obligated institution was made, and the connection times with this system (Article 76 Section 1 of the P.P.P.F.T. Act).

Unlike the solutions specified in Great Britain, Polish AML/CFT solutions do not include the ‘Super SAR’ procedure in the P.P.P.F.T. Act as a common way of identifying common suspicions about the behaviour of clients of different obligated institutions. Therefore, it seems that the current legal status in accordance with the P.P.P.F.T. Act only allows for building a common SAR of entities included in the group and covered by the so-called group procedure. However, the Polish Bank Association (hereinafter referred to as: ZBP\(^{26}\)) and KIR S.A. are jointly currently working on a new initiative, which has been defined as the Sector AML Service Center (hereinafter referred to as: SCU-AML), which is to be an element of technical support for banks as obligated institutions for the purposes of constructing ‘Super SAR’.

**British organisational solutions aimed at improving the quality of SARs**

Similar technical solutions as the designed SCU-AML are also in force in other countries. For example, in Great Britain, there is the Mule Insights Tactical Solution (hereinafter: MITS). MITS Technology, developed by Vocalink, uses technology to combat financial crime, and tracks illicit funds as they move between bank and building society accounts, regardless of whether the payment amount is split between multiple accounts or whether these accounts belong to the same financial institution or various financial institutions. The technology is being rolled out as part of a coordinated crackdown on app fraud, in which customers are tricked into sending funds to fake accounts. The model creates a visual map of where and when money was moved, providing new insights for fraud teams to take action.\(^{27}\) The UK financial network solution tracks the flow of funds through the financial system and identifies suspicious mule networks. By combining payment data from multiple banks and overlaying it with


state-of-the-art proprietary analytics and algorithms, MITS can pinpoint individual accounts – known as ‘mule accounts’ – that are engaged in illegal or suspicious activity.\textsuperscript{28} The technological system itself also focuses on fraud and money laundering methods. It is important not to look for individual symptoms, but to build knowledge and patterns of large and more complicated transactions made by perpetrators of economic crimes. This usually includes unusual spikes and drops in a person’s bank balance. Mastercard’s Vocalink runs MITS, which, with the consent of member banks, monitors a large proportion of UK accounts for distinctive mule account patterns. Money often leaves ‘mule accounts’ in nanoseconds, facilitated by bots, which makes it harder to track. Cooperation between banks is hampered by data protection regulations. UK Finance is seeking new powers from the government to enable banks to share information in situations where there is reasonable suspicion of illegal activity.\textsuperscript{29} MITS was created by Vocalink, the infrastructure provider for the Faster Payments service, as part of a suite of measures shared and developed by the industry to further protect consumers online. MITS relies on Vocalink’s financial crime solution, Anti Money Laundering Insights, which therefore uses advanced analyses of payment data from multiple institutions to help them address money laundering and mule networks.\textsuperscript{30} The British initiative in the form of MITS also overlaps with the ability to generate ‘Super SARs’ under the POCA Act.

**Dutch organisational and legal initiative to improve the fight against financial crime**

Another solution is the Dutch Transaction Monitoring Netherlands system (hereinafter referred to as: TMNL). Five Dutch banks – ABN AMRO, ING, Rabobank, Triodos Bank and Volksbank (referred to as the founding banks) – joined forces in 2019, creating a common system for the above-mentioned purposes. The aim of the project is to jointly fight financial crime by jointly monitoring bank payment transactions for signs that could potentially indicate money laundering or terrorist financing. The system operates on the basis of a shareholders’ agreement. On July 8, 2020, the founding banks announced that they had signed a TMNL shareholders’ agreement establishing TMNL as an independent private limited liability company. Their activities were integrated into the *Action Plan against money laundering* (2019).\textsuperscript{31} The study found that bulk transactions will

\textsuperscript{28} Money mule – someone who is paid or coerced by a criminal to launder money from his or her bank account in order to make suspicious transactions more difficult to track.


allow for better and more effective detection of criminal money flows and networks in addition to what banks can achieve individually with their own transaction data. The above-mentioned action plan included, among other things: amendment to the Act on Counteracting Money Laundering and Terrorist Financing (Dutch: Wet tegen witwassen en terrorismefinanciering or Wwft; hereinafter referred to as: Wwft),\(^{32}\) which was to enable full-scale monitoring of collective transactions (Article 3b Wwft). For the financial services sector, one of the most important changes proposed by the bill is the possibility of joint monitoring of transactions by banks and outsourcings this monitoring. How is TMNL supposed to work? To prevent criminal activity, participating banks send encrypted transaction data to TMNL, which then monitors these transactions to detect unusual activity that potentially indicates money laundering. Once detected, TMNL sends the transactions to the banks involved. The bank is then responsible for reporting the suspicious activity to the Financial Intelligence Unit for further investigation of said transaction. It is worth noting that TMNL currently only monitors business accounts [company accounts].\(^{33}\) The TMNL system uses advanced algorithms and machine learning technologies to detect patterns and anomalies in transaction data. This helps financial institutions identify unusual transactions and behaviour that may indicate financial crimes. TMNL also provides real-time alerts and notifications to financial institutions, allowing them to take quick action to prevent financial crimes.\(^{34}\) Joint transaction monitoring will allow banks to better identify unusual transaction patterns. TMNL is an addition to banks’ individual transaction monitoring efforts and focuses on identifying unusual patterns in payment traffic that individual banks are unable to identify. The two most important regulations relating to TMNL are the Wwft, which sets out the legal framework for the implementation of banks’ statutory obligations, and the General Data Protection Regulation.\(^{35}\) The current basis for sharing data by banks participating in TMNL as a processing entity

---


is the legitimate interest of participating banks (Article 6 Section 1 point f of the RODO [GDPR]) as part of their obligation to comply with the provisions of Art. 3 Wwft (customer survey). TMNL was positively assessed by the Dutch Banking Association (NVB). It was pointed out that, in addition to banks fulfilling their own obligations as elements of the AML/CFT system, effectively dealing with money laundering and terrorism financing requires a national (chain) approach. Therefore, banks cooperate closely with government partners, such as the Ministry of Finance, the Ministry of Justice, the Ministry of Security, FIOD (Dutch: De Fiscale inlichtingen-en oppsporingsdienst; Fiscal Information and Investigation Service) and the Financial Intelligence Unit (FIU). Together, the goal is to significantly increase the return on the chain from identification to detection, prosecution and conviction of a crime. The banks took up this initiative, expecting that it will be sanctioned in a future amendment to the Wwft Act.

The final version of the Wwft Act is currently in the legislative process, which was also implemented in 2022. During this process, several changes were adopted after sharp criticism of privacy issues from the Dutch Council of State (hereinafter referred to as: RS) (negative opinion of 13 January 2021), an independent consultant to the Dutch government and the Dutch Data Protection Authority (AP). The RS opinion noted in particular that ‘as important as the fight against money laundering and terrorist financing is, in the case of these measures the question arises whether the ends justify the means. These resources go too far in the context of the bill. This concerns the exchange of information during joint monitoring of banking transactions and customer due diligence and that the indicated measures remain: a disproportionately far-reaching violation of the fundamental rights of Dutch citizens’. As a result, the final proposal limits the scope of monitoring and the types of data that can be shared and processed between banks. More conditions have been added regarding the protection and security of personal data. Moreover, the draft law provides that the activities must be evaluated after four years of operation. According to the RODO [GDPR], the processing of ‘per-

---

36 Processing is lawful only if, and to the extent to which, at least one of the following conditions is met: the processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual requiring protection of personal data, in particular where the data subject is a child.


39 Ibid.

sonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a person or data on health or data relating to someone’s sexual behaviour or orientation sexual’ (Article 9 Section 1 of the RODO [GDPR]) is prohibited. However, the Wwft Act amendment will enable banks to process such data. For banks, this means that data will have to be made available to an independent institution that will collect and analyse all this data from and on behalf of banks.41

AML Bridge – Estonian mechanism to support institutional activities in the fight against financial crime

AML Bridge is an information and data exchange platform created in 2019, based on the start-up (venture capital) Salv (created in 2018), which enables financial institutions to combat financial crime more effectively. This secure online platform helps banks exchange and enrich data about negatively marked entities, enabling them (banks) to strengthen their anti-money laundering efforts. As its authors point out, the exchange system is encrypted and fully compliant with the latest data protection regulations. As a result, AML Bridge can help financial institutions cooperate proactively across borders, across legal jurisdictions and against transnational criminal networks.42 Estonia’s banks have united in an anti-money laundering (AML) initiative created by the regtech startup Salv. Participating banks are Swedbank, SEB, Luminor, LHV, Bigbank, Citadele, OP Bank, Coop, TBB and Inbank. These entities have partnered with Salv to create the AML Bridge information and data exchange platform. AML Bridge legally and securely facilitates collaboration between financial institutions across borders and legal jurisdictions so that international criminal networks can be combated more holistically. Salv Bridge uses end-to-end encryption as well as a password-protected key system, in addition to two-factor authentication (2FA) and IP whitelisting. Salv does not have access to data exchanged over the Salv Bridge network. AML Bridge has made the most progress in the Baltics and the United Kingdom, but work is underway to expand its operation to Poland,43 Sweden and Germany. Salv acts

41 Ibid.
43 Salv received nearly PLN 20 million (EUR 4 million) for the development of infrastructure in Poland. Extension of the so-called seed round was led by the Polish-American fund ffVC Tech & Gaming and the German G+D Ventures (financing was also provided by existing investors). Thanks to this support, the start-up plans to open an office in Poland where it will employ engineers and business development specialists. The Warsaw team will help companies and financial institutions not only from our country, but also from the entire region of Central and Eastern Europe. See: Duszczyk M, Estończycy chcą skończyć z praniem pieniędzy nad Wisłą. To „cyfrowi policjanci”. Electronic source: https://cyfrowa.rp.pl/biznes-ludzie-startupy/art37905351-estończycy-chcą-skonczyć-z-praniem-pieniędzy-nad-wisłą-to-cyfrowi-policjanci, accessed: 10.05.2023.
as a data processor, which means that from a financial data protection point of view, the institutions remain the data controllers, and Salv only ensures that the data is processed only in accordance with the instructions of the controllers’ RODO [GDPR] combined with national regulations on countering money laundering and terrorism financing, which create the so-called the core platform for EU-wide use of AML Bridge. 44

Initiative of the Polish Bank Association and KIR S.A. – the SCU-AML project

Polish Bank Association and KIR S.A. jointly undertook to implement a new initiative, which has been defined, as previously mentioned, as SCU-AML. In Section 3 [Dział 3] of the National Court Register, 45 you can read that KIR S.A. – indicated as the implementing entity – expanded its activities to include the subject of the remaining activities of the entrepreneur for KIR S.A., indicated as task 63, 11, Z, defined as: ‘providing services supporting the management of operational risk of banks and cooperative savings and credit unions and other providers of payment services, in particular services supporting the prevention of the use of their activities in order to conceal criminal activities or for purposes aimed at connection with a crime, including fiscal crime or money laundering and terrorism financing.’ 46

Details of the scope of the term ‘provision of supporting services’ can be found in various statements by decision-makers: The Sector AML Service Center is intended as structural and organisational assistance for banks in fulfilling numerous obligations arising from money laundering regulations. The idea is to achieve a synergy effect within the framework of the quite extensive information systems maintained separately in KIR and ZBP. However, using them jointly makes it possible to support banks in performing their duties in such areas as, for example, analysis and detection of suspicious transactions, typing of suspicious transactions, identification of actual transaction chains of criminal activities, KYC (Know Your Customer) processes for individual and corporate clients, sector PEP (Politically Exposed Persons) list, sector tools for verifying sanction lists, and other solutions planned at a later stage, such as centralisation of responses for law enforcement agencies’. 47

45 Pursuant to Art. 40 of Ustawa z 20 sierpnia 1997 o Krajowym Rejestrze Sądowym (DzU, 2023, items 685, 825, 1705).
47 Wywiad z wiceprezesem ZBP T. Białkiem przeprowadzony przez R. Lidke, Sektor bankowy wprowadza rozwiązanie wykrywające transakcje przestępstw. Electronic source: https://zbp.pl/Aktualnosci/Wydarzenia/Sektor-bankowy-wprowadza-rozwiazanie-wykry-
is the identification of actual chains of criminal transactions. From the perspective of an individual bank, it is not possible to notice a number of circumstances beyond a given bank. Only after receiving information from a larger number of banks is it possible to identify patterns of certain behaviours and relationships between transactions that indicate that they are of a criminal nature.\footnote{Ibid.} Thanks to cooperation in this area, it will be possible, for example, to limit criminal transactions more broadly.

As Tomasz Roszak notes, the main beneficiaries of a broader, sectoral view of data should be KYC (Know Your Customer) processes, CDD (customer due diligence requirements), identification of the path of suspicious transaction flows and the ‘mule’ accounts involved (accounts created for so-called pillars that are intended only to mask money laundering or terrorism financing).\footnote{Roszak T, Raport Specjalny | BEZPIECZEŃSTWO BANKÓW — KIR | Sektorowe Centrum Usług AML. \textit{Electronic source}: https://bank.pl/raport-specjalny-bezpieczenstwo-bankow-kir-sektorowe-centrum-uslug-aml/?id=410920&catid=36799, \textit{accessed}: 16.05.2023.} It is assumed that the GIIF [GIFI] will be able to receive, through SCU-AML, more precise information constituting the results of cross-sectional analyses carried out within this institution. According to the assumptions, the operational processes and technical solutions of SCU-AML will be located at KIR S.A. and in ZBP, depending on the catalogue of services, and the location of the data, systems and analysts. The main source of data will be STIR, \textit{i.e.} the Clearing House Teleinformatic System (together with data obtained for the needs of the Financial Information System (SInF) planned to be introduced),\footnote{Ustawa z 1 grudnia 2022 o Systemie Informacji Finansowej (DzU, 2023, item 180).} supplemented with data from the Elixir and Express Elixir systems, as well as the interbank information exchange systems of the Polish Bank Association, including: database of compromised accounts, database of compromised identities, database of compromised IP addresses and database of people wanted on wanted lists. Data exchange services will, in principle, be based on existing data exchange channels: banks – KIR S.A. and banks – ZBP [Polish Bank Association]. The services planned to be made available include the following: signalling of a client’s PEP status, signalling of a client’s appearance on sanctions lists, sector information about a corporate client, verification of the actual business activity of a corporate client, analysis of reported suspicious accounts, detection of suspicious accounts and transactions, reporting information on terminated business relations and reporting above-threshold transactions to the GIIF [GIFI].\footnote{NBP, Polish Payment System Oversight Report for 2021. \textit{Electronic source}: https://www.nbp.pl/systemplatniczy/rada/sprawozdanie_2021.pdf, \textit{accessed}: 16.05.2023.} The SCU-AML project will enable banks to support them in performing their current AML/CFT obligations in such areas as: analysis and detection of suspicious transactions, typing of suspicious transactions, identification of actual chains of criminal transactions, KYC processes, sector PEP (Politically Exposed Persons) list (persons holding politically exposed positions),
sector tools for verifying sanctions lists, and centralisation of responses for law enforcement agencies. Information from more media shows that SCU is an initiative beyond the P.P.P.F.T. Act and is not fully anchored in it. In fact, it seems that the SCU-AML project is a continuation of the services previously provided by KIR S.A. for banks in areas other than AML. This one is dedicated to the area of anti-money laundering. The existing solutions could be based on the content of Art. 13 of the P.P.P.F.T. Act, which states that in order to counteract money laundering and terrorism financing, clearing houses established pursuant to Art. 67 of the Banking Law and institutions established pursuant to Art. 105 Section 4 of this Act [the P.P.P.F.T. Act] provide the GIIF [GIFI], at its request, with information and documents covered by this request. This type of action could also be taken on the basis of the provisions of Art. 47 of the P.P.P.F.T. Act. It seems that KIR S.A. should not be considered an additional obligated institution, but only an indirect technical entity that could, in addition to verification Activities, also undertake activities of associating institutions according to specific criteria, when these institutions individually undertake AML/CFT obligations independently of each other towards the same entities. Identification of identical but unknown interests and their merging could lead to the possibility of preparing joint, collective SARs for the financial intelligence unit.

Summary

The experience acquired over the years in the operation of the AML/CFT system, focusing on the creation of SAR reports based on risk assessments and the financial security measures for clients and transaction monitoring, seems to only partially meet the assumptions of effectiveness. It should be noted that this approach also created a number of negative behaviours in the relations between obligated institutions and other entities, including financial intelligence units. These negative issues include an excessive number of reports submitted, the actual information value of which is small or non-existent. The issue is related to, among other things, concern on the part of the obligated institutions to impose administrative penalties for failure to comply with obligations in the AML/CFT system. Another issue is the lack of understanding or reluctance, as well as the implementation of an internal security policy, which leads to debanking or derisking – towards entities and potential clients from the high-risk area, which may expose the obligated institutions to problems related to involvement in the perpetration of predicate crimes, fraud,

---

52 Article 67 of the Banking Law – ‘The State Treasury or banks, together with banking chambers of commerce, may establish clearing houses in the form of commercial companies for the purpose of exchanging payment orders and determining mutual receivables arising from these orders. The State Treasury may be a shareholder or shareholder of the clearing house. In order to secure settlement, the clearing house may create a guarantee fund from banks’ funds; the funds of this fund are not subject to enforcement against the bank’s assets’. 
money laundering or financing terrorism. As a consequence, there is a lack of knowledge about the most critical behaviours of perpetrators, and as a result, obligated institutions inform financial intelligence units only about ‘lower quality’ behaviours of selected clients. Additionally, attention should be paid to the limited possibilities of cooperation with cooperating entities and exchange of information with other obligated institutions outside the group. In addition, there is a dysfunction between the freezing of funds of entities designated on sanctions lists and the ability to track and monitor the transactions they order or the funds they collect. Another solution that limits the quality of building knowledge about suspicions of money laundering or terrorism financing is the introduction of solutions similar to those in AML/CFT systems to other issues related to, for example, the need to combat tax crime and react with sanctions to instigated war conflicts that are incompatible with the UN Charter. Sometimes, the perpetrators appear not only in these configurations but are also associated with money laundering and terrorism financing.

Despite constant pressure from the FATF to build SARs that are qualitatively adequate to the disclosed threats, only isolated cases can be noted in which legal solutions – at the level of the Act – ensure the construction of the so-called common, possibly collective SARs (UK, POCA). The specificity of committing ML/FT crimes is related to the need to coordinate many places where perpetrators leave traces related to money laundering or terrorism financing. Consequently, several financial institutions, but also other types of obligated institutions, may be harmed in one operation. This disproportion is related to the heterogeneous preparation of obligated institutions to assess risk and the ability to recognise it and build compliance processes. Obtaining a combination of the results of these activities and knowledge about individual links in this chain requires cooperation between obligated institutions not only at the level of disclosure but also with the monitoring of customers’ behaviour as potential perpetrators. This canon of understanding the phenomenon and counteracting it triggers various initiatives in the field of building schemes and entities that would ensure mutual cooperation of obligated institutions. However, this type of solutions is most often hindered by regulations requiring strict compliance with the confidentiality of financial information and relations with the financial intelligence unit, as well as personal data protection RODO [GDPR]. Developing a consensus in this area seems to be not only an urgent challenge, but also a desirable one. Moreover, two assessment regimes should be balanced and maintained. The first is basic and related to the assessment of risk and the application of financial security measures, individually by a given single obligated institution. The second one is related to the exchange of information between the obligated institutions and, as a consequence, the creation of a common SAR, which will consist of knowledge and monitoring carried out by more than one obligated institution. It seems that in such a situation, it is possible to adopt two basic solutions. The first one is when the legislator, in a specific act, develops provisions that may provide the basis for the so-called common SAR. In
such a case, it would be possible to adopt a solution in which the initiative for such a model of operation remains with the obligated institution, and its implementation (with the possibility of monitoring) is approved and influenced by the financial intelligence unit. This path was chosen by Great Britain and the Kingdom of the Netherlands. And the second solution, when the initiative in this respect remains with the financial intelligence unit, which at the same time reserves coordination activities in this area. It is also possible to provide a third solution, i.e. the introduction of national provisions enabling – depending on the assessment of the situation and other decisive factors – the possibility of implementing both variants of the models for achieving a common SAR. An alternative is to build a technical centre to which inquiries would be directed in an encrypted form, but this would result in a message that the same entity is interested in more than one institution. The message would be sent back to those institutions that expressed interest in this entity.

Moreover, it is necessary that the management of information whose processing is aimed at obtaining the effect of a common SAR is adequately protected against its disclosure or transfer to an unauthorised entity managing this information on behalf of the obligated institution. It should be considered whether it should be possible to entrust data processing on behalf of the obligated institution to an entity that is not part of the status-based countermeasure system – the obligated institution. You should also not undertake a construction that – as a pretext for performing AML/CFT tasks – would also enable the use of the acquired data for purposes other than those related to counteracting money laundering and financing terrorism. If obligated institutions are granted the right to jointly process data for the purpose of creating a common SAR, these institutions should perform this task jointly. The decision to outsource the execution of a joint SAR cannot be an excuse not to perform its own individual analyses of the recognition of ML/FT-related events. Additionally, obligated institutions should have the right to compensation in the event of providing incorrect or false information for the preparation of a joint SAR. Similarly, the entity to which the joint SAR applies should also have this right towards both the institution and the supporting external entity. The case concerns liability between the external entity and individual banks and between the banks/external entity and the client. After all, the client only has a relationship with a given obligated institution.

From an evidentiary point of view, it should be borne in mind that the findings made at the level of the obligated institution may subsequently be recognised as evidence and included in the files of the proceedings conducted by the prosecutor. Therefore, the issue of combining events, facts and traces of ML/FT perpetrators while adopting an individual approach of individual obligated institutions to customer/transaction risk without support from other obligated institutions at the level before submitting the SAR to the financial intelligence unit can only be implemented at the analytical level of this unit. Thus, the issue of combining events, facts and traces of ML/FT perpetrators while the individual obligated institutions
adopt unique approaches to client/transaction risk without support from other institutions obligated at the prior level, and transferring the SAR to the financial intelligence unit can only be implemented at the analytical level of this unit or in prosecutorial proceedings independently or in cooperation with other entities such as police or special services. As a consequence, analytical consistency will be possible to achieve at the level of financial analysis, criminal analysis, or tactics of prosecutorial proceedings. The introduction of the ‘Super SAR’ into this adopted structure should make it possible to shift (in terms of content and time) the issues of not only the recognition of ML/FT traces but also a broader association of events at the level of analysis of the obligated institutions. Unfortunately, this higher analytical level of suspicion will not be achieved without the cooperation of several obligated institutions. Hence, there are proposals aimed at building a common SAR based on the executive and analytical involvement of several obligated institutions.

However, the FATF should also consider the possibility of introducing a more universally applicable model of conduct. However, in this respect, its implementation only becomes more complicated. While it would be possible to create a situation in which, at the national level, individual entities of the AML/CFT system striving to develop a common SAR could develop organisational and legal conditions for the protection of fundamental rights, it would be difficult to develop substantive and basic provisions in this regard, e.g. exchanges of sensitive information between the EU and third countries. This could probably only apply to branches of obligated institutions based in countries third to the EU. The lack of supervision by the competent data protection authorities could violate the fundamental rights of EU citizens, but also be a temptation to use them outside the system (outside the AML/CFT system). Therefore, you should be very careful when planning this type of solutions. Moreover, the client’s behaviour model adopted on a risk-based basis should not be violated, for example, by financial intelligence units initiating analytical proceedings in a given and several obligated institutions for the purpose of creating a common SAR.

Taking into account the experience of individual countries in building common SAR systems, the Polish initiative of ZBP [Polish Bank Association] and KIR S.A. [National Clearing House], referred to as SCU-AML, also fits into this trend. Similar to solutions available in other countries, this initiative should also be assessed positively. Nevertheless, we cannot forget that it should operate on the basis of and within the limits of the law. Therefore, entities such as the GIIF [GIFI], the Inspector General for Personal Data Protection and the Polish Financial Supervision Authority should take official positions regarding this initiative. Obtaining a positive opinion from these three bodies should constitute the basis for implementing the SCU-AML project itself. Otherwise, an initiative similar to the solutions in Dutch legislation should be undertaken. Moreover, the low level of initiative on the part of the FATF in relation to complex and multi-entity transactions as elements of money laundering and terrorism financing chains is surprising. It seems that relying solely on two
advantages – i.e. individual risk assessment and, as a result, obtaining a partial effect in the form of a SAR report and the not entirely possible coordination of this information by the financial intelligence unit – does not make it possible to effectively obtain not only of a summary of information but also their coherent analysis in the light of the need to submit a notification of suspicion of committing a crime to the organisational unit of the prosecutor’s office. It should be noted that the current systemic solutions within AML/CFT focus on individual risk assessment, from which the institutional risk assessment is also derived. This individual approach even prevents a collective approach to risk assessment, which in its initial phase was negatively reflected in the derisking and debanking process.

It is clearly necessary to revise the existing solutions, which should remain the basis for counteracting ML/FT, but also critically evaluate the extreme lack of effectiveness in identifying the ML/FT phenomenon. Controlling administrative penalties alone is not a sufficient mechanism to stimulate effectiveness and further initiatives. Hence, one of the demands should be universal permission to build common SARs, taking into account the role of national financial analysis units. This state of affairs requires a change in the countermeasure paradigm, and thus a new assessment of the value of obligations created for the obligated institutions, especially focusing on the quality rather than the quantity of information and refraining from looking for various excuses to not carry out the institutional and individual risk assessment in these institutions.

It should also be borne in mind that the wide-ranging reform of the EU AML/CFT system that is being prepared is intended to make the rules for the use by obliged institutions of the Client Due Diligence (CDD) analysis already performed by other obliged institutions, as well as the rules for outsourcing CDD processes to third parties, more specific by issuing new regulations.

Despite the similarity of the AML/CFT principles to other similar system solutions in other areas, their effective implementation cannot remain indifferent. This means that a new countermeasure system cannot be implemented based only on the principle of compliance, but it must also meet the requirements of the principle of effectiveness. Therefore, as long as the SWIFT system operates and provides sensitivity to the American financial system, it remains the domain of superpower values in creating security policy. As a consequence, a new financial doctrine is being created – in the face of globalisation – which is the AML/CFT doctrine, depending on who defines a given entity or country as conductive to systemic changes and under what conditions. The mechanisms for building a common SAR also constitute a departure from global solutions in favour of national countermeasure instruments built at the level of implementing the AML/CFT obligations of obligated institutions.

In the context of building ‘Super SAR’, the issue of amending the Tax Ordinance Act\textsuperscript{54} should also be noted, in which Art. 119zu § 2a allows KIR S.A. to use data, including information from the Financial Information System, for the purpose of applying financial security measures by the clearing house, and to conduct and document the results of the current analysis of transactions referred to in Art. 43 section 3 of the P.P.P.F.T. Act. KIR S.A. may conduct activities for banks, cooperative savings and credit unions and obligated institutions, as well as for the activities necessary for the indicated entities to apply financial security measures and to conduct and document the results of the ongoing analysis of transactions referred to in Art. 43 section 3 of the P.P.P.F.T. Act.

References

13. Komunikat GIIF nr 35 w sprawie ogólnogrupowych procedur w zakresie AML/CFT oraz korzystania z usług podmiotów trzecich przy stosowaniu środków bezpieczeństwa finan-

\textsuperscript{54} Ustawa z 29 sierpnia 1997 - Ordynacja podatkowa (DzU, 2022, items 2651, 2707; DzU, 2023, items 180, 326, 511, 556, 614, 1059, 1193, 1234, 1450, 1598, 1705).


19. Raad van State opinion regarding: Wet plan van aanpak witwassen, Kamerstukken II 2022/23, 36228, No. 4. Electronic source: https://www.raadvanstate.nl/adviezen/a25338/w06-20-0354-.


30. Ustawa z 1 grudnia 2022 o Systemie Informacji Finansowej (DzU, 2023, item 180).

31. Ustawa z 1 marca 2018 o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU, 2023, items 1124, 1285, 1723, 1843).

32. Ustawa z 20 sierpnia 1997 o Krajowym Rejestrze Sądowym (DzU, 2023, items 685, 825, 1705).

33. Ustawa z 29 sierpnia 1997 - Ordnacjacja podatkowa (DzU, 2022, items 2651, 2707; DzU, 2023, items 180, 326, 511, 556, 614, 1059, 1193, 1234, 1450, 1598, 1705).

34. Ustawa z 29 sierpnia 1997 – Prawo bankowe (DzU, 2023, item 2488).

35. Ustawa z 6 czerwca 1997 – Kodeks karny (DzU, 2022, items 1138, 1726, 1855, 2339, 2600; DzU, 2023, items 289, 403, 818, 852, 1234, 1834).


**DOI:** 10.5604/01.3001.0053.9763  
**http://dx.doi.org/ 10.5604/01.3001.0053.9763**

**Keywords:** ‘Super SAR’, joint/cumulative SAR, report, money laundering, financing of terrorism, obligated institution

**Summary:** Obligated institutions report SARs to financial intelligence units as part of performing their obligations under the AML/CFT system. These actions are taken as a result of an individual customer/transaction risk assessment, as well as a countermeasure policy based on the analysis and assessment of institutional risk. Such structure of the behaviour of the obligated institutions was to be a counterbalance to potential and actual perpetrators of money laundering and terrorist financing crimes. As a consequence, individually obligated institutions were to recognise the components of a broad chain of perpetration and legalisation of funds originating from prohibited acts and constituting an element of camouflage of the source and beneficiaries of funds intended for terrorists. Over time, the ineffectiveness of this type of countermeasures began to be noticed, especially since the information provided to the financial intelligence units were positively verified and sent to the prosecutor’s office as notifications of suspected crime to a limited extent.

Subsequently, new counteracting schemes based on the participation of several obligated institutions and mutual exchange of information on negatively marked entities began to emerge. These concepts, even though they differ both in terms of content and technical implementation, constitute an important counterbalance to individualised analyses of risk created and assessed exclusively in a particular individualised obligated institution.

**Palabras clave:** "Súper ROS", ROS colectivo, informe, blanqueo de capitales, financiación del terrorismo, institución obligada

**Resumen:** Los informes de ROS a las UIF constituyen el cumplimiento de las obligaciones de las instituciones obligadas en virtud del régimen de PBC/FT. Dichas medidas se adoptan como resultado de la evaluación del riesgo de un cliente/operación individual, pero también de una política de prevención basada en el análisis y la evaluación del riesgo institucional. Esta construcción del comportamiento de las instituciones obligadas pretendía servir de contrapeso a los autores potenciales y reales de delitos de blanqueo de capitales y financiación del terrorismo. En consecuencia, cada una de las instituciones obligadas debía identificar a los componentes de una amplia cadena de delitos, legalizando los fondos procedentes de actos delictivos y formando parte del camuflaje de su origen y de sus beneficiarios con fines terroristas. Con el tiempo, se empezó a reconocer la ineficacia de este tipo de contramedidas, sobre todo porque la información facilitada a la UIF casi no se verificaba positivamente y se remitía a las autoridades fiscales en forma de notificaciones de sospecha. Sucesivamente, empezaron a surgir nuevos esquemas de contramedidas, basados en la participación de varias instituciones obligadas y en el intercambio mutuo de información sobre las entidades marcadas negativamente. Aunque estos conceptos difieren tanto en su contenido como en su aplicación técnica, representan un importante contrapeso a los análisis personalizados de los riesgos creados y evaluados exclusivamente en la institución obligada particular e individualizada.