Internal Security Review
2025, no. 33, pp. 347–390

https://doi.org/10.4467/20801335PBW.25.035.22652

ARTICLE

Behaviourist approach as the need to use methods based on recognising customer behaviour in support of the AML/CFT system

MACIEJ ALEKSANDER KĘDZIERSKI

Independent author

https://orcid.org/0000-0003-3074-1355

Abstract

Behavioural science, as a method based on the observation of behaviour, can be widely used to profile and identify clients of obligated institutions as potential perpetrators/suspects in money laundering or terrorist financing. This applies to both the assessment of the client's physical behaviour in the relationship with the institution and their online behaviour, e.g. within the scope of the online banking offer. In the first area, an approach based on psychology, sociotechnics and rhetoric also becomes useful. In the second case, the latest technological solutions based on artificial intelligence and traces left on mobile devices are used. The behavioural approach to the assessment of the client's behaviour, and thus the assessment of the risk associated with it, can be an element of a broader risk assessment. It is part of the client's relationship with the obligated institution as part of the legally required obligations to identify, verify and monitor its activity. The aim of this article is to confirm the thesis that, given the need to analyse risks and select financial security measures in a state of specific ML/FT threat, the obligated institution is required to take action to identify and recognise customer behaviour, taking into account behavioural factors.

Keywords

behavioural science, behaviour, obligated institution, risk, money laundering, terrorist financing

Introduction

Behaviourism is a branch of psychology that focuses primarily on observable behaviour rather than mental processes such as thinking and emotions. According to this theory, organisms learn through conditioning, which occurs as a result of interaction with the environment, and observable behaviours are responses to external stimuli. The behavioural approach can be applied in various fields of science, including security sciences. It can be used, among other things, in the area of anti-money laundering and countering the financing of terrorism (AML/CFT). In 2000, the Act on Counteracting Money Laundering and Terrorist Financing (hereinafter: the AML/CFT Act/2000) introduced – as one of the factors to be taken into account when analysing the level of risk in an obligated institution (hereinafter: OI) – the need to take into account a behavioural criterion consisting in unusual customer behaviour in a given situation (Art. 10a(3)(4) of the AML/CFT Act/2000)[1]. The introduction of this criterion stemmed from the belief that this 'atypicality' was caused by something. The reason for this could be that the organisation of money laundering or terrorist financing (hereinafter: ML/FT) could have an impact on the customer. However, this behaviour should be assessed from two perspectives – as a learned behaviour influenced by stimuli and as an intuitive behaviour (encoded in the mind as a result of past actions). The European Banking Authority (EBA) guidelines[2] in point 2.3(c) state that: (…) *institutions should take into account the risk associated with* (…) *the nature and behaviour of the customer and the beneficial owner, including whether this may indicate an increased risk of terrorist financing*. In this case, customer behaviour also means the manner of acting and/or conducting oneself, and not just the reaction itself.

---

1 *Act of 16 November 2000 on counteracting money laundering and terrorist financing*. In the *Act of 25 June 2009 amending the Act on counteracting the introduction into financial circulation of assets derived from illegal or undisclosed sources and on counteracting the financing of terrorism, and amending certain other acts*, a new provision was introduced in Art. 10a(3)(4), according to which: 'when conducting an analysis to determine the level of risk, the obligated institution should take into account, in particular, the following criterion: behavioural – consisting of unusual customer behaviour in a given situation'.

2 *Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849*, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016937/Guidelines%20ML%20TF%20Risk%20Factors_PL.pdf [accessed: 28 XI 2024].

Since risk should be measurable – in order to eliminate factors of uncertainty (they should be reduced to the level of probability) and develop measures to neutralise it – the behaviour of the institution's customer should also be included in a specific framework that will make it possible to be measured. Adopting a behavioural criterion as a reference to something measurable is important because customer behaviour should not be a factor that increases uncertainty (immeasurable uncertainty) and limits the ability to assess the risk posed by the customer (measurable probability). Adopting such an approach involves developing an individual risk value scale linked to the assessment of institutional and operational risk of the OI. The behaviour patterns of a specific customer should also be taken into account, such as: transaction frequency, average transaction value, transaction types and changes in transaction patterns over time, spending patterns and transaction location. These factors create conditions for capturing customer behaviour as measurable (the characteristics can be objectively converted into a mathematical algorithm, including the use of artificial intelligence, hereinafter: AI). At the same time, it is pointed out that risk is a psychological concept based on individual perception rather than empirical facts, which may make it difficult to assess the relationship between behaviour and risk level[3]. On the one hand, customer behaviour may be the result of specific stimuli related to the preparation for and commission of criminal activities, and on the other hand, a specific accumulation of these stimuli may individually characterise their externalised behaviour. The application of a behavioural approach in OI involves assessing behaviour in order to identify anomalies that may indicate an intensification of ML/FT risk (scale and dynamics)[4], as well as behaviour that reflects the phase of criminal activity (planning, reconnaissance, execution). In such an assessment, the OI representative will inevitably view the customer's behaviour from a criminological and forensic perspective and will analyse the risk in terms of the need to implement adequate financial security measures. The aim is not to determine the customer's sanity, but to assess their behaviour towards the OI. On the one hand, such an assessment by the OI takes into account the personality of the offender, their motivation and attitudes towards life, and on the other hand, the personality of the potential perpetrator of the criminal act from the point of view of the subject of the offence. It makes it possible to establish the mandatory signs

[3] P. Slovic, E.U. Weber, *Perception of Risk Posed by Extreme Events*, in: *Regulation of Toxic Substances and Hazardous Waste*, issue 2, J.S. Applegate, J.G Laitos, J.M. Gaba, N.M. Sachs (eds.), 2011.

[4] See: J.R. Meloy et. al., *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*, "Behavioral Sciences and the Law" 2012, vol. 30, no. 3, pp. 256–279. https://doi.org/10.1002/bsl.999.

of a crime, such as age, sanity, mental attitude towards the act (in this case, factors identifying ML/FT activities), etc.[5]

The research assumption adopted in the article is that the OI is required to analyse customer behaviour due to the need to assess risk and, as a consequence of this assessment, to select financial security measures in a state of specific ML/FT risk. The research objective is to highlight the need to revise the AML/CFT system in terms of risk analysis based on customer behaviour assessment.

The aim of the study is to describe a behavioural approach to risk analysis and the identification of customer behaviour as a potentially deviant behaviour that can be assessed negatively from an ML/FT perspective. The research problem identified not only the need to obtain behavioural traces for the purpose of preliminary assessment of the risk generated by the customer of the OI (this applies to initial customer – OI relations and preliminary risk assessment on the part of the customer), as suggested by the provisions of the AML/CTF Act/2000, but also the assessment of customer behaviour in subsequent relations with the OI, using products and services that classify customer behaviour as specific non-pattern-based behaviour. The research methods used included text analysis, literature review and assessment of behaviour based on the use of devices identifying customer relationships with the OI in order to obtain traces in the AML/CFT system, including through behavioural biometrics. The behavioural approach becomes a particular element of assessment, as the carriers of traces are physical entities – customers who are assessed for possible criminal behaviour.

The criteria for assessing customer behaviour should take into account, among other things: types of transactions, accounts and types of services and products offered by obligated institutions. Thus, the OI is obliged to develop a profile of the customer's activities and the nature and purpose of the OI's relationship with the customer. In the case of a customer associated with FT, it should be considered that if they act as an acolyte, supporter of terrorist methods[6] or perpetrator, they

[5] See in more detail: К.А. Викторович, Ш.О. Алексеевна, *Террористический акт: особенности уголовноправовой и криминалистической характеристик*, "Союз Криминалистов и криминологов" (K.A. Viktorovich, Sh.O. Alekseyevna, *Terroristicheskiy akt: osobennostiugolovnopravovoy i kriminalisticheskoy kharakteristik*, "Soyuz Kriminalistov i kriminologov") 2023, no. 1, https://crimeinfo.ru/wp-content/uploads/2023/08/2023-01.pdf, pp. 98–104 [accessed: 28 XI 2024].

[6] See: J.P. Bjelopera, *The Islamic State's Acolytes and the Challenges They Pose to U.S. Law Enforcement*, https://sgp.fas.org/crs/terror/R44110.pdf [accessed: 29 X 2025]; N.M.H. Al-Obaidi, *Motives of the Terrorism Phenomenon Among Youth and the Role of Laws in Dealing with It*, "Akkad Journal of Law and Public Policy" 2021, no. 4, vol. 1, pp. 182–197. https://doi.org/10.55202/ajlpp.v1i4.85. For the purposes of this article, the author has assumed that an 'acolyte' is a supporter of terrorism who, at some stage, wishes to become actively involved in terrorist activities. A 'supporter of terrorist methods', on the other hand, is a person who supports terrorist methods from a distance, e.g. by financing

are characterised by a set of beliefs that guide their behaviour and, in their opinion, justify it. The OI's observation of the customer's behaviour may help to reveal certain characteristics, e.g. support for terrorism, a propensity to use weapons, extremist views. The thesis of the considerations is as follows: in its risk assessment, the OI should take into account both psychological factors and the customer's observable behaviour. Only such an approach allows for a comprehensive assessment of a customer identified as a potential perpetrator of ML/FT offences. The question arises as to what extent the OI is able to properly assess the customer's behaviour, whether it is the result of an external stimulus or an expression of the functioning of their psyche.

The use of behavioural analysis in OI in the context of ML/FT risk assessment

Behavioural analysis allows employees of financial institutions to detect unusual behaviour patterns and anomalies in customer transactions related to both the deliberate use of products and/or services for criminal purposes and the creation of unusual ways of using products and/or services[7] offered by the OI (as a result of generalised analysis) as well as assessing the risk associated with the activities of a specific customer. Customer due diligence measures, including customer assessment and understanding of customer behaviour, play a key role in combating ML/FT. Furthermore, a behavioural approach, especially one based on verifying customer behaviour, remains consistent with the identification and verification of individual customers in the AML/CFT process, as well as in determining other causal behaviours related to predicate offences for ML and FT (e.g. fraud). Customer identification and verification are based on individualised behaviour and can be used to personalise products and/or services, and consequently to give the customer unique characteristics that will distinguish them from other customers (this scope does not apply to criminal behaviour). In this regard, the OI can use AI support. AI models can extract patterns and behaviours represented in transaction data and customer interactions and learn them, as well as process other relevant data. Conclusions from customer marketing profiling can be used to profile ML/FT perpetrators. In this regard, the assessment of behaviour aims to determine the degree of the customer's

them, publicly endorsing them, including on social media, and who wishes to remain anonymous to some extent.

7 The 'typical' pattern will be the manner of handling the product and/or service as established in the OI prior to their introduction to the market. This pattern includes using them within the limits of the law (e.g. statutes and internal regulations in the OI).

involvement in criminal activity and the factors that contributed to it. Behavioural analysis in the context of AML/CFT should be viewed as an assessment of behaviour that should appear unnatural in the circumstances and be associated with ML/FT, i.e. behaviour classified by the OI as suspicious. Suspicious behaviour refers to transactions or patterns of activity that are unusual or inconsistent with the known behaviour or profile of the customer (e.g. changes in transaction types, beneficiaries or methods of conduct without clear justification, deviating from regular patterns). For the purposes of undertaking the indicated risk assessment activities at the OI, it is necessary to introduce behavioural analytics[8]. The obligated institution should define a natural behaviour pattern for an individual customer (normal behaviour profile)[9] so that it can be compared with the pattern in question. A result indicating suspicious behaviour would signal potential risk and, consequently, the need to apply financial security measures. Behavioural analytics is responsible for analysing customer interactions, distinguishing patterns and, ultimately, the expected behaviour profile. It is possible to examine what stimuli influenced the customer, who, under their influence, does not follow the pattern based on the financial product offered. There are many opportunities to use machine learning-based methods for behavioural analysis and anomaly detection. They help identify patterns of financial crime by creating triage-level alerts based on risk levels and dynamic customer risk assessment. This assessment combines transactional behaviour with external data verification and existing rule-based alerts to calculate an individual risk score, as well as network analysis using large amounts of payment data to identify clusters of related accounts in the payment service providers' customer database[10].

---

8 Behavioural analytics is a field that involves collecting, measuring and analysing user data from digital channels (such as websites, applications and other online platforms) to understand how people interact and behave, and ultimately why they do so. The goal of this analysis is to discover patterns and trends in user motivations, preferences and behaviours, enabling organisations to make informed decisions, improve user experiences, optimise strategies and personalise offerings. See: E. Estevez, *Behavioral Analytics: Meaning, Types, Criticism*, Investopedia, 29 I 2023, https://www.investopedia.com/terms/b/behavioral-analytics.asp [accessed: 15 VII 2025]. In the case in question, the assessment of behaviour should be based on a much broader assessment field than just those related to digital channels. This is also related to conventional methods of delivering financial products and services with OI.

9 A normal profile may be the result of the adoption of standard product handling procedures at the OI and the customer's previous behaviour in the customer – OI relationship, which will be viewed positively by the OI. Thus, a normal profile will be the result of a combination of the general standard and a particularly positive assessment of individual behaviour.

10 R. Francis, L. He, *Managing money laundering risks in digital payments. How digital payment providers can combat financial crime*, OliverWyman, https://www.oliverwyman.com/our-expertise/insights/2023/oct/anti-money-laundering-strategies-for-digital-payment-providers.html [accessed: 15 VII 2025].

Initially, behaviourism was associated exclusively with observing the physical behaviour of customers in OI. Today, it is approached more broadly, e.g. it is used in biometrics to identify and verify customers based on their unique biometric characteristics. The original idea of behaviourism has also changed, and the cognitive-behavioural approach currently dominates. In the context of AML/CFT, this cognitive approach means combining the OI decision-maker's observation skills with an understanding of customer behaviour and up-to-date knowledge of ML/FT tactics. This will be supported by the use of behavioural criteria to ascertain the customer's knowledge of the service, how they use it, and their reactions and attitudes to commercial proposals (e.g. in terms of capital building, profit multiplication, investment diversification and financial investment). An analysis of the transaction patterns of a specific customer may prove to be a helpful tool. The material obtained allows for the classification of unusual behaviour, e.g. irregularities in terms of time or amount. In assessing customer behaviour in both traditional and online banking, factors such as divorce, death in the family, job loss, lack of social mobility, ethnic and ritual conditions (references to symbols, mysticism, repetitive behaviour) or experience of discrimination are important. The behavioural approach also applies to assessments based on observations of the 'stimulus-response' and 'reinforcement-punishment' mechanisms. In the first case, observations and assessments are limited solely to the customer's behaviour as the subject of assessment from the perspective of the Know Your Customer (KYC) procedure. This approach is insufficient. The assessment should be broadened to include issues related to the observation of the customer's behaviour, assuming that they may be acting under the influence of a prior stimulus (e.g. learned for the purpose of preparing to commit a crime). These stimuli may be independent of the customer, e.g. as a result of imitating observed situations associated with ML/FT, or dependent, e.g. as an action resulting from stimulation by an external entity (the organiser of the criminal activity)[11]. A typical relationship of this kind would be that between a front man and the organiser and/or instigator of criminal activity (for ML) or between a customer and a mentor or charismatic leader (for FT). In the latter case, it is possible to assess the client's behaviour when the reinforcement of behavioural stimuli comes from, for example, a sales advisor at a bank. It is also possible to observe the reaction of a customer who is keen to see the proposed transaction go ahead or who may wish to withdraw from it because it does not fit in with their usual pattern of criminal activity (e.g. due to an increased risk of traces of activity being detected, uncertainty about the achievement of the criminal objective, fears

[11] This type of behaviour was noticed by bank employees and involved setting up accounts for so-called front men for the purposes of tax carousels.

related to the failure to carry out the criminal enterprise and a negative reaction from its initiator). As part of ML/FT risk analysis, the behavioural approach can therefore be used to assess the risk associated with:

- customer behaviour, especially in relation to the OI[12],
- customer transaction behaviour[13].

Customers may experience various emotions and mental states, such as anxiety, fear and nervousness. Therefore, from a behavioural perspective, a linear[14], static approach to assessing customer behaviour may be insufficient. It is worth supplementing it with a dynamic approach, which seeks to identify determinants and stimuli that vary over time in order to influence the variability of the customer's behaviour and observe their behaviour over time, thereby revealing their actual motivations[15]. The risk of customer involvement in ML/FT is the sum of factors related not only to the customer as an individual, but also to the situation, environment and potential criminal objective. A dynamic approach to customer behaviour assessment will also be linked to changes in the financial market in which most OIs operate. It is also possible to provide a dynamic assessment of customer behaviour without interference from the OI. The observation of the 'stimulus-response' mechanism can be used both in direct contact between the customer and the OI representative and in online contact. It is also possible to deliberately and discretionally stimulate behaviour if the customer is monitored without their knowledge (this approach is permitted by the risk assessment and financial security

---

12 The bank representative should take into account behavioural factors that may indicate that the customer, for example, is under the influence of intoxicating substances, is not acting independently, or is not aware that they are entering into a relationship with the bank (they are not aware that the actions taken mean concluding a contract, e.g. for maintaining an account). See: *The position of the Polish Financial Supervision Authority on the identification of institutional customers and verification of their identity in the financial sector supervised by the Polish Financial Supervision Authority based on the video verification method*, https://static.fintek.pl/uploads/2022/03/Stanowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf, p. 5 [accessed: 28 XI 2024].

13 This scope may concern, for example, the frequency of transaction orders, their complexity, customer behaviour in the event of problems with their execution, failure to receive funds by the beneficiary of the order, use of specific transaction patterns – classified as high-risk patterns, etc.

14 See: *Comparison: Terrorist Financing, Money Laundering, and Financing the Proliferation of Weapons of Mass Destruction*, Jersey Financial Services Commission, 14 IV 2022, https://www.jerseyfsc.org/industry/guidance-and-policy/comparison-terrorist-financing-money-laundering-and-financing-the-proliferation-of-weapons-of-mass-destruction/ [accessed: 12 X 2025]; *Counter Proliferation Financing. Guidance Notes*, https://www.fsc.gi/uploads/CPF%20Guidance%20Notes.pdf [accessed: 12 X 2025].

15 For example, consistency in customer behaviour may indicate that they are managing a dormant account, while variability may indicate that they are directly involved in managing assets intended for use in preparing a terrorist act.

measures taken under AML/CFT). This approach is more effective in the case of a passive customer, and unnecessary in a situation where the customer shows initiative. Attention should also be paid to customers who do not commit primary offences but launder money from other offences as part of their otherwise legal activities. The customer's observed behaviour may be an expression of a desire to satisfy a need for security. The stimulus may be a failing business, the threat of unemployment, or even physical danger (blackmail, threats, danger to other family members)[16]. A psychological assessment by the OI should be conducted on such a customer, who may be both the perpetrator and the victim, in order to gain knowledge about the real reasons for the suspicious behaviour and the real initiator. This type of behaviour may be manifested as desperate when the client acts under the influence of nervousness, a lack of realistic assessment of the threat, or a desire to maintain positive relations with the OI. The client may exhibit surprising behaviour in the OI's assessment, make unnecessary changes to their current business profile, make irrational decisions, or opt out of services that may be associated with excessive supervision by the institution.

The behavioural approach can also be used to distinguish between 'normal' and 'criminal' customers. In this regard, it is important to observe the customer's marketing behaviour in the OI. 'Normal' customers are most likely to choose products or services that maximise the value they receive. Value for the customer is sometimes defined as the sum of the utility offered to the buyer. The value delivered to the customer is the difference between the total value of the product to the customer and the cost they must incur to obtain it. It is therefore a specific financial calculation[17]. For a 'criminal' client, this cost is included in the price of the original crime. Often, ML offences involve some loss of assets in order to legalise the remainder, including those obtained illegally. This is primarily the cost of investing funds both to recover them from the acquired assets and to multiply them. The profit in this case is the legal status of the funds, which can be reinvested (operating costs of criminal profit). In this case, the price criterion is shifted outside the OI (especially when the OI is commercial in nature). What becomes important,

---

16 D. Thomas, *Profiling Part 1: The Psychology of Anti Money Launderers*, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/white-paper/the-psychology-of-money-launderers.pdf [accessed: 28 XI 2024].

17 R. Wolniak, B. Skotnicka-Zasadzień, *Wybrane metody badania satysfakcji klienta i oceny dostawców w organizacjach* (Eng. Selected methods for measuring customer satisfaction and evaluating suppliers in organisations), https://www.researchgate.net/profile/Radoslaw-Wolniak/publication/41199963_Wybrane_metody_badania_satysfakcji_klienta_i_oceny_dostawcow_w_organizacjach/links/5ab63b2ba6fdcc46d3b45829/Wybrane-metody-badania-satysfakcji-klienta-i-oceny-dostawcow-w-organizacjach.pdf, p. 31 [accessed: 18 XI 2024].

however, is the criterion of the functionality of the product and/or service, which should be linked to the characteristics of the direct use of the product. This assessment can be combined with the temporary dysfunctionality of generating profits from the client's assets, visible to the OI. Functionality should be seen as an assessment of the client as a perpetrator using a particular product and/or service to achieve the intended criminal objective. The behaviour of the customer as a perpetrator also becomes a configuration of non-economic activities that can be classified in the non-institutional economic and administrative space (this applies, for example, to consumer behaviour)[18]. Certain customer behaviour may be related to a decision to carry out a terrorist attack (e.g. urgent request to terminate an account agreement, transfer of funds to family members, order to transfer funds to a radical organisation, difficult contact between the OI and the customer). Observation and assessment of customer behaviour also provide insight not only into their initial attitude, but also into the radicalisation of their views, which may lead to the use of force as a behavioural consequence of radicalisation. Therefore, the transition from cognitive radicalisation to behavioural radicalisation may also be considered. This should be borne in mind when financing terrorism and the organisation of terrorist crimes themselves. A change in a customer's behaviour in relation to the OI may be the result of changes in their personality under the influence of radical ideas[19].

The temporal (time) factor can be used as a distinguishing feature for classifying customer behaviour as inappropriate. For example, there may be a temporal dysfunction of the costs and profits of observable assets or a temporal dysfunction of the customer's past and present activities. In addition, it is possible to infer unusual behaviour based on the temporal dysfunction of transaction orders when there is no logical explanation for their nature. Another factor shaping customer behaviour as a perpetrator may be economic and financial knowledge, which distinguishes perpetrators of economic crimes similar to ML/FT crimes

---

[18] *Major factors influencing consumer behavior*, Clootrack, https://www.clootrack.com/knowledge-base/major-factors-influencing-consumer-behavior [accessed: 18 XI 2024]. Purchasing decisions are influenced by factors such as the buyer's age, income and occupation, their attitude towards specific products or services, social media, cultural norms, traditions and values.

[19] The European Commission identifies factors that contribute to radicalisation. These include: individual factors (such as feelings of alienation, injustice, victimisation), social factors (social exclusion, actual or perceived discrimination, limited social mobility), political factors (views on the effects of political actions, events and conflicts), ideological and religious factors, cultural factors (cultural marginalisation, solidarity with a particular ethnic/religious group), the activities of radicals and recruiters, including for terrorist or extremist groups, and the influence of social media. See: M. Ranstrop, *The Root Causes of Violent Extremism*, Brussels: European Commission, 2016, in: J. Mazurczak, *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu*, "Miscellanea Anthropologica et Sociologica" 2020, no. 21(2), pp. 45–73.

in particular. Economic and financial knowledge allows perpetrators to use it in theory or in practice to organise crimes. Particularly in OIs in the financial and economic sectors, it will be possible to observe and assess the degree of skill and professionalism in committing ML/FT offences. Perpetrators of economic and financial crimes differ from perpetrators of other types of crimes due to certain characteristics. They are familiar with the regulations governing their professional field and exploit certain legal loopholes, ambiguities and frequent changes in regulations to operate on the fringes of the law[20].

It is also possible that an OI employee could conduct a behavioural interview with the customer, which – similar to a psychological assessment – would allow the OI decision-maker to decide on further action in risk assessment. This situation could apply to both terrorist acolytes (supporters) and self-organising terrorists (e.g. lone actors or copycats). An approach based, for example, on behavioural learning theory[21] and cognitive theories would be helpful here. The purpose of such an interview would be to establish correlations between the observed behaviour in the customer – OI relationship, rather than to formulate an assessment based on a coincidental approach. The behavioural interview used as part of KYC would aim to identify factors such as individual socio-psychological factors, social and cultural factors, and, when the OI uses open sources of information, also assess the influence of social media[22].

Requirements related to the behavioural approach within AML/CFT

The current provisions of the 2018 Act on Counteracting Money Laundering and Terrorist Financing[23] (hereinafter: the AML/CFT Act/2018) do not explicitly indicate the need to take customer behaviour into account when assessing risk factors. Nevertheless, this is indirectly indicated by the provisions of the Act relating to the gradation of financial security measures. Obligated institutions should build behavioural profiles of their customers for the purposes of risk assessment and the application of financial security measures. However, the OI's approach should

20 K. Milanovic, *Money Laundering and Other Forms of Financial Crime*, "Journal of Law and Politics" 2024, no. 5, pp. 57–78. https://doi.org//10.69648/JJDU2862.

21 For example, Albert Bandura's social cognitive theory. See: A. Bandura, *Teoria społecznego uczenia się* (Eng. Social learning theory), Warszawa 2007.

22 See in more detail: J. Mazurczak, *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu* (Eng. Radicalisation as a process leading to extremism and terrorism), "Miscellanea Anthropologica et Sociologica" 2020, no. 21(2), pp. 45–73.

23 *Act of 1 March 2018 on counteracting money laundering and terrorist financing.*

focus in particular on behavioural analysis (in this case, let us assume an assessment of the customer's external behaviour resulting from both internal and external impulses), and not solely on the analysis of customer behaviour (in which the only subject of assessment is their externalised behaviour as a result of an external impulse arousing emotions)[24]. It is also important to pay attention to the behaviour of customers who request unusual transactions or transactions without obvious reasons, as this may indicate an attempt to misuse the OI product or service for the purpose of ML or FT. The OI representative should pay attention to: the customer's nervousness when asked detailed questions about their business activities; the customer's lack of knowledge about their business activities; the customer's ignorance of the law and technical conditions in an area closely related to the purpose of the transaction; the customer's intoxication when in contact with the OI representative; attempts to hide the face; the customer coming to the OI accompanied by third parties and remaining passive in this situation; unusual transport of cash (plastic bags, travel bags, etc.)[25]. When profiling a potential suicide bomber, characteristics such as nervousness, sweating, drug-like behaviour, dilated pupils, dull eyes, agitation and incoherent behaviour are noted[26]. The following may also be suspicious: unusual

---

[24] Behavioural analysis combines the assessment of external behaviours (so-called public behaviours, i.e. those observable from the outside) and internal behaviours (so-called private behaviours, i.e. those accessible only to the person experiencing them; these include emotions, physiological reactions of the body and thoughts). It also includes the interpretation of behaviours and understanding their causes. Behaviour analysis (derived from radical behaviourism), on the other hand, focuses on direct observations and measurements of specific activities. Three branches of behaviour analysis have emerged: experimental analysis of behaviour, applied behaviour analysis, and conceptual analysis of behaviour. Consequently, contrary to what most psychological concepts claim, private behaviours such as thoughts or emotions cannot be the cause of public behaviours, as they themselves require explanation in terms of cause and effect. See in more detail: P. Bąbel, *Terapia behawioralna zaburzeń rozwoju z perspektywy analizy zachowania* (Eng. Behavioural therapy for developmental disorders from the perspective of behaviour analysis), "Psychologia Rozwojowa" 2011, vol. 16, no. 3, pp. 27–38. https://doi.org/10.4467/20843879PR.11.016.0189. In Poland, the terms behavioural analysis and behaviour analysis are treated as synonyms. For the purposes of this article, the author has adopted the distinction indicated between these concepts.

[25] M. Hara, R. Kierzynka, P. Kołodziejski, *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz* (Eng. Act on Counteracting Money Laundering and Terrorist Financing. Commentary), issue 1, legal status as of 12 May 2013, Warszawa, p. 126.

[26] K. Liedel, *Profilowanie sprawców przestępstw terrorystycznych* (Eng. Profiling perpetrators of terrorist offences), in: *Profilowanie kryminalne*, J. Konieczny, M. Szostak (eds.), Warszawa 2011, p. 199. This type of behaviour should be considered in the case of self-financing suicide bombers. Research conducted by Ariel Merari shows that most suicide bombers did not exhibit any of the risk factors associated with suicide, such as mood disorders, schizophrenia, substance abuse or previous suicide attempts. See in more detail: A. Merari, *Academic research and government policy on terrorism*, "Terrorism and Political Violence" 1991, vol. 3, pp. 88–102. This research result can be explained by

transaction patterns, e.g. when a customer buys identical items or makes several purchases for the same amount; changes in location, e.g. when a customer logs in from a new country or region (it is particularly suspicious when a customer logs in from a high-risk third country[27]); suspicious login attempts, e.g. when a customer changes their password several times or fails to log in, the customer exhibits unusual typing patterns or touch gestures; changes in user information, e.g. when a customer provides a new shipping address, phone number, payment method, etc.[28] The examples provided may suggest that behavioural criteria in ML/FT risk assessment serve not so much to build a psychological profile as to assess behaviour that may indicate a contradiction between the declared purpose of the relationship and its hidden criminal purpose. Based on a dynamic risk assessment, the OI may also draw conclusions about changes in the behaviour of a customer who is identified as a person providing assistance to terrorists. Consequently, the conclusions may concern changes over time in the type of assistance provided to terrorists, or its reduction or intensification. This, in turn, may indicate the selection of a location for an attack, the preparation of a terrorist act, or a geographical change in the organisation's activities. An individual behavioural profile of the customer should be developed as part of KYC[29]. What is important is that this data can only be generated by the customer and through their involvement in the relationship with the OI. The perpetrator of criminal activities may also be a third party who is not a customer of the OI (e.g. an instigator, terrorist accomplice, beneficial owner, person controlling a business entity involved in financing terrorist activities), under whose influence the customer may act. In such a case, the customer will play the role

the fact that suicide bombers are not ultimately interested in committing suicide, because their goal is to realise an idea: martyrdom, religious or social.

[27] Pursuant to Art. 2(2)(13) of the AML/CFT Act/2018, a high-risk third country is understood as: 'a country identified on the basis of information from reliable sources, including reports on the evaluation of national anti-money laundering and counter-terrorist financing systems carried out by the Financial Action Task Force (FATF) and its affiliated bodies or organisations, as not having an effective anti-money laundering or counter-terrorist financing regime or having significant deficiencies in its anti-money laundering or counter-terrorist financing regime, in particular a third country identified by the European Commission in a delegated act adopted pursuant to Art. 9 of Directive 2015/849'. See: *Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies*. For example, such countries include North Korea, Iran, Algeria, Angola, Côte d'Ivoire, Kenya, Laos, Lebanon, Monaco, Namibia, Nepal and Venezuela.

[28] O. Skrebneva, A. Abramova, *Why Behavioral Analytics is Key to Fraud Detection Today*, The Sumsuber, 14 V 2024, https://sumsub.com/blog/behavioral-analytics/ [accessed: 24 XI 2024].

[29] As a result, a pattern of normal customer behaviour is established, which is obtained by assessing the customer's transactional behaviour in previous monitoring periods by the OI.

of a so-called front man ('mule')[30], a subsidiary entity, and sometimes a third party will direct their behaviour. In this case, the customer's behaviour should be assessed in terms of how autonomous it is and to what extent it has been dictated by the OI. When defining unusual and unjustified transactions and customer behaviour, the OI representative should take two aspects into account:

- unusual or unjustified behaviour of the customer in the context of the product or service offered or in the context of the type of customer,
- unusual or unjustified nature of the customer's behaviour in relation to the information that OI has about them[31].

The assessment of customer behaviour is part of a broader customer control process in a given OI and may be part of customer profiling. When considering the fulfilment of the OI's obligations, it should be assumed that the institution operates in accordance with the provisions of the AML/CFT Act/2000, i.e. situations in which, for example, a representative of the OI knowingly cooperates with a customer in criminal activities are not considered.

When examining customer behaviour in the context of the AML/CFT system, the following factors should therefore be taken into account:

- natural human behaviour resulting from education, environment, illness, experience, etc.;
- consciously 'artificially' created human behaviour resulting from learning a pattern of behaviour, imitation, the desire to be different, identification with a specific real or fictional character[32];

[30] The recruitment of 'money mules' usually takes place online. Criminals tempt them with easy money and describe the 'job' as safe and uncomplicated. Such offers mainly target people looking for quick income. These people often do not realise that they are participating in illegal activities and that their bank account is being used as a tool for money laundering. See: *„Muły finansowe" – ukryte zagrożenie w świecie bankowości online* (Eng. Financial mules – a hidden threat in the world of online banking), prnews.pl, 2 XII 2024, https://prnews.pl/muly-finansowe-ukryte-zagrozenie-w-swiecie-bankowosci-online-481242 [accessed: 12 X 2025].

[31] *The definition of unusual and unjustified transactions from the perspective of the risk of money laundering and terrorist financing*, https://www.cnb.cz/export/sites/cnb/en/faq/galleries/definition_of_unusual_and_unjustified_transactions_from_the_perspective_of_the_risk_of_money_laundering_and_terrorist_financing.pdf [accessed: 14 III 2024].

[32] Within the context of functioning in a terrorist group, such behaviour may be a socio-psychological result consistent with the process of radicalisation, which includes: in-group and/or out-group, conformity, compliance, groupthink, group polarisation and diffusion of responsibility. See in more detail: D. Aziz Sbeih, *Which Group has a More Sustainable Model of Terrorism*, https://washingtoncollegereview.files.wordpress.com/2019/09/sbeih_which-group-has-a-more-sustainable-model-of-terrorism-al-qaeda-or-isis.pdf [accessed: 24 XI 2024].

– specific customer behaviour in a situation that may indicate their involvement in an ML/FT event (this includes both inspiration to commit a crime and preparation for a crime, including its financing)[33].

Thus, for AML/CFT purposes, behavioural factors can be distinguished that characterise:

– both standard and non-standard customers (customer behavioural factors), e.g. behavioural factors characteristic of customers purchasing eco-friendly buildings on credit (e.g. as consumer behaviour);
– criminal clients (behavioural factors of a criminal client), including behavioural factors of the client of money laundering and terrorism financing[34].

ML/FT risk assessments assigned during onboarding should be updated. A static approach means that even if a customer's behaviour changes, e.g. if they switch from domestic to international transfers or become involved in high-risk sectors, they may still be treated as a low-risk customer. For customer behaviour that changes over time, a dynamic ML/FT risk analysis should be recommended. This approach should be appropriate to changes in the customer's personality and external factors. This variability over time may indicate that the customer is involved in illegal activities. According to the UK Financial Conduct Authority (FCA), risk scoring models should take into account emerging threats, changes in customer behaviour and updates to the regulatory framework[35].

New customers who want to enter into a relationship with an OI in order to commit crimes may behave in a specific manner, e.g. avoid contact with the institution or minimise it significantly. In the case of online services, an institution that suspects unusual behaviour should introduce other types of factors to identify such behaviour. Such behaviour may include: failure to answer questions about

[33] This issue may be relevant in the case of so-called lone wolves, i.e. terrorists acting alone, without links to an organisation or sponsor. This means that the client fulfils two conditions – being both the inspirer and the executor of the model of behaviour towards the OI.

[34] For AML/CFT purposes, behavioural analysis may be extended to include analysis of IO employees, especially in the context of their potential involvement with customers in money laundering. See: *Act of 6 June 1997 – Criminal Code*, Art. 299 § 2: 'The penalty specified in § 1 shall be imposed on anyone who, being an employee or acting on behalf of or for a bank, financial or credit institution or other entity which is required by law to register transactions and persons conducting transactions, accepts, contrary to the provisions, means of payment, financial instruments, securities, foreign exchange, transfers or converts them, or accepts them in other circumstances giving rise to reasonable suspicion that they are the subject of an act specified in § 1, or provides other services to conceal their criminal origin or services to protect them from seizure'.

[35] *Guidance for a Risk-Based Approach the Banking Sector*, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf [accessed: 20 I 2025].

the customer or their company, failure to specify the ultimate (actual) beneficiary, customer embarrassment, nervousness, the need for immediate consultation with a third party, or even threats regarding the violation of the customer's fundamental rights and the consequences of such behaviour. The institution should consider whether this is suspicious, especially if the customer may have criminal connections or unusual knowledge of the ML process.

As Jacek Grzywacz notes, customer segmentation is also possible by understanding how the buyer perceives the offer: *Using this criterion, it is possible to determine the customer's reaction to the price of financial services, their willingness to take advantage of so-called special offers, and their preferred method of service distribution (e.g. via electronic banking)*[36]. Taking into account the purpose of the offer and the customer's needs, their behaviour can be compared with the offer template adopted in the OI, in terms of meeting the needs and objectives in accordance with the model of the instrument introduced to the financial market, and actions inconsistent with its intended use and declared purpose. In this way, a set of unusual customer behaviours (consumer judgement) is created, which should be identified in the context of AML/CFT. In the case of so-called remote identification, which mainly concerns information, documents and data that the customer will use in their relationship with the OI, the assessment factor in the form of the customer's behavioural reactions is lost. Remote operation allows the customer to be monitored in terms of how they use mobile devices, e.g. how they log in, mistakes in entering codes, speed and manner of typing characters in correspondence with the institution.

Using a behavioural approach to identify unusual customer behaviour

The examination of the behavioural 'trace'[37] left by the customer, both at the level of direct, physical relations with the OI and at a distance, remains an important element of the behavioural approach in AML/CFT. The customer behaviours assessed include: reluctance to provide identification data or providing it in a limited manner, this also applies to representatives; agreeing to high penalties; making transactions without logical justification; ordering transactions after obtaining

[36] J. Grzywacz, *Segmentacja na rynku usług bankowych* (Eng. Segmentation in the banking services market), "Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne" 2014, vol. 20, p. 44.

[37] See in more detail: K. Olszak-Häußler, *Rozumienie pojęcia „ślad" w ujęciu profilowania kryminalnego* (Eng. Understanding the concept of 'trace' in criminal profiling), "Problemy Kryminalistyki" 2016, no. 291, pp. 7–11.

funds from unknown or difficult to determine sources[38]. Any changes in objective reality that bring them closer to a forensic assessment will be traces of OI activities. The obligated institution does not use, for example, a polygraph, so it should ensure that it is able to reveal and identify traces of behavioural patterns in order to identify the customer and obtain knowledge about them. Importantly, if the customer becomes active, it will be necessary to assess their sense of effectiveness in committing the crime or their perceived control over their behaviour. The temporal correlation between the action and the commission of the crime may be an important distinguishing factor, as well as the assessment of the psychological connection with the crime expressed in the behaviour of the client-perpetrator[39]. This may be, for example, an indifferent attitude accompanying the stage of preparation for committing a crime, e.g. by signing a bank account agreement, considering offers of services related to this account, or as a relationship with the OI in a state of internal consultation. The customer's behaviour may be different if they are concerned about the time of service delivery, the speed of the transfer, the execution of an occasional transaction, especially if there are additional factors increasing the risk in this respect, e.g. transfer of funds to a third EU country, a country neighbouring terrorist activity or a country identified with a weak legal security system and a high level of crime risk. In this regard, the client's ability[40] to carry out negative actions should also be taken into account. Importantly, although the OI should aim to identify irregularities in order to prove an offence under Articles 299 and 165a of the Criminal Code[41], there is no mention of the need for the OI to demonstrate, let alone prove, the guilt of the customer – the potential perpetrator. Thus, the institution investigating the customer's behaviour is not subject to criminal proceedings. Therefore, it may investigate the behaviour of the customer and/or perpetrator, including characteristics unrelated to the legal interest protected by the sanctioned norm underlying this type of prohibited act. With regard to the findings of the OI, the legislator currently refers explicitly to circumstances that may indicate suspicion of a crime, rather than to the guilt of the customer identified as the perpetrator (Art. 74(1) of the AML/CFT Act/2018). Guilt should be considered in relation to the prohibited act, not to the personality traits, character

[38] *Risk assess your business for money laundering supervision*, Gov.UK, 23 X 2014, https://www.gov.uk/guidance/money-laundering-regulations-risk-assessments [accessed: 18 XI 2024].

[39] Human behaviour must manifest itself in objective reality.

[40] One of them may be the customer adopting an attitude that they can mislead the OI representative as to the real motive for establishing a relationship with the institution. Here, too, malicious activity can be identified using what is known as rule-based detection, in which observed events are matched to known patterns of threatening behaviour.

[41] *Act of 6 June 1997 – Criminal Code.*

and lifestyle of the client and/or perpetrator. Circumstances indicating suspicion of a crime may also include an assessment of these elements, provided that they serve to identify suspicious activities. Furthermore, they need not be limited to the time of the offence, but should take it into account as a point of reference. The assessment focuses on the client's behaviour and only then on what they did or could have done. Punishable behaviour in the strict sense is specified in Art. 299 § 1 of the Criminal Code:

> Whoever accepts, possesses, uses, transfers or exports abroad, conceals, transfers or converts, assists in the transfer of ownership or possession of, or takes other actions that may prevent or significantly impede the recovery of means of payment, financial instruments, securities, foreign currency, property rights or other movable or immovable property derived from the proceeds of a prohibited act, shall be subject to imprisonment for a term of between 6 months and 8 years.

and in Art. 165a § 1 of the Criminal Code:

> Whoever collects, transfers or offers means of payment, financial instruments, securities, foreign currency, property rights or other movable or immovable property with the intention of financing a terrorist offence or an offence referred to in Articles 120, 121, 136, 166, 167, 171, 252, 255a or 259a shall be subject to imprisonment for a term of between 2 and 15 years.

These behaviours were treated differently due to the purpose of the crime. In the case of ML, it is to ensure the legality of income from prohibited activities, and in the case of FT, it is to transfer funds to a terrorist beneficiary (especially another entity), with self-financing being an exception. Hence, ML is considered to be cyclical in nature, while FT is considered to be linear[42].

In connection with these considerations, a division into behavioural science concerning:

– criminal offence – assessment of a person's behaviour in terms of committing a criminal offence (Art. 299 of the Criminal Code, Art. 165a of the Criminal Code) as fulfilling the objective aspect of the offence;
– suspicious relationship – assessment of a person's behaviour in relation to the OI, indicating circumstances suggesting ML/FT or handling of assets

[42] *Comparison: Terrorist Financing, Money Laundering, and Financing…*; *Counter Proliferation Financing. Guidance Notes…*

in a manner that justifies the suspicion that a specific transaction or assets may be related to ML/FT;

– services and/or products provided, excluding the two previous items. This applies to behaviour towards supervised and unsupervised entities or registered and unregistered services, e.g. relations with a representative of a hawala service provider.

The assumption behind the use of customer behavioural assessment may be that the behaviour of perpetrators of ML/FT is recognisable and repeatable. The aim of ML is to legalise funds derived from a prohibited act, while in the case of terrorist financing, the aim is to support terrorist activity. We may therefore encounter similar behaviours, and in some phases of the activity, these behaviours may be identical for ML and FT. It is therefore difficult to identify a specific distinguishing feature that could alert decision-makers in the AML/CFT division and units cooperating in the OI to the possibility of criminal activity. A distinguishing feature in this regard may be the behavioural assessment of the customer as a perpetrator. However, while the scenarios and tactics are known and may even be predictable, perpetrators differ significantly in terms of their individual characteristics (no two people have the same personality traits) and the incentives that drive them. Perpetrators may use a specific set of tools, but this is combined with other types of actions they take (dominated by individual characteristics). This distinguishing and individualising feature of the customer's personality can reveal the customer's involvement in the process and also help to monitor their behaviour remotely. Consequently, the OI will have to obtain knowledge about the customer's behaviour that provides a behavioural pattern as part of KYC. This approach can be helpful especially when the customer – OI relationship is expected to last for a long time and when the OI has offered the customer a product available online. Obtaining behavioural KYC, especially taking into account disorders, may be useful for identifying a customer as a terrorist who may be planning to self-finance their act (e.g. seeking a high level of autonomy in their relationship with the OI and in the management of the products or services made available to them). In such a case, an unknown perpetrator is sought, but behavioural observation may allow the risk to be identified. An indicator of risk is, for example, the customer's activity on internet forums dedicated to spreading extremist behaviour.

A good practice preceding the assessment of the behaviour of customers identified as potential ML/FT perpetrators would be to learn about the psychological mechanisms related to the sale of products offered by a given OI[43]. This will enable

[43] See in more detail: A. Falkowski, T. Tyszka, *Psychologia zachowań konsumenckich* (Eng. Consumer behaviour psychology), Gdańsk 2001.

the institution's representative to know how standard customers should behave towards the products offered and to recognise deviations from established sales patterns. To this end, tests can be performed, e.g. the DISC test[44], which covers four main categories according to which a person can be analysed. These are behavioural styles:

1) dominant – this describes how people view challenges and obstacles. People with this trait are goal-oriented and have strong opinions,
2) influential – characterises people who are confident and open to ideas. Such people influence their environment – they inspire others with their ideas,
3) stable – indicates how a person reacts to their environment. People with this trait are good listeners, calm and value consistency,
4) conscientious – indicates how people react to a given situation. Such people are analytical and base their decisions primarily on knowledge and facts[45].

Every person is a combination of these traits to varying degrees. By recognising the signals coming from potential customers, you will be able to understand them better and establish better contact with them. It is important to identify the determinants that influence customer behaviour as perpetrators. Comprehensive application of KYC will allow you to build a specific area of movement within customer recognition, thus making a behavioural approach easier. It will focus exclusively on the relationship between customer behaviour and identifying the customer as a perpetrator of a crime (identifying the customer as involved in circumstances that may indicate suspicion of ML/FT or raising reasonable suspicion that their actions are aimed at using funds and/or transactions for ML/FT). The activities of the OI are aimed at recognising the configuration of events and the customer's participation in them and are carried out in connection with the need to determine the risk of unlawful behaviour and to draw conclusions which, in the form specified by law, must then be forwarded to the financial intelligence unit. It is important to eliminate from the assessment those determinants of the perpetrator's suspicious behaviour that are related to other causes (e.g. sociopathic behaviour, low self-esteem, intellectual disability, depression, medication use, etc.) and do not qualify the customer as a potential perpetrator of ML/FT offences. Ultimately, only those

[44] DISC (*dominance*, *inducement*, *submission*, *and compliance*) is a model of four behavioural styles developed on the basis of research by American psychologist William Marston.

[45] H. Sekar, *Recognize Your Customers: A Complete Guide on Customer Behavioral Cues and Building Customer Relationships*, 8 VII 2019, https://www.freshworks.com/freshdesk/customer-engagement/customer-behavioral-cues-building-customer-relationships-blog/ [accessed: 12 III 2024].

determinants that can be linked to the perpetrator's unusual behaviour, qualifying him or her as a suspect in criminal activity, remain to be assessed. The decision-maker in the OI should strive in behavioural KYC to retain only those determinants that are relevant to the perpetrator's behaviour and are considered suspicious. The rest may be the result of various circumstances, lack of experience or shyness, illness, low level of education, or lack of knowledge about market mechanisms. However, they will not be causally related to the role that the customer plays in ML/FT. In view of the above, it can be concluded that the perpetrator may be a person who:

- has characteristics associated with the effective commission of ML/FT offences using products or services offered by the OI,
- originates from criminal circles (and thus exhibits certain antisocial behaviours), who was used to carry out ML/FT activities,
- is not in conflict with the law, who was chosen to play an active role in ML/FT due to personality traits,
- self-fulfils in the role of both the perpetrator and the financier of the crime.

In order to gain insight into a customer's propensity to act under the influence of specific factors (e.g. income, financial resources, financial situation, preferences, promotions, but also individual character traits and disposition), it is essential to engage in conversation with them. This will allow you to learn not only about their expectations towards the OI, but also to predict their behaviour as a potential partner in relations with the institution. An OI representative may have an advantage over the customer because they should be more familiar with the products or services offered and know their attributes[46], in accordance with the commercial and business policy objectives[47] adopted by the OI. This can help them assess the customer and draw conclusions about their behaviour when making an offer. Experience in sales psychology and customer conversations will also be helpful. The monitoring entity should have the knowledge to assess the customer's individual predisposition to ML/FT. The conversation should reveal his motive for establishing a relationship

[46] Attributes are specific characteristics of a product that are used to describe and classify it, but do not directly affect its price or availability. In the case of financial products, characteristics such as risk, duration, potential benefits, rate of return and type of instrument (e.g. shares, bonds, deposits) are taken into account, which distinguish it from others and allow its value to the customer to be assessed. In addition to the specific characteristics of the product, its perception is also influenced by intangible attributes, such as brand image and customer service quality. See: Di Wu, Xuhui Li, *A Systematic Literature Review of Financial Product Recommendation Systems*, "Information" 2025, no. 16. https://doi.org/10.3390/info16030196.

[47] Refers to the actions of companies that aim to increase their profits by, for example, aggressively promoting products or setting prices.

with this type of OI and obtaining access to a specific product or service. In the presented customer – OI relationship, it is also important that the OI does not make the mistake of making an inappropriate offer to the customer that does not meet their expectations. The consequences of such an OI error can be classified as inappropriate customer behaviour. Customer selection may also have economic grounds, but in the case of ML/FT activities, it will be motivated, for example, by the possibility of providing a limited amount of personal and other data that more broadly identifies the customer, the institution's limitations in accessing databases that would allow for more in-depth verification of the customer, the possibility of quick transfer of funds both domestically and abroad, the possibility of using a package of various services, extensive possibilities of disposing of funds without the need for physical presence at the institution's premises, the type of customers served with whom the customer identifies or whose behaviour they emulate, and negative opinions about the institution posted in public and social media.

Criminal behaviour is seen by behaviourists as a learned response to environmental stimuli, rather than the result of innate personality or character traits. These behaviours are reinforced by rewards such as gaining money or power, or avoiding negative consequences such as punishment or social disapproval[48] (inducing someone to commit a crime in exchange for a specific amount of money or a share of the profits is no exception). This approach is linked to an important assumption of behaviourism, which is the external controllability of human beings. Therefore, within the framework of AML/CFT, it is necessary to assess whether the entity in a relationship with the OI is who they claim to be, whether they are acting of their own free will, or whether another entity is behind their actions. This may be the case when a person pretends to be someone else (e.g. as a result of data theft), when a crime is committed by a so-called front man, and when a silent partner or actual beneficiary is hiding behind the perpetrator. These are not isolated cases and do not only concern ML or FT-related crime. This reservation is important because, as part of their AML/CFT duties, OI representatives should not only recognise situations in which such events occur, but also classify them for the purposes of identifying objectives identical to those of ML and FT offences. The essence of the assessment is to ask whether a person entering into a relationship with the OI is acting of their own free will, or whether their behaviour is a response to an external stimulus or the result of a dependency. The second question concerns

[48] A.J. McKee, *behaviorism | Definition*, Doc's CJ Glossary, https://docmckee.com/cj/docs-criminal-justice-glossary/behaviorism-definition/ [accessed: 12 III 2024].

whether and to what extent such action translates into the scale of risk and the type of financial security measures that need to be applied[49].

It should not be assumed that a customer involved in ML/FT will make a mistake. The perpetrator will try to avoid mistakes that could reveal their malicious intentions, or leave false traces to mislead the decision-maker in the OI. They may create alternative scenarios, have the ability to play their role perfectly in their relationship with the OI, be resistant to stress and perform well under time pressure, have the ability to manipulate psychologically, or have a predisposition to such behaviour[50]. They may be determined to achieve their goal in a thoughtful and logical manner (in accordance with a developed or acquired algorithm of conduct), skilfully play the role of a standard customer towards an OI representative, use social engineering and manipulation techniques[51], have knowledge of finance and economics, mental resistance to errors and cognitive distortions (usually committed under the influence of emotions) or the ability to confabulate. Unfortunately, in the case of assessing the perpetrator's behaviour as defined in Art. 165a § 4 of the Criminal Code (committing a prohibited act unintentionally), the matter may be problematic. Behaviour that may seem inappropriate to an OI representative may result from the perpetrator's intellectual and social deficiencies, from confrontation with activities and decisions that are complex in their assessment, which must be taken in order to achieve the criminal objective, while at the same time not revealing the true motive for the conduct. Furthermore, the situation in which the client finds themselves in relation to a given type of OI may be a new experience for them, and it may be impossible for them to behave appropriately in the circumstances. A lack of self-control and low emotional intelligence may result in the use of inappropriate gestures and words or those learned in the past (e.g. from a criminal environment, prison, extreme terrorist ideology) and betray the real goals of the relationship established by the client. This may reveal the hidden motive behind the relationship, especially in a situation where several states are offering to make a decision, and may manifest itself in a cessation of logical behaviour as a result of a change in the OI's offer or increasingly aggressive attempts to subjugate the OI representative. Incorrect

[49] The assessment concerns only the customer – OI relationship. It cannot be ruled out that the verification of transactional behaviour will be linked to the verification of other types of behaviour, e.g. contact with the media to notify of a planned attack or to confess to a terrorist act.

[50] Members of terrorist groups use social engineering techniques to recruit supporters and convince them of their views and radical methods of implementing them in social relations (e.g. exercising control over supporters). Therefore, these techniques may have an impact on relations with the OI.

[51] This means that it will not be possible to properly and adequately profile and assess the risks.

behaviour may also be the result of a lack of understanding or misunderstanding of the offer made by the institution, which disrupts the prepared tactics of conduct[52].

The OI representative must also bear in mind the possibility of entering into a relationship with a so-called professional money launderer[53], e.g. when the lines of protection at the executive, compliance and management levels have failed, but also when the OI consciously supports such an entity. This may give rise to corruption and a positive assessment of the benefits and losses in the event of a possible financial penalty for the OI. Such perpetrators are characterised by the need to engage in criminal activity (it is their way of earning a living), the need to belong and be needed (to provide criminal services), the need to be respected as a professional in criminal circles and to realise their own potential. These are individuals who are or were members of a criminal group, who change their roles and risk exposure from a perceived 'hard' crime to a more sophisticated 'white-collar' crime, or independent individuals offering their services to representatives of other types of crime[54]. Such individuals are characterised by their knowledge of regulations, business and finance, their courage in confronting problems, and their expansiveness. They may suggest sharing profits with OI decision-makers, offer to cooperate with the OI (including making corrupt offers to decision-makers) in order to camouflage ML transactions so that they are not disclosed. This category of professional perpetrators can be divided into two groups. The first are

52 This may apply to a situation where a customer refers to a similar solution that was successfully implemented in relation to another institution, while at the same time expressing disapproval that, in the current state of relations, he is being denied a positive outcome in establishing relations or bringing them to an end. This is particularly the case when the customer has received a reward for effectively committing criminal acts in order to achieve the desired outcome in their relationship with the previous institution.

53 Professional money laundering (PML) 'is an advanced form of criminal activity that involves professional assistance in concealing the origin, owners and destination of illegal income. Its purpose is to introduce such funds into the financial system in such a way that it is invisible to institutions controlling the flow of funds'. See in more detail: *Czym jest PML i jakie zagrożenie stanowi dla AML? Metody działania umożliwiające przestępcom profesjonalne pranie pieniędzy oraz strategie w walce z PML* (Eng. What is PML and what threat does it pose to AML? Methods enabling criminals to launder money professionally and strategies for combating PML), iaml, 6 X 2025, https://www.iaml.com.pl/wiedza/pml/ [accessed: 12 X 2025]. The perpetrators are individuals who profit from the legalisation of funds derived from crimes committed by others. They receive a specific commission for their 'legalisation activities'. Professionals use complex financial structures, front companies, virtual currencies and other methods to cover their tracks and reintroduce money into the legal economy. They are also constantly improving their methods and learning new financial market instruments to perfect their criminal ventures. They are also often used to support the camouflaging of proliferation financing processes. See: *FATF REPORT. Professional Money Laundering*, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf [accessed: 12 X 2025].

54 D. Thomas, *Profiling Part 1: The Psychology of Anti Money Launderers*…, p. 6.

disclosed perpetrators who do not hide their criminal behaviour and, as bidders or OI employees, carry it out with intent. The second are those who do not disclose their intentions to the OI and perfect the practice of money laundering. Undisclosed perpetrators tend to stick to methods that work and only change them when they cease to work or become too risky[55]. They are also able to exploit gaps in the knowledge of OI representatives and their psychological weaknesses.

This does not mean that observation of perpetrators' behaviour for AML/CFT purposes can only be used in the customer – OI relationship. It should be noted that there are other entities involved in combating these practices within the AML/CFT system. The behavioural approach will be helpful in the performance of tasks, e.g. by the Border Guard, which cooperates in identifying persons who may be smuggling cash (but also artefacts, works of art or other products that may be the subject of ML or FT offences) across the border. Behavioural patterns can also be observed for the purposes of investigative or operational and reconnaissance activities (e.g. during interrogations or cooperation with human sources of information). This is because the assessment of the perpetrator's behaviour must be based on a combination of an assessment of the person's inner sphere (psyche) and an assessment of their behaviour.

Unfortunately, within the behavioural approach, we may encounter situations where it is not possible to measure the customer's hidden behaviour. Thus, the observation will only concern the customer's external behaviour, without the possibility of classifying their thoughts and emotions on this basis. In this case, alternative scenarios or micro-simulations of events can be used to observe how the customer copes in these situations. Such activities require in-depth knowledge of the product or service offered, the ability to talk to the customer and assess their behaviour from a psychological point of view. This approach can be implemented in stages in order to assess how the customer behaved at a given stage. This will allow the OI representative to focus primarily on the stage at which the customer behaved most irrationally as a result of the disruption of their accepted criminal scenario. The impulse may be to present the customer with a structured offer[56] for further investment through other services provided by the OI[57]. The reaction

[55] D. Thomas, *Profiling Part 2: The Psychology of Anti Money Launderers*, https://www.world-check.com/media/d/content_whitepaper_reference/WhitePaper_The_Psychology_Of_Anti_Money_Launderers.pdf [accessed: 28 XI 2024].

[56] Structured products offered by banks combine the security of a deposit with the potential return on investment, where part of the funds are protected and the remainder is invested in financial instruments such as shares, indexes or currencies.

[57] For example: a customer who makes the same transaction every month at approximately the same time (e.g. paying rent or utilities on payday) may be asked to set up a monthly standing order; a customer who has had unused funds in their current account for a long time may be asked to transfer

of the OI representative should not be exaggerated, as the institution should be keen to maintain relations and continue monitoring the customer's behaviour. Further action may only be excluded if the conditions specified in Art. 41(1) of the AML/CFT Act/2018 are met.

Within the behavioural approach, it is also worth mentioning the theory of economic man (Latin: *homo oeconomicus*). It assumes that humans, as rational beings, always strive to maximise their profits and make choices based on the economic value of the results of those choices. When choosing an action from among those possible in a given situation, economic man opts for the one that offers the greatest advantage in terms of benefits over losses[58]. Neither ML nor FT offences are committed for profit. In the first case, the profit from the prohibited act has already been achieved. The aim is to make it appear that it comes from legal activities. In the second case, the aim is to provide funds for the implementation of a specific idea by unlawful means (often the profit is mental benefits), i.e. to provide material and financial support to the perpetrators and organisers of terrorist acts. Thus, the profit and loss approach can be used to assess behaviour, especially in the case of OIs as financial institutions. This means that when an OI representative enters into a relationship with a customer – a potential ML/FT perpetrator – they will not obtain direct knowledge of the intention to establish and maintain a relationship with the institution. This intention is concealed by the customer due to the need to carry out criminal tactics, i.e. to legalise the proceeds of crime or move them closer to terrorist decision-makers and use them for criminal purposes in preparation for an attack or to maintain logistical security. Disclosure could result in the relationship not being established or being terminated (see: de-risking measures), as well as restrictions on the use of funds pursuant to Art. 86 of the AML/CFT Act/2018. Thus, the OI representative can only assess the behaviour of such a customer and either stimulate them appropriately or wait for them to make a mistake. This

---

the money to a high-interest savings account; a customer making payments from an interest-bearing savings account when there are sufficient funds in their current account may be asked to use the funds in their current account without losing interest on their savings account. See in more detail: S. Fernando, *Behavioral Authentication: Improving Security and CX Without Compromise*, WSO2, 21 VII 2023, https://wso2.com/library/whitepapers/behavioral-authentication-improving-security-and-cx-without-compromise/ [accessed: 28 XI 2024].

58 See: W. Załuski, *Założenie deskryptywne ekonomicznej analizy prawa: człowiek jako homo oeconomicus* (Eng. The descriptive assumption of economic analysis of law: man as homo oeconomicus), in: *System prawny a porządek prawny*, O. Bogucki, S. Czepita (eds.), Szczecin 2008, p. 297 and further; N. Artienwicz, *Rachunkowość behawioralna jako interdyscyplinarny nurt rachunkowości i społecznych nauk o zachowaniu* (Eng. Behavioural accounting as an interdisciplinary field of accounting and social behavioural sciences), https://ztr.skwp.pl/api/files/view/148818.pdf, pp. 7–23 [accessed: 28 XI 2024].

observation will also confirm or refute the thesis that the person in question may be involved in ML/FT. External behaviour thus reveals not only the attitude towards the institution, but also towards the product and/or service offered (as the object of behaviour). Hence, it will be possible to support the use of solutions referred to as sales psychology. Understanding the psychological aspects of the customer service process can increase sales effectiveness, but also confront anti-sales behaviour on the part of the customer in the context of product profitability. It can also reveal the hidden purpose of the customer's activity. Possible behaviours assessed in terms of the customer's involvement in ML/FT include:

- inconsistent information or unwillingness to provide information and unwillingness to explain details and errors,
- unjustified disproportion between the position and/or profession, financial profile and customer transactions,
- demonstrating a customer attitude that differs from general customer attitude models,
- intensification of a negative attitude towards using various arguments,
- use of false identification with varying intensity and effect,
- nervousness and reluctance to explain or lying when asked about media reports that the customer is associated with known terrorist organisations or involved in terrorist activities,
- reluctance to give their name when formalising relations with the OI,
- pretending to negotiate contract terms and making an 'offer' of the possibility of informally obtaining certain relations (e.g. regarding the amount of the transaction),
- constantly seeking to conduct transactions in cash,
- asking the institution's representative about the possibility of not recording the transaction,
- confusing concepts, geographical areas or essential elements of the subject matter of the agreement, contract or transaction,
- unjustified customer activity on the account compared to the previous observable transaction statistics,
- a radical change in the types of transactions ordered (e.g. suggesting criminal behaviour),
- making cash deposits in the case of conducting business based mainly on non-cash transactions.

Another issue to consider is how to deal with politically exposed persons (PEPs) and entities associated with them (economically, family-related). In the case of such persons, their behaviour could be linked to issues such as the desire to obtain faster, higher or long-term benefits. PEPs are associated with increased risk, which is why the OI must apply enhanced financial security measures to them. The OI employee should pay attention to: the amount of contracts in relation to standard remuneration for a given procedure and the result obtained, the type of links with the decision-maker or the time of obtaining promises, permits, authorisations (e.g. a significant reduction in the time needed to obtain such documentation, or even non-compliance with administrative deadlines), and, where applicable, the location of potential activities (change in land status, construction in the vicinity of national parks, green zones, areas designated for the development of logistics/road infrastructure, etc.). Analysis of this information allows the OI decision-maker to prepare appropriate strategies, including those suggested for use (or omission) by a member of the institution's management board. Incentives may influence PEPs in relation to potential corrupt behaviour, intimidation, distribution of public funds, influencing financial transactions or arrangements within complex corporate structures. Particular attention should be paid to situations where, given a specifically designed formal structure, the only missing element is the financial component. However, in this case, it is not a matter of control or manipulation, but of determining whether such a formal structure was created as a result of influence peddling, damage to the reputation of a public trust institution (which is often also a financial institution) or obtaining an unauthorised financial advantage (e.g. when it was found that the documents submitted were incomplete and/or inappropriate, yet were approved by the decision-maker). Therefore, the customer's behaviour remains to be assessed, which may manifest itself in: increased self-confidence, invoking connections, including in 'circles of power', suggestions to call people with whom everything has been agreed, nervousness when the decision-maker requires additional explanations and/or documents, aggression on the part of a customer who is dissatisfied with the conduct of the OI employee and demands intervention from his superior. It is important to ascertain whether the customer has the appropriate skills or knowledge to obtain the contract they wish to finalise with the OI. By observing their behaviour, the OI representative should create an information report based on their behaviour for the purposes of assessing the risk associated with that person. It can be assumed that in such a case, the documents submitted will remain in accordance with their formal use, and only the customer's behaviour will make it possible to assess whether their use was the result of corruption or whether they are intended to increase the profits of a wider group of people (including, for example, PEPs). Factors influencing the customer's behaviour may be related to the choice of a given OI, the possibility of manipulating the decisions of OI managers within the framework of supervision, or maintaining social relations with OI decision-makers. Therefore, on the one hand, a representative of this institution will have little room for manoeuvre, and on the other hand, with this assumption, they may broaden their assessment and focus on the customer's relationship and behaviour in this situation, which is different from serving a regular customer. When considering corrupt behaviour, the customer's behaviour can be assessed at various stages – the attempt to offer a benefit or the expectation of a benefit in return for the benefits offered. PEPs may also cover their tracks by providing misinformation, including about their intentions, the purpose of closing an account, changing proxies, introducing new representatives, beneficial owners (e.g. under the pretext of changing the business profile, departure to a diplomatic mission, taking up a managerial position in a representation in a third country of the EU, etc.), and the use of legal provisions to avoid disclosure and publication of financial statements (and, in the event of publication, not disclosing all relevant financial information in their content).

The problem that an OI representative may face in relation to customer behaviour, especially concerning the willingness to support terrorist activities, will be the attitude of a terrorist acolyte (supporter). This will apply to those who do not want to or cannot be direct perpetrators of terrorist acts, but who, due to their beliefs and attitude to life, try to support this course of action in some way. One way of providing such support is to provide financial assistance for the implementation of executive projects. These activities may be carried out either on one's own initiative or as a result of external determinants (e.g. the organisation of illegal fund-raising). This attitude is currently reinforced by the activity of terrorists on social media, who create supportive attitudes, recruit people to participate in terrorist activities, or organise fundraisers for supporters of their ideological goals pursued through terrorist methods. In this regard, it is also worth noting whether the customer's behaviour suggests that this is their first such action or whether it is a repetition of previous actions. Instrumental conditioning is a specific way of learning. If behaviour is followed by a positive consequence (such as a reward), there is a greater likelihood that the behaviour will be repeated in the future[59]. Especially since this reward may be a real or imagined assessment[60] based on the terrorist act that has taken place. It should be emphasised here that while members of a terrorist group are also motivated by financial gain in some way, in the case of acolytes, this gain is not financial, but rather relates to satisfaction.

59 A. Beltrani, *Understanding Behaviorism*, Palo Alto University, https://concept.paloaltou.edu/resources/business-of-practice-blog/understanding-behaviorsm [accessed: 14 III 2024].

60 For example, when a third party transfers funds to a specific terrorist group, which shortly afterwards carries out a terrorist attack, the person providing the support may understand that their financial support directly contributed to the terrorist act.

Article 299 § 2 of the Criminal Code provides for the punishment of an OI employee who cooperates with the perpetrator of ML. Thus, the behavioural approach can also be applied to the assessment of the behaviour of OI representatives[61]. In order to detect irregularities, UEBA[62] (User and Entity Behaviour Analytics) can be used. OI employees leave digital traces on the network: they access specific files at specific times, start and finish work according to routine, visit more or less the same websites, etc. UEBA monitors the activities of users and entities and collects data about them from system logs, using advanced machine learning methods to analyse vast amounts of data. The collected data is used to create a reference point for user behaviour, identify patterns of behaviour and intervals between actions, and set thresholds and deviations within which behaviour is considered normal or acceptable. A database of user behaviour patterns is then created and compared with the behaviour of employees with similar responsibilities in order to refine and detect any deviations. If an anomaly is detected, the system estimates the degree of deviation and its risk level and sends real-time alerts to security personnel. Each UEBA solution records a unique set of data according to the use cases it covers. For example, UEBA software may collect the following information: login and logout times, requests for access to sensitive resources, websites visited, applications launched, USB devices connected, keystroke dynamics. The effectiveness of all other levels of behaviour monitoring depends on the data collected at this stage[63]. In the case of detecting internal threats, behavioural profiles are used to create a set of negative baseline behaviours based on accepted user behaviour patterns

[61] In this regard, we can highlight the following unusual behaviours: changes in employee characteristics (e.g. lavish lifestyle, avoiding holidays), changes in the performance of an employee or agent (e.g. a salesperson selling products for cash has recorded a significant or unexpected increase in performance), any transactions with an agent in which the identity of the ultimate beneficiary or counterparty remains undisclosed, which is contrary to the usual procedure for the type of activity in question. See in more detail: *Types of Suspicious Activities or Transactions*, Financial Intelligence Unit Belize, 2016, https://fiubelize.org/types-of-suspicious-activities-or-transactions/ [accessed: 18 XI 2024].

[62] User and Entity Behaviour Analytics (UEBA) is 'an advanced analytical tool that monitors, analyses and detects anomalies in the behaviour of users and other entities (such as devices, applications and servers) on the network. UEBA uses machine learning and behavioural analysis techniques to identify unusual activity patterns that may indicate security threats'. Quoted after: *Co to jest User and Entity Behavior Analytics?* (Eng. What is User and Entity Behaviour Analytics?), nFlo, https://nflo.pl/slownik/user-and-entity-behavior-analytics/ [accessed: 12 X 2025].

[63] See: L. Pryimenko, *5 Levels of User Behavior Monitoring and Analytics*, Syteca, 13 XII 2023, https://www.ekransystem.com/en/blog/5-levels-user-behavior-monitoring [accessed: 18 XI 2024]; A. Babko, *7 Best Practices for Building a Baseline of User Behavior in Organizations*, Syteca, 7 VII 2021, https://www.ekransystem.com/en/blog/best-practices-building-baseline-user-behavior [accessed: 18 XI 2024].

(as training sets). This baseline helps the system to detect abnormal user behaviour using machine learning methods.

Behavioural biometrics as a method of identifying and verifying customers of obligated institutions

For some time now, biometrics has been used not only to identify and verify a person's identity (including that of an OI customer) for the purposes of maintaining a relationship with an institution, but also to fulfil obligations related to the AML/CFT system. The use of behavioural biometrics increases the number of factors taken into account in analytical algorithms (including training subsets) and accelerates the real-time identification of deviations from established customer behaviour patterns with the support of AI.

Biometrics uses two types of data: physical and behavioural. The former is collected by scanning a person's physical characteristics: fingerprints, face, hand geometry, iris or vein pattern. The latter is based on the study and evaluation of behaviours that are specific to a given user and difficult to imitate. In this case, it is not so much the reactions in OI – customer contacts that are examined, but rather the relationship between the customer and the device they are using (this also applies to interactions on websites). Biometrics is used to obtain information about the customer's individual characteristics, verify their activity and whether the source of this activity is the person whose behavioural identification data was collected at the initial stage of establishing contact with the OI. Thanks to this, the customer does not have to constantly confirm their identity, and the OI has additional tools to monitor customer behaviour in terms of risk assessment and the application of financial security measures. Continuous monitoring of customer behaviour increases the possibility of verifying their identity at any time during an active session, not just at the registration or login stage, as well as the possibility of detecting malicious activity and taking appropriate countermeasures in a timely manner[64].

Behavioural biometrics takes into account the unique way in which a user interacts with the technical device they use to manage their funds. The study does not concern what exactly the customer does in electronic banking, but how they do it. The customer's interaction with applications and websites creates a pattern and ultimately a profile of expected behaviour. In this case, behaviours such as the time of login, mouse click speed, character input and page scrolling speed, angle at which

[64] *Behavioral Biometrics: What it is and How to Enable it*, Arkose Labs, https://www.arkoselabs.com/explained/behavioral-biometrics/ [accessed: 12 III 2024].

the smartphone is held, scrolling patterns, keyboard shortcut/gesture patterns, walking style/speed, typing style (speed, pressure on the keyboard, finger position). This is behavioural analysis via velocity rules[65]. Behavioural analysis of keyboard speed focuses on the user's interaction with the keyboard, which is used in areas such as musical performance, behavioural biometrics and user performance[66].

Express payments work by analysing the frequency with which a buyer attempts to make a transaction via the OI website and raise an alarm if a crime is suspected (e.g. due to a high frequency of failed transactions by a single customer within a day or week). The following parameters are used: user locations and IP address details, devices used to connect and duration, times of day when logins typically occur, use of VPNs or proxy servers, browser and system configuration, typical purchasing patterns, usual transaction values, cards used[67]. The assessment techniques introduced also allow banks to collect data from the gyroscope in the phone and analyse typical screen positioning. Behavioural verification covers the way keys are used (alphanumeric, navigation, manipulation). It is also possible to use data recording user interaction with the application, which provides information using heat maps, user flow diagrams and user navigation paths. The system will recognise usage patterns that do not match our profile, such as pressing the keyboard too slowly or too quickly[68]. Behavioural biometrics is also based on how customers interact

65 Velocity checks are a fraud prevention method used in payment processing. They work by monitoring the frequency and pattern of transactions made within a specific time frame and detecting unusual activity, such as a large number of transactions from a single account or IP address. Fraudsters often try to use stolen card details as quickly as possible before the cardholder notices, and a sudden increase in transaction attempts can be a warning sign of possible fraud. Velocity checks can generate alerts or block transactions if they exceed certain thresholds, helping to protect businesses and customers from fraud. See: *What is a velocity check in payments? What businesses should know*, stripe, 30 VIII 2024, https://stripe.com/en-pl/resources/more/what-is-a-velocity-check-in-payments-what-businesses-should-know [accessed: 12 X 2025].

66 In this regard, it is possible to apply, among other things, a velocity rule (or velocity filter), which is a logic-based condition that evaluates the frequency of certain behaviours over a specific period of time. Velocity rules are essential when static, one-off checks are not sufficient. They detect subtle, time-dependent patterns that reveal bots, credential stuffing attempts, and other high-speed fraud attempts before they cause damage. See: *Velocity Checks*, https://seon.io/resources/dictionary/velocity-check/ [accessed: 12 X 2025].

67 *Behavioral Analysis*, https://seon.io/resources/dictionary/behavioral-analysis/ [accessed: 27 XI 2024].

68 Behavioural biometrics 'enables ongoing analysis of characteristic user behaviour patterns when using electronic banking. Identification of deviations from a previously registered profile enables the detection of unauthorised access attempts and account takeovers. In this way, it provides banks with an additional layer of security, working in parallel with existing authentication methods'. Quoted after: W. Macierzyński, M. Macierzyński, *Wykorzystanie biometrii behawioralnej w kontekście cyberbezpieczeństwa polskiego sektora bankowego (2019–2024)* (Eng. The use of behavioural biometrics in the context of cybersecurity in the Polish banking sector (2019–2024)), "Journal of Finance and

with their finances, manage transactions and accounts (digital wallets, investment platforms)[69]. Similar solutions are used in relation to chatbots. As a result, these activities may also lead to the search for specific relationships between brain activity and external behaviour (neurobehavioural science[70]). By incorporating behavioural analysis into the risk analysis process (including AI-assisted processes), you can achieve immediate return on investment (ROI)[71], reduce fraud-related losses, lower operating costs and improve customer satisfaction[72].

Financial Law" 2025, vol. 3, no. 47, p. 105. https://doi.org/10.18778/2391-6478.3.47.07. Furthermore, 'thanks to behavioural biometrics, it is possible to see not only which letters are being entered, but also how they are being entered. The system sees that the password is correct, but the way it is entered is not. This is because someone is holding the phone differently, entering the password with their left hand instead of their right, or leaving too much time between entering each letter. This is because we enter a password that we have memorised at a different pace than a password that we are writing down letter by letter from a piece of paper'. Quoted after: W. Boczoń, *Naganowski: Nadchodzi biometria behawioralna* (Eng. Naganowski: Behavioural biometrics is coming), prnews.pl, 16 I 2018, https://prnews.pl/naganowski-nadchodzi-biometria-behawioralna-432582 [accessed: 12 X 2025].

69 Such solutions are also based on emotions, independence in decision-making, and the desire for personal fulfilment in managing and controlling assets. See more: S. Jahandari, J. Shaman, *Estimation in Networks With Spatiotemporally Correlated Noise*, "IEEE Transactions on Automatic Control" 2025, vol. 70, no. 10, pp. 6885–6892. https://doi.org/10.1109/TAC.2025.3565015; S. Jahandari, D. Materassi, *How Can We Be Robust Against Graph Uncertainties*, in: *2023 American Control Conference (ACC)*, pp. 1946–1951. https://doi.org/10.23919/ACC55779.2023.10156615.

70 Neurobehavioural science has been defined as any behavioural response resulting from central nervous system processing. Neurobehaviour is considered to be the basis for performance in activities of daily living (ADL) and refers to the cognitive and perceptual components of behaviour, including praxis, attention, memory, spatial relations, sequencing and problem solving. See: G. Gillen, K. Brockmann Rubio, *Treatment of Cognitive-Perceptual Deficits: A Function-Based Approach*, https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9780323172813000277/first-page-pdf [accessed: 12 X 2025]. Neurobehavioural responses can be disrupted by environmental factors such as exposure to neurotoxins. Neurobehavioural disinhibition can occur in adults years later, which is referred to as neurobehavioural disinhibition, which is a latent trait derived from a number of indicators of insufficient behavioural control, including executive cognitive functions, externalising symptomatology and emotional dysregulation. Hence, it is possible to identify individual clients through an in-depth relationship with the OI as part of the financial security measures (verification) applied. Influencing factors include social maladjustment and drug use.

71 It is divided into: Trending ROI – these are early, progress-oriented indicators that suggest that an AI initiative is delivering value, even if that value has not yet translated into revenue or savings; and Realised ROI – this is the measurable, results-oriented impact of AI investment. See: M. Bokich, *Measuring AI ROI: How to Build an AI Strategy That Captures Business Value*, Propeller, 8 V 2025, https://propeller.com/blog/measuring-ai-roi-how-to-build-an-ai-strategy-that-captures-business-value [accessed: 12 X 2025].

72 Z. Salman, *Behavioral Biometrics and Customer Identity Authentication*, Fico Blog, 19 I 2021, https://www.fico.com/blogs/behavioral-biometrics-and-customer-identity-authentication [accessed: 14 III 2024].

Authentication based on user activity can be used to assess whether this activity does not correspond to the characteristics of being a perpetrator of ML or FT. By examining individual cases and behaviours, the OI can generate patterns of how customers with the characteristics of potential ML/FT perpetrators behave. The obligated institution may take measures aimed at individual identification based on the assessment of behaviour or behavioural biometrics, also using other factors quantifying the customer's criminality resulting from general factors indicating criminal behaviour, individual factors related to the provision of specific services (general offers) by the OI, but also on the basis of individual offers addressed to a specific customer, which in their behaviour deviate from the pattern of using financial instruments associated with a given individual offer, developed and adopted by the OI.

Online banking therefore represents a change in supervision by the OI, taking into account behavioural factors other than those that would be selected to assess behaviour resulting from the customer's physical presence at the institution's premises. The behavioural characteristics used are: signatures (shape and dynamics), voice, keyboard typing dynamics, walking style, etc. Information and communication technologies are used for this purpose. One way to verify a user is to use keystroke dynamics for authentication or identification. This refers to an automated method of identifying or confirming a person's identity based on their typing style and rhythm. Typing patterns are mainly collected from computer keyboards, but information can potentially be collected from any device equipped with traditional touch-sensitive keys (for example, mobile phones, PDAs, laptops, palmtop computers, netbooks, etc.). In the case of keystroke dynamics, the biometric template used to identify a person is based on their typing style, rhythm and speed. The measurements used for keystroke dynamics are dwell time and flight time. Dwell time is the time a key is pressed. Dwell time, on the other hand, is the time between releasing one key and pressing the next key. Unlike physiological biometrics, there is no such thing as an absolute match in behavioural biometrics. Therefore, it is difficult to argue for the uniqueness of a typing pattern. It must be clear that with the dynamics of keystrokes, it is not possible to achieve FAR[73] and FRR[74] rates as low as those achieved with better physiological biometrics, and therefore it cannot be the sole factor for identifying or authenticating a person[75].

[73] FAR, or false acceptance rate, is the probability that the system will incorrectly authorise an unauthorised person as a result of incorrect matching of biometric data to the template.

[74] FRR, or false rejection rate, is the probability that the system will incorrectly deny access to an authorised person due to a mismatch between their biometric data and the template.

[75] *Biometric Solutions*, https://www.biometric-solutions.com/keystroke-dynamics.html [accessed: 12 III 2024].

Another way to assess customers using behavioural biometrics is cognitive biometrics[76]. It aims to obtain information about users by generating external stimuli, such as displaying images, to analyse the nervous system's response, or by analysing places that the user frequently visits. This serves to create a unique identity that changes depending on the user's behaviour in a given location. Monitoring user activity patterns serves to achieve the goal of detecting unusual activities that indicate a higher risk of fraud (both by the user themselves and by someone impersonating them). Possible anomalies include transactions made from an unusual location, inconsistent with the user's normal location-related behaviour, or requests to transfer large amounts of money to an unknown account. This enables real-time signalling and prevention of fraudulent activity[77]. For this purpose, data sets can be built based on data from situations such as: a specific customer's behaviour to date, when there were no suspicions about their behaviour, or based on general patterns revealed in various cases where a specific type of behaviour was identified as the behaviour of an ML/FT perpetrator.

Behavioural biometrics can also be one of the elements of so-called multi-factor authentication. This is a method of electronic authentication that requires at least two factors (e.g. a password and voice recognition) for a user to access a website or application.

Kinesthetics should also be taken into account. Each person has a unique posture, walking style and way of holding a mobile device. For example, body position can help to understand body weight distribution, and gait analysis can provide information about walking speed or stride length. For this purpose, it is possible to use CCTV recordings from cameras installed as part of OI security systems.

[76] 'Biometric characteristics measure distinct features of individuals, usually (but not always or entirely) dictated by their genetics. They are based on measurements and data obtained from direct measurement of a specific part of the human body. Fingerprints, iris, face, scent, retina, ear, vascular pattern, lips, palm geometry and DNA are examples of physiological biometrics'. Quoted after: A. Grzybowski, *Sztuczna inteligencja w okulistyce 2023* (Eng. Artificial intelligence in ophthalmology 2023), Przegląd Okulistyczny, https://przegladokulistyczny.pl/2024/09/13/sztuczna-inteligencja-w-okulistyce-2023-2 [accessed: 15 X 2025]. In the case in question, it allows for the identification of the customer and their behaviour in a situation where there is a device between the customer and the OI – an information signal transmitter that also serves as a customer identifier. See in more detail: P. Magee, M. Ienca, N. Farahany, *Beyond neural data: Cognitive biometrics and mental Privacy*, "Neuron" 2024, vol. 112, issue 18, pp. 3017–3028. https://doi.org/10.1016/j.neuron.2024.09.004.

[77] *How is behavioral biometrics used for authentication?*, Incognia, https://www.incognia.com/the-authentication-reference/how-is-behavioral-biometrics-used-for-authentication [accessed: 15 III 2024].

Summary

Behavioural science, as a method based on observing behaviour, can be used to profile and identify OI customers as potential perpetrators and/or suspects in money laundering or terrorist financing. An institution can observe a person and generate data from their behaviour for the purposes of customer identification, verification and monitoring. This data is so unique and individual that it allows a person to be identified both in physical relations with the OI and in online relations. However, behaviour is only one of the dimensions on the basis of which a customer's conduct can be assessed. Another is the psychological dimension – understanding the psychology of criminals. Many people involved in ML do not believe they are committing a crime. They justify their actions by saying that they do not cause social harm, or present them as necessary in the circumstances. Identifying these justifications can help uncover early signs of criminal intent.

The rapid development of behavioural biometrics in recent years, coupled with the recognition that this method of identification and verification is more effective than existing code-based methods, is becoming the future for technology industries seeking to ensure the security of both financial institutions and their customers. In this regard, it is important to ensure that institutions are able to collect this type of data on an ongoing basis for the purpose of creating training sets and processing this knowledge with the support of AI and machine learning. This applies in particular to institutions that serve a large number of customers and therefore need to analyse a lot of data. This information can also be used, for example, for advertising, user profiling or website analysis. Such analysis is useful when the OI uses open sources of information to identify the real motives for entering into a relationship with a customer. Behavioural and biometric authentication as part of customer identification can be helpful in verifying and monitoring customers as part of the OI's individual ML/FT risk assessment. This specific behaviour mapping allows conclusions to be drawn about the customer's involvement in ML or FT. Thanks to the use of a behavioural approach and behavioural biometrics, it will be possible to segment customers and build a broader profile that goes beyond economic relations with the OI. It may also concern issues related to behaviour and the sources of the behaviour presented by the customer. As a result, the OI can build an additional area and risk assessment factors for the purposes of ML/FT risk assessment and analysis, and thus qualify the scope and intensity of financial security measures.

Relying solely on behavioural assessment is not sufficient to classify a customer as a person suspected of involvement in ML/FT. To this end, behavioural methods should be combined with other methods (e.g. psychological, from

the field of neuroscience[78]). Similarly, it will be possible to examine the customer's transactional behaviour aimed at a specific criminal objective, but also for the purpose of assessing whether there is a reasonable suspicion that a specific transaction or specific assets may be related to ML or FT (Art. 86 of the AML/CFT Act/2018). Furthermore, due to technological developments, it should be considered whether, for the purposes of KYC and risk analysis, OIs should be granted formal powers to conduct behavioural analysis[79]. However, only a combination of psychological elements and externalised behaviour can provide a complete behavioural picture of the customer for the purposes of not only reactive and proactive detection of ML/FT offences, but also a full risk analysis at the OI[80].

The general research assumption adopted by the author of the article, recognising that in view of the need to analyse risk and select financial security measures in a state of specific ML/FT threat, the OI is required to take action to identify and recognise customer behaviour, taking into account behavioural factors, has been positively verified. Based on the presented diagnosis, it should be recognised that one of the basic elements of KYC assessment should be the creation of a customer's behavioural profile as a result of an assessment of their behaviour resulting from their character, motivation, criminal intent, ability to identify threats and behaviour resulting from external impulses (e.g. succumbing to persuasion to commit a crime, blackmail, the need to repay debt at another financial institution)[81]. Behavioural assessment provides insight into the motives and objectives of the customer's actions. It is related to their personality, the variability of their behaviour, including behaviour under the influence of third parties.

---

78 Cf. P. Piotrowski, *Neurobiologiczne i psychospołeczne uwarunkowania racjonalności zachowań przestępczych – przegląd badań* (Eng. Neurobiological and psychosocial determinants of rational criminal behaviour: a review of research), https://bazhum.muzhp.pl/media/texts/resocjalizacja-polska-polish-journal-of-social-rehabilitation/2011-tom-2/resocjalizacja_polska_polish_journal_of_social_rehabilitation-r2011-t2-s197-232.pdf [accessed: 12 X 2025].

79 For example, performing actions such as: evaluating the method of selecting a type and creating an account, similarly filling out a contract form, sending a form, adding further services to an existing basket, managing a shopping basket, subscribing to a newsletter, or purchasing an item or subscription.

80 M. Sotiriou, entry on LinkedIn portal, https://www.linkedin.com/posts/makis-sotiriou_the-psychology-of-money-launderers-a-missing-activity-7265318888265957377-izS3 [accessed: 28 XI 2024].

81 See: A. Tajak-Bobek, *Proces decyzyjny na przykładzie przestępczości przeciwko mieniu. Analiza jakościowa wywiadów pogłębionych* (Eng. The decision-making process based on the example of property crime. Qualitative analysis of in-depth interviews.), "Ogrody Nauk i Sztuk" 2022, no. 12, vol. 12. https://doi.org/10.15503/onis2022.29.46.

Bibliography

Al-Obaidi N.M.H., *Motives of the Terrorism Phenomenon Among Youth and the Role of Laws in Dealing with It*, "Akkad Journal of Law and Public Policy" 2021, no. 4, vol. 1, pp. 182–197. https://doi.org/10.55202/ajlpp.v1i4.85.

Bandura A., *Teoria społecznego uczenia się* (Eng. Social learning theory), Warszawa 2007.

Bąbel P., *Terapia behawioralna zaburzeń rozwoju z perspektywy analizy zachowania* (Eng. Behavioural therapy for developmental disorders from the perspective of behaviour analysis), "Psychologia Rozwojowa" 2011, vol. 16, no. 3, pp. 27–38. https://doi.org/10.4467/20843879PR.11.016.0189.

Di Wu, Xuhui Li, *A Systematic Literature Review of Financial Product Recommendation Systems*, "Information" 2025, no. 16. https://doi.org/10.3390/info16030196.

Falkowski A., Tyszka T., *Psychologia zachowań konsumenckich* (Eng. Consumer behaviour psychology), Gdańsk 2001.

Grzywacz J., *Segmentacja na rynku usług bankowych* (Eng. Segmentation in the banking services market), "Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne" 2014, vol. 20, pp. 37–53.

Hara M., Kierzynka R., Kołodziejski P., *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz* (Eng. Act on Counteracting Money Laundering and Terrorist Financing. Commentary), issue 1, legal status as of 12 May 2013.

Jahandari S., Materassi D., *How Can We Be Robust Against Graph Uncertainties*, in: *2023 American Control Conference (ACC)*, pp. 1946–1951. https://doi.org/10.23919/ACC55779.2023.10156615.

Jahandari S., Shaman J., *Estimation in Networks With Spatiotemporally Correlated Noise*, "IEEE Transactions on Automatic Control" 2025, vol. 70, no. 10, pp. 6885–6892. https://doi.org/10.1109/TAC.2025.3565015.

Liedel K., *Profilowanie sprawców przestępstw terrorystycznych* (Eng. Profiling perpetrators of terrorist offences), in: *Profilowanie kryminalne*, J. Konieczny, M. Szostak (eds.) Warszawa 2011, p. 199.

Macierzyński W., Macierzyński M., *Wykorzystanie biometrii behawioralnej w kontekście cyberbezpieczeństwa polskiego sektora bankowego (2019–2024)* (Eng. The use of behavioural biometrics in the context of cybersecurity in the Polish banking sector (2019–2024)), "Journal of Finance and Financial Law" 2025, vol. 3, no. 47, pp. 103–128. https://doi.org/10.18778/2391-6478.3.47.07.

Magee P., Ienca M., Farahany N., *Beyond neural data: Cognitive biometrics and mental Privacy*, “Neuron” 2024, vol. 112, issue 18, pp. 3017–3028. https://doi.org/10.1016/j.neuron.2024.09.004.

Mazurczak J., *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu* (Eng. Radicalisation as a process leading to extremism and terrorism), “Miscellanea Anthropologica et Sociologica” 2020, no. 21(2), pp. 45–73.

Meloy J.R., Hoffmann J., Guldimann A., James D., *The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology*, “Behavioral Sciences and the Law” 2012, vol. 30, no. 3, pp. 256–279. https://doi.org/10.1002/bsl.999.

Merari A., *Academic research and government policy on terrorism*, “Terrorism and Political Violence” 1991, vol. 3, pp. 88–102.

Milanovic K., *Money Laundering and Other Forms of Financial Crime*, “Journal of Law and Politics” 2024, no. 5, pp. 57–78. https://doi.org//10.69648/JJDU2862.

Olszak-Häußler K., *Rozumienie pojęcia „ślad” w ujęciu profilowania kryminalnego* (Eng. Understanding the concept of ‘trace’ in criminal profiling), “Problemy Kryminalistyki” 2016, no. 291, pp. 7–11.

Ranstrop M., *The Root Causes of Violent Extremism*, Brussels: European Commission, 2016, in: J. Mazurczak, *Radykalizacja jako proces prowadzący do ekstremizmu i terroryzmu*, “Miscellanea Anthropologica et Sociologica” 2020, no. 21(2), pp. 45–73.

Slovic P., Weber E.U., *Perception of Risk Posed by Extreme Events*, in: *Regulation of Toxic Substances and Hazardous Waste*, issue 2, J.S. Applegate, J.G Laitos, J.M. Gaba, N.M. Sachs (eds.), 2011.

Tajak-Bobek A., *Proces decyzyjny na przykładzie przestępczości przeciwko mieniu. Analiza jakościowa wywiadów pogłębionych* (Eng. The decision-making process based on the example of property crime. Qualitative analysis of in-depth interviews), “Ogrody Nauk i Sztuk” 2022, no. 12, vol. 12. https://doi.org/10.15503/onis2022.29.46.

Załuski W., *Założenie deskryptywne ekonomicznej analizy prawa: człowiek jako homo oeconomicus* (Eng. The descriptive assumption of economic analysis of law: man as homo oeconomicus), in: *System prawny a porządek prawny*, O. Bogucki, S. Czepita (eds.), Szczecin 2008.

Internet sources

Artienwicz N., *Rachunkowość behawioralna jako interdyscyplinarny nurt rachunkowości i społecznych nauk o zachowaniu* (Eng. Behavioural accounting as an interdisciplinary field of accounting and social behavioural sciences), https://ztr.skwp.pl/api/files/view/148818.pdf [accessed: 28 XI 2024].

Aziz Sbeih D., *Which Group has a More Sustainable Model of Terrorism*, https://washington-collegereview.files.wordpress.com/2019/09/sbeih_which-group-has-a-more-sustainable-model-of-terrorism-al-qaeda-or-isis.pdf [accessed: 24 XI 2024].

Babko A., *7 Best Practices for Building a Baseline of User Behavior in Organizations*, Syteca, 7 VII 2021, https://www.ekransystem.com/en/blog/best-practices-building-baseline-user-behavior [accessed: 18 XI 2024].

Behavioral Analysis, https://seon.io/resources/dictionary/behavioral-analysis/ [accessed: 27 XI 2024].

Behavioral Biometrics: What it is and How to Enable it, Arkose Labs, https://www.arkoselabs.com/explained/behavioral-biometrics/ [accessed: 12 III 2024].

Beltrani A., *Understanding Behaviorism*, Palo Alto University, https://concept.paloaltou.edu/resources/business-of-practice-blog/understanding-behaviorsm [accessed: 14 III 2024].

Biometric Solutions, https://www.biometric-solutions.com/keystroke-dynamics.html [accessed: 12 III 2024].

Bjelopera J.P., *The Islamic State's Acolytes and the Challenges They Pose to U.S. Law Enforcement*, https://sgp.fas.org/crs/terror/R44110.pdf [accessed: 29 X 2025].

Boczoń W., *Naganowski: Nadchodzi biometria behawioralna* (Eng. Naganowski: Behavioural biometrics is coming), prnews.pl, 16 I 2018, https://prnews.pl/naganowski-nadchodzi-biometria-behawioralna-432582 [accessed: 12 X 2025].

Bokich M., *Measuring AI ROI: How to Build an AI Strategy That Captures Business Value*, Propeller, 8 V 2025, https://propeller.com/blog/measuring-ai-roi-how-to-build-an-ai-strategy-that-captures-business-value [accessed: 12 X 2025].

Co to jest User and Entity Behavior Analytics? (Eng. What is User and Entity Behaviour Analytics?), nFlo, https://nflo.pl/slownik/user-and-entity-behavior-analytics/ [accessed: 12 X 2025].

Comparison: Terrorist Financing, Money Laundering, and Financing the Proliferation of Weapons of Mass Destruction, Jersey Financial Services Commission, 14 IV 2022, https://www.jerseyfsc.org/industry/guidance-and-policy/comparison-terrorist-financing-money-laundering-and-financing-the-proliferation-of-weapons-of-mass-destruction/ [accessed: 12 X 2025].

Counter Proliferation Financing. Guidance Notes, https://www.fsc.gi/uploads/CPF%20Guidance%20Notes.pdf [accessed: 12 X 2025].

Czym jest PML i jakie zagrożenie stanowi dla AML? Metody działania umożliwiające przestępcom profesjonalne pranie pieniędzy oraz strategie w walce z PML (Eng. What is PML and what threat does it pose to AML? Methods enabling criminals to launder money professionally and strategies for combating PML), iaml, 6 X 2025, https://www.iaml.com.pl/wiedza/pml/ [accessed: 12 X 2025].

Estevez E., *Behavioral Analytics: Meaning, Types, Criticism*, Investopedia, 29 I 2023, https://www.investopedia.com/terms/b/behavioral-analytics.asp [accessed: 15 VII 2025].

Fernando S., *Behavioral Authentication: Improving Security and CX Without Compromise*, WSO2, 21 VII 2023, https://wso2.com/library/whitepapers/behavioral-authentication-improving-security-and-cx-without-compromise [accessed: 28 XI 2024].

Francis R., He L., *Managing money laundering risks in digital payments. How digital payment providers can combat financial crime*, OliverWyman, https://www.oliverwyman.com/our-expertise/insights/2023/oct/anti-money-laundering-strategies-for-digital-payment-providers.html [accessed: 15 VII 2025].

Gillen G., Brockmann Rubio K., *Treatment of Cognitive-Perceptual Deficits: A Function-Based Approach*, https://www.sciencedirect.com/sdfe/pdf/download/eid/3-s2.0-B9780323172813000277/first-page-pdf [accessed: 12 X 2025].

Grzybowski A., *Sztuczna inteligencja w okulistyce 2023* (Eng. Artificial intelligence in ophthalmology 2023), Przegląd Okulistyczny, https://przegladokulistyczny.pl/2024/09/13/sztuczna-inteligencja-w-okulistyce-2023-2 [accessed: 15 X 2025].

Guidance for a Risk-Based Approach the Banking Sector, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf [accessed: 20 I 2025].

How is behavioral biometrics used for authentication?, Incognia, https://www.incognia.com/the-authentication-reference/how-is-behavioral-biometrics-used-for-authentication [accessed: 15 III 2024].

Major factors influencing consumer behavior, Clootrack, https://www.clootrack.com/knowledge-base/major-factors-influencing-consumer-behavior [accessed: 18 XI 2024].

McKee A.J., *behaviorism | Definition*, Doc's CJ Glossary, https://docmckee.com/cj/docs-criminal-justice-glossary/behaviorism-definition/ [accessed: 12 III 2024].

"Muły finansowe" – ukryte zagrożenie w świecie bankowości online (Eng. Financial mules – a hidden threat in the world of online banking), prnews.pl, 2 XII 2024, https://prnews.pl/muly-finansowe-ukryte-zagrozenie-w-swiecie-bankowosci-online-481242 [accessed: 12 X 2025].

Piotrowski P., *Neurobiologiczne i psychospołeczne uwarunkowania racjonalności zachowań przestępczych – przegląd badań* (Eng. Neurobiological and psychosocial determinants of rational criminal behaviour: a review of research), https://bazhum.muzhp.pl/media/texts/resocjalizacja-polska-polish-journal-of-social-rehabilitation/2011-tom-2/resocjalizacja_polska_polish_journal_of_social_rehabilitation-r2011-t2-s197-232.pdf [accessed: 12 X 2025].

Pryimenko L., *5 Levels of User Behavior Monitoring and Analytics*, Syteca, 13 XII 2023, https://www.ekransystem.com/en/blog/5-levels-user-behavior-monitoring [accessed: 18 XI 2024].

Risk assess your business for money laundering supervision, Gov.UK, 23 X 2014, https://www.gov.uk/guidance/money-laundering-regulations-risk-assessments [accessed: 18 XI 2024].

Salman Z., *Behavioral Biometrics and Customer Identity Authentication*, Fico Blog, 19 I 2021, https://www.fico.com/blogs/behavioral-biometrics-and-customer-identity-authentication [accessed: 14 III 2024].

Sekar H., *Recognize Your Customers: A Complete Guide on Customer Behavioral Cues and Building Customer Relationships*, 8 VII 2019, https://www.freshworks.com/freshdesk/customer-engagement/customer-behavioral-cues-building-customer-relationships-blog/ [accessed: 12 III 2024].

Skrebneva O., Abramova A., *Why Behavioral Analytics is Key to Fraud Detection Today*, The Sumsuber, 14 V 2024, https://sumsub.com/blog/behavioral-analytics/ [accessed: 24 XI 2024].

Sotiriou M., entry on LinkedIn portal, https://www.linkedin.com/posts/makis-sotiriou_the-psychology-of-money-launderers-a-missing-activity-7265318888265957377-izS3 [accessed: 28 XI 2024].

The definition of unusual and unjustified transactions from the perspective of the risk of money laundering and terrorist financing, https://www.cnb.cz/export/sites/cnb/en/faq/.galleries/definition_of_unusual_and_unjustified_transactions_from_the_perspective_of_the_risk_of_money_laundering_and_terrorist_financing.pdf [accessed: 14 III 2024].

Thomas D., *Profiling Part 1: The Psychology of Anti Money Launderers*, https://www.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/white-paper/the-psychology-of-money-launderers.pdf [accessed: 28 XI 2024].

Thomas D., *Profiling Part 2: The Psychology of Anti Money Launderers*, https://www.world-check.com/media/d/content_whitepaper_reference/WhitePaper_The_Psychology_Of_Anti_Money_Launderers.pdf [accessed: 28 XI 2024].

Types of Suspicious Activities or Transactions, Financial Intelligence Unit Belize, 2016, https://fiubelize.org/types-of-suspicious-activities-or-transactions/ [accessed: 18 XI 2024].

Velocity Checks, https://seon.io/resources/dictionary/velocity-check/ [accessed: 12 X 2025].

What is a velocity check in payments? What businesses should know, stripe, 30 VIII 2024, https://stripe.com/en-pl/resources/more/what-is-a-velocity-check-in-payments-what-businesses-should-know [accessed: 12 X 2025].

Wolniak R., Skotnicka-Zasadzień B., *Wybrane metody badania satysfakcji klienta i oceny dostawców w organizacjach* (Eng. Selected methods for measuring customer satisfaction and evaluating suppliers in organisations), https://www.researchgate.net/profile/Radoslaw-Wolniak/publication/41199963_Wybrane_metody_badania_satysfakcji_klienta_i_oceny_dostawcow_w_organizacjach/links/5ab63b2ba6fdcc46d3b45829/Wybrane-metody-badania-satysfakcji-klienta-i-oceny-dostawcow-w-organizacjach.pdf [accessed: 18 XI 2024].

Russian internet sources

Викторович К.А., Алексеевна Ш.О., *Террористический акт: особенности уголовноправовой и криминалистической характеристик*, "Союз Криминалистов и криминологов" (Viktorovich K.A., Alekseyevna Sh.O., *Terroristicheskiy akt: osobennostiugolovnopravovoy i kriminalisticheskoy kharakteristik*, "Soyuz Kriminalistov i kriminologov") 2023, no. 1, https://crimeinfo.ru/wp-content/uploads/2023/08/2023-01.pdf, pp. 98–104 [accessed: 28 XI 2024].

Legal acts

Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Official Journal of the European Union L 254/1 of 5 August 2025).

Act of 1 March 2018 on counteracting money laundering and terrorist financing (Journal of Laws of 2025, item 644).

Act of 25 June 2009 amending the Act on counteracting the introduction into financial circulation of assets derived from illegal or undisclosed sources and on counteracting the financing of terrorism, and amending certain other acts (Journal of Laws of 2009, no. 166, item 1317).

Act of 16 November 2000 on counteracting money laundering and terrorist financing (Journal of Laws of 2000, no. 116, item 1216).

Act of 6 June 1997 – Criminal Code (consolidated text, Journal of Laws of 2025, item 383).

Other documents

FATF REPORT. Professional Money Laundering, https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf [accessed: 12 X 2025].

Stanowisko Urzędu Komisji Nadzoru Finansowego dotyczące identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideo weryfikacji (Eng. Position of the Polish Financial Supervision Authority on the identification of institutional clients and verification of their identity in the financial sector supervised by the Polish Financial Supervision Authority based on the video verification method), https://static.fintek.pl/uploads/2022/03/Stanowisko_UKNF_dot_wideoweryfikacji_klientow_instytucjonalnych.pdf [accessed: 28 XI 2024].

Wytyczne na podstawie art. 17 i art. 18 ust. 4 dyrektywy (UE) 2015/849 dotyczących środków należytej staranności wobec klienta oraz czynników, które instytucje kredytowe i finansowe powinny uwzględnić podczas oceny ryzyka prania pieniędzy i finansowania terroryzmu związanego z indywidualnymi stosunkami gospodarczymi i transakcjami sporadycznymi („wytyczne w sprawie czynników ryzyka prania pieniędzy i finansowania terroryzmu") uchylające i zastępujące wytyczne JC/2017/37 (Eng. Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016937/Guidelines%20ML%20TF%20Risk%20Factors_PL.pdf [accessed: 28 XI 2024].

Maciej Aleksander Kędzierski, PhD

Doctor of Law, independent researcher, lecturer at Kozminski University in Warsaw, legal advisor, retired police officer. Author of articles and monographs on organised crime, anti-money laundering and counter-terrorism financing, financial analytics, financial sanctions and compliance activities.