International Journal of Law and Society
2025, Vol. 8, No. 4, pp. 349–359
https://doi.org/10.11648/j.ijls.20250804.18

Methodology Article

Attributive-criminological Characterization of ML/FT Crimes as a Method of Information Analysis in the AML/CFT System

Matthias Alexander Kędzierski*

Independent Scholar, Warsaw, Poland

Abstract

The article proposes a methodological approach to the analysis of intelligence and financial information by applying the - attributive - forensic characterization of ML/FT crimes (AFCC). The purpose of using AFCC is to obtain the highest level of certainty (probability) of criminal events and various types of connections with them, which coherently reflect the characteristics of a given crime (ML/FT). This pursuit of "certainty" is understandably associated with assigning an act to a specific person and demonstrating its occurrence as penalized behavior. But also a transition from the state of probability of threat - used at the level of risk analysis and the use of mitigants to neutralize it, to the state of actual typing of elements of crime threat. The introduction of AFCC should affect the general organization and tactics of criminal investigations in the field of ML/FT using identification and analytical mechanisms (for risk assessment purposes) available to the countermeasure system itself based on IO (obligated institutions) - national FIU (Financial Intelligence Unit) relations. AFCC broadens the scope of the search for and interpretation of facts/events that can be linked in the IO to the characteristics of money laundering and money laundering crimes. AFCC aims to give information vectors to information generated already at the stage of its possession in the IO. These vectors may be multiple and determined also by factors internal and external to the IO, but they are characterized by the evidentiary direction of the future investigation.. The AFCC method, on the other hand, offers the potential to strengthen the evidentiary process of "suspicious activity" identified analytically and then procedurally by the ML/FT perpetrator. For these purposes, it is crucial to develop a suspiciousness attribute within the IO that will identify suspicious behavior, transactions, and relationships between the client and the institution. Actions undertaken using this factor can contribute to establishing both a monetary and criminal trail.

Keywords

AML/CFT, AFCC, Forensics, Method, Risk

1. Thematic Introduction

One of the challenges in properly defining operational risk status at an obligated institution (hereinafter referred to as an OI) is leaving the methods for its classification to the institutions themselves. This is achieved without implementing rules of conduct, while applying very general guidelines specifying which risk assessment elements should be included in a given OI, depending on its individual characteristics. In such a case, it is necessary to introduce a specific information (data) handling pattern within a given OI (or several similar ones) and to structure the analytical process. The OI decision-maker thus

*Corresponding author: sulawezi.mk@onet.eu (Matthias Alexander Kędzierski)

Received: 28 October 2025; **Accepted:** 10 November 2025; **Published:** 9 December 2025

becomes the independent designer of the environment in which they will implement ML/FT countermeasures and risk intelligence analysis. This period would include identifying anomalies for Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) and developing Suspicious Activity Reporting (SAR) information for submission to Financial Intelligence Units (FIUs). This translates analytical information into financial information. Patterns, often built on algorithms, should focus, as in the AML/CFT system, on "transactions" and "customers." However, the goal here is not to meet the formal and substantive requirements for SARs, but to obtain a substantively valuable result from the analysis of ML/FT threat identification related to a transaction or customer handled within the institution. One of the optimization problems is to find the smallest set of event features generated within and outside the OI, with the greatest return value for identification, online, or predictive classification of the event as suspicious. The area in which the decision-maker will operate in the OI will be called the "space" $\| X \|$, i.e., the "superior" set over other sets and actions undertaken within the OI regarding AML/CFT. Input data for the intelligence analysis process comes from both structured and unstructured information, administered and created by both the intelligence unit itself and other entities, including those with only minimal ties to the AML/CFT system. This external data, as well as some IO data, will not be subordinated to the AML/CFT process (e.g., because it originates from non-system entities), which consequently generates the need to increase the quantification of input data from non-system entities, albeit those whose potential can be leveraged for the AML/CFT system. Quantification must identify the element and the relationships between it and other elements of the information network (events). The goal is to achieve the appropriate level of data axiomatization. This applies to the decision-maker's activity, both at the stage of initiating intelligence analysis and its execution (threat identification). Importantly, it may be misleading, in the same process, to talk about risk assessment (especially operational risk) on the one hand and, on the other hand, to search for a key in OI to the optimal set of information identifying events that occurred in it and are classified as ML/FT (e.g. for training sets using machine learning).

The proposed new AFCC method – the subject of this article – aims to combine both of these countermeasures and direct activities towards achieving the goal of neutralizing the threat of crime. In other words, analytical activities should be subordinated to the crime detection process by implementing a risk identification process and its causes, in conjunction with the disclosure of ML/FT crimes, and potentially obtaining information identifying the perpetrator of these crimes. Clearly, the emphasis in this method should be on the detection process as a precursor to the process of proving the perpetrator, which is crucial – in the long run – to the ongoing criminal proceedings. Taking into account that the perpetrator of a punishable act can only be a human being (e.g. a customer), we will treat the forensic assessment of the "transaction" in this case as an indirect human action, the effect of criminal action with an asset that is properly recorded or physically present (e.g. when the customer himself operation using it of actual/online banking, or when the OI makes a suspicious transaction at his request).

2. Purpose of the Article

The purpose of this article is to present a new method for identifying, profiling, and processing data within in OI end in the Financial Intelligence Unit (FIU), with the intention of using it not only in risk analysis and reporting to the FIU, but also in identifying attributes indicating "suspicious" incidents involving IOs, as well as their early, specialized "forensic" interpretation for use in evidentiary proceedings in criminal proceedings (this is a combination of attributive and forensic criteria). Legal techniques were used in the preparation of this article and the development of the analytical information management method, including analysis of Polish and foreign legal provisions and active observation of the direct implementation of information management regulations and techniques within the department constituting the national FIU. A qualitative analysis of existing solutions in the area of forensics and AML/CFT was also conducted to understand and interpret the applicable legal provisions and their implications for law enforcement practices, including the use of detection tactics. Graph theory, vector computation, and a mathematical approach to spatial properties also provided support. The article primarily presents the basic theoretical assumptions for implementing the presented method. Due to the identified problems, an AFCC model based on OI attributes and forensic characteristics of ML/FT crimes was proposed as a starting point. The research problem identified was the need to develop a model that would optimally characterize events recognized in OI in terms of variables that most closely approximate attributive-forensic ML/FT identification. To obtain results, it is necessary to identify the features, their dimensions, and the interrelationships that determine the recognition of offender behavior that most closely resembles the characteristics of ML/FT crimes. Given the large amount of data to be processed, a mathematical approach was proposed, incorporating elements of linear regression and operations on functions and sets. To facilitate interpretation, a linear formula was used.

3. Basic Issues of the AFCC Method

The AML/CFT system is a multi-stage process, usually starting from a certain state "0" for the intelligence activities of OI end of the Financial Investigative Unit (FIU). State "0" does not mean that the OI/FIU initially has no data; on the contrary, there is a large amount of data. However, the OI does not have an assessment of its quality. To achieve this, it must implement analytical procedures to identify the risk and

the resulting threat scale. Their initiation is related to the occurrence of an event (either a single event or the result of cyclical activities). Subsequently, the information passes through the intelligence analysis stage, which concludes with a decision-making stage based on the established state of affairs (knowledge). At this stage, the obtained set of information – information on suspicious events – is forwarded to the FIU (factual translation of information). In the next stage, the FIU re-evaluates the information and conclusions to undertake further analytical activities – i.e., analyze the financial information and, consequently, forward a notification of a suspected ML/CFT offense to the prosecutor's office or initiate cooperation with cooperating units (CU) and continue the analysis as its own (but also file the information).

The activity in question constitutes a vectorial action, a vector of directed analytical procedure. At individual stages, it can be "multiplied" by a scalar (number), which, if positive (+), multiplies it in the designated direction, while if negative (-), it results in a return to repeat the event information assessment. This means that each new contribution resulting from the event's attribution (its scalars attribution) can increase or decrease the vector's value over time (multiplying the information value or knowledge). A scalar can be: new information, an analysis result, a scoring result, a query from law enforcement, a query from the FIU, etc. If the scalar equals 0, vectorial actions are suspended (e.g., due to a lack of confirmation of ML/FT characteristics, a determination that the event should be associated with another crime, including one not designated as the primary/source crime). It is also possible to "multiply" two or more vectors, especially when certain activities in the same or different OIs are conducted against the same entities (creating a "super SAR"). Consequently, it will also be possible to obtain the result of a vector extension, a change in direction, or its reversal (the criminal characterization of an event in one OI does not have to be understood in the same way in another OI various OI). For reconnaissance, the direction is clearly defined – it is a prohibited act (ML/FT) appropriately classified by the legislator in the Penal Code. The perpetrator's ML/FT conduct in the space ‖ X ‖ is also a vector, with the perpetrator himself having the right to implement it. At the intersection with the perpetrator's vector WS, it is possible to obtain information coordinates that characterize the state of suspicion. In such a case, the perpetrator, wishing to obtain the postulated result, must pass through specific spaces in the OI (they cannot omit them, and the OI's task is to construct the space of planes to ensure their completeness to protect their own security interests). The ‖ X ‖ space is primarily a space of information and its processing. Knowledge about the perpetrator's vector also constitutes information to which the OI must respond in a specific way. Consequently, the elements of ‖ X ‖ space must be measurable. This postulate can be achieved by introducing gradation and scoring of behaviors in the OI (mathematically assigning a score to the characteristics of the assessed behaviors). t is also important that d [the decision-maker] obtains the possibility of counting the distances between specific points (numbers) of the space scalars |A−B|, which will evaluate the behavior of the perpetrator-client. Here you can use the following formula: The formula for the distance between two points P1=(x_1, y_1) and P2=(x_2, y_2) in two-dimensional Euclidean space is $s = \sqrt{((x_2 - x_1)^2 + (y_2 - y_1)^2)}$, where x_1, y_1, - coordinates of the first point, x_2, y_2, - coordinates of the second point. Let's say we have two points P_1 and P_2 in an n-dimensional vector space. Their coordinates are: $P_1 = (x_1, y_1, z_1,..., n_1)$ $P_2 = (x_2, y_2, z_2,..., n_2)$ Then the formula for the distance (d) between these points is: $d(P_1, P_2) = \sqrt{[(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2 +... + (n_2 - n_1)^2]}$ That is, we sum the squares of the differences of the corresponding coordinates, and then calculate the square root of this sum [1]. Measurability of distance is important given the need to "measure" movement and assess it in terms of route usability and deviations from a rational assessment of the perpetrator's vector's direction of action (which seems obvious from the point of view of the need to assess customer behavior and transaction dynamics). Obtaining an OI image is possible by applying the rules of social network analysis, SNA, or conducting an analysis using graph theory [2]. For the mathematical solutions introduced in AFCC, it will be important whether we assume linear operations at the plane level (two coordinates) or with respect to a point in space (three coordinates). Further considerations will be conducted at the plane level. In machine learning, distance is used to compare feature vectors of data, for example to group similar objects.

In connection with the proposal of a new countermeasure concept in this state of affairs, it is also necessary to consider the use – as an auxiliary method – of another method referred to as forensic characteristics crime, FCC. It can be used to determine the value of the index k' (similarly to the quantifier of the first-order predicate calculus), to introduce a regression model [3] A. N. Kolesnichenko and V. E. Konovalova: pointed out that "a forensic characterization is a system of information about forensically significant signs of a type of crime, reflecting natural connections between them and serving to build and verify investigative leads in order to solve specific investigative tasks" [4]. Forensic science was originally created as a science for preliminary investigation; the trial has traditionally remained out of sight of the most forensic scientists. However, in recent years, the situation has begun to change. There is no consensus among criminalists regarding the possibility of using forensic data at the stage of judicial consideration of criminal cases [5-8]. According to H. Malewski: "A forensic characterization of a crime contains a fixed set of data, such as: modus operandi, typical consequences of the act (e.g. description of the type of forensic traces left), methods used by perpetrators to avoid criminal responsibility, circumstances of the event that must be established and investigated in similar cases, data indicating the personality of the potential criminal and his/her personality traits, possible motives and goals of the action, description of circumstances standard for a given type of crime that facilitate

its commission, and others" [9]. In its original assumption, the method concerned primarily operational and reconnaissance activities, including forensic activities - carried out for the purposes of prosecuting perpetrators of crimes and collecting evidence in criminal proceedings, as well as developing investigative versions. Currently, the introduction of an attributive-forensic characterization of crimes (AFCC) model is being proposed for coherent countermeasures against ML/FT threats in the AML/OI. This stems from the diversity of stages and decision-makers involved in creating an image of ML/FT crimes within the AML/CFT system. The FCC should enable the determination of coordinates of ML/FT forensic features for the AFCC model. Through the attributive-forensic assessment, data from analyzed events undergoes axiomatization to assign them a negative (on minus) information value, k' (information about suspicion). Only such treatment of data from the considered space constitutes an appropriate and conscious narrowing for the purposes of determining the maximum value of $i_{ML/FT}$ information in the OI. Forensic characteristics of a crime allow for the creation of a pattern/set (axiomatic construction) of negative ML/FT axioms, i.e., properties that data must satisfy to allow for the assessment of suspicious circumstances surrounding a client/transaction/account, forensic assessment of traces that can be revealed and secured in the IO, but not the evidentiary value of these actions or, at a later stage, the perpetrator's "guilt." Some of the axiomatization elements possess measurable evaluative characteristics k', which can be included in the adequate set. It is not based on treating FT in a "negative cooperation" configuration (as a fight, in praxeological terms), due to the possibility of interpretation errors. The k' indicator (as a feature of the "comprehensive trace" k', combining multiple data sources) can be determined on the basis of statistical studies in the following areas: the quality of alerts, the duration of alert examination and analytical reconnaissance, the number of SAR reports, the false positive rate, the rate of closing an analytical case in the OI or FIU, the number of revealed traces of increased risk, but also the number of FIU-prosecutor's office notifications based on SAR, the number of initiated ML/FT cases, the number of convictions of perpetrators, etc. For this purpose, regression models were used. Regression lineary itself is a method that allows for modeling the relationship between variables (features X_t, a $X_{t+1.}$ when adopting a time variable, but another determinant is also possible that is adequate to assess the suspiciousness, this may refer to quantitative changes) and using this knowledge to predict unknown values of one variable $Y_{k'}$ based on knowledge of the others. The obtained result of the target variable Y with the index k' is the desired result allowing for assessing whether the complex of all variables used provides a set of knowledge Za/k that will create an effective SAR/STR for the FIU. The phenomenon occurring in the population can be described by the following general linear equation: $Y = X_{\varrho} + \varepsilon$, where: y - vector of values of the dependent (dependent) variable, X - matrix of explanatory (independent) variables, ϱ - vector of unknown parameters, ε - random component (stochastic factor of the equation). It is proposed that k' be derived from the values of explanatory variables obtained at the level of analytical recognition of the OI, as well as at further stages of the FIU/prosecutor's office.. $Y_{k'} = \varrho 0 + \varrho_1 X_{t,1} + \varrho_2 X_{t,2} + ... + \varrho_n X_{t,k} + \varepsilon t$, where $X_{t,1}$ - - observed values of explanatory variables, $Y_{k'}$ - observed values of the explained variables, εt – unknown value of the random component, $\varrho 1$ - unknown values of the model parameters. Consequently, the coefficient k' will measure the differences between the vectors A and A' taking into account all coordinates adopted in the OI for the model, including the coordinates of forensic features. It is also possible before $\varrho_1 X_{t,1}$ A negative sign is introduced when the coefficient does not generate information about the purpose of the action or the effect is a reduction in risk. The model should also assume that the perpetrator has a "profitability" in committing the crime, but not in financial terms but in achieving the goal. The solution adopted for k' in both ‖ X ‖ and ‖ O" ‖, where its value may vary, should be assessed by the coefficient of determination R^2. Axiom k' is an indirect creator of a " comprehensive trace" by marking the elements of the set. This determines the percentage of the variability in the explained variable explained by the explanatory variables. In a given AFCC model, this means to what extent the collected features will determine the elements indicating that the given actions will be classified as ML/FT. As a result of the typing and measurement, the higher the R^2, the more accurately the given features will be determined. The coefficient of determination R^2 is a measure of the fit of a statistical model to the data, which determines what percentage of the variation in the dependent variable is explained by the independent variables in the regression model. In the case of an unexplained portion of the variability, these features will not be needed for the ML/FT-determined assessment, but may be used to assess other negative phenomena occurring in the OI structure. A "comprehensive trace" in forensics refers to the complete, detailed history and origin of evidence, from its discovery at a crime scene to its final analysis and reporting. This includes a full record of the chain of custody, every step of physical or digital analysis, and the provenance of digital data or physical samples. It is crucial for ensuring the evidence is admissible in court, as it allows for a rigorous assessment of its integrity and reproducibility. The "comprehensive trace" is built on the basis of the evaluation of data and facts using the axiom k' not only "evidentially", but also "analytically", based on the assessment of deviations of the customer's behavior from the pattern adopted in the OI.

The AFCC model does not take into account the characteristic division of ML practices, "Placement-Layering-Integration". Instead, it is based on the forensic structure of ML/FT crimes themselves, as defined in the AML/CFT system and the Penal Code. It also relies on operating within the diversity and individuality of OI, but with the intention of achieving a single goal (intermediate result) – the earliest attributive-forensic structure of information about

ML/FT crimes [10]. This is achieved through the appropriate selection of attributes and the forensic identification of their correlations. The AFCC theory is based on introducing comprehensive reasoning into the AML/CFT system for the purpose of establishing (directional) relationships between individual types of intelligence activities (stages, parallel proceedings), and, given the need to achieve an optimal final outcome at a later stage – evidentiary criminal proceedings dedicated to proving the existence of ML/FT crimes and identifying the perpetrators. The attributive-forensic set should effectively identify the subject of the crime, such as assets (financial and non-financial) subject to freezing and subsequent forfeiture. Reasoning should incorporate both a subjective and objective (private, individual) approach, hence the need for a comprehensive approach. AFCC also assumes that the perpetrator's actions are not impulsive but planned, deliberate, and serve a specific purpose. As an example, an axiom in ML/FT is that money launderers and terrorist financers must have access to financial institutions as instruments for achieving their criminal goals. These institutions provide these individuals with the means to transfer assets between other financial institutions. [11]. From state 0, as the initial information phase, the OI should aim to retrospectively and predictively classify information not only in terms of risk but also from a forensic perspective, seeking connections and building a chain of connections from the initiator to the beneficiary of ML/FT crimes. The key is to eliminate free (empty) variables, meaning data that are not bound by any quantifier (they cannot be classified as graph nodes, and thus it will be outside the graph scheme, i.e. outside the system of information marked with k'). Thus, the OI does not construct the idea of a transaction as unusual and not fitting normal patterns, but rather quantifies it attributively, directionally, towards the evidentiary nature of ML/FT findings. The OI cannot be unaware of the crime, as all analytical activities at this institution are subordinated to the qualification of "suspiciousness" (pol. podejrzalność, is an established (detected) feature or features of a single event or a set of events that may indicate the nature of: circumstances that justify indicating the possibility of committing a money laundering/terrorist financing offense or the occurrence of a justified suspicion that a specific transaction or specific assets may be related to money laundering/terrorist financing [12]) and its arguments in SARs/STRs submitted to the FIU. OI should not relinquish its directional determination qualification to other entities in the AML/CFT chain, but should strive for substantively qualitative SARs, reducing false-positive and false-negative reports. Due to the limited functional and competence scope of OIs, forensic characterization of information and events should enable the identification of unidentified links in such a chain and increase the efficiency of financial information analysis conducted at the FIU level (obtaining a result in the form of forensic quantification of financial information). In such a case, we distinguish between the primary and secondary AFCC entities. The primary entity focuses on optimally classifying events and connections in the OI with the forensic classification of the act. The secondary entity supports the actions of the decision-maker in criminal proceedings in their role of managing information during evidentiary proceedings (officer compliance, FIU). The use of AFCC in the initial phase of incident recognition should prompt decision-makers to adopt a specific (forensic) approach to assessing the facts, the circumstances of their occurrence (the event's environment), and to identify clients and transactions for the purpose of (building attributes) – in future stages – identifying these events for the purpose of establishing ML/FT crimes and their perpetrators (AFCC reasoning). It is therefore an extensive, backward-looking "detection process" identifying events that may be assessed as criminal in the future. This task is undertaken by the OI in the "unpained investigation" phase [11]. In this case, attributes may, but do not have to, raise suspicion in the forensic sense, and in this respect, they will remain within the context of the negatively classified activity. This requires developing a physical and intellectual assessment of the potential for committing an ML/FT crime, as well as assessing the camouflage of the criminal purpose and limiting the "traces" of such activity (i.e., the mental element).

The decision-maker in the IO should strive to ensure that such countermeasures are not only undertaken in parallel but also in synergy (coordination) of their application. AFCC is therefore a mixed "functional-doctrinal" process, in which the core of functional activities derives from the ML/FT countermeasures system of analytical-administrative (attributive) provenance. The doctrinal element, however, is known in criminal law doctrine as being closer to the dogmatic definition of a crime (as an unlawful act and action, forensically speaking). Consequently, a comprehensive trace is built as a set of logically and forensically related, revealed, and demonstrated features of events. k' - identifying them with the features of a crime ML/FT, $E_{k'}= \{i_1, i_2, \ldots i_n\}$, where i is an element of the set E marked by the axiom k'. Set E will become the basis for constructing a SAR/STR or filing a notice of alleged ML/FT crime. Thus, the SAR will be composed solely of k' valuable elements. It's like building another negative subset based on axiom k'. AFCC is not limited to "*follow the money*" alone; it considers a range of elements beyond those related to money flow, such as customer behavior, sales patterns of OI products, the scope of the crime's subject matter, and the characteristics of the subject of the act. AFCC addresses various areas in the "evidence-generating" space, ‖X‖, which are initially qualified only in terms of OI risk (their attribution), not "forensic," which may delay or undermine their forensic evidentiary nature. The AFCC goal should be formulated from the matrix of ML/FT elements, as defined by the provisions of the Penal Code. The method is intended to achieve a specific, complex target state, the parameters of which allow for obtaining a specific number (minimum for evidentiary conditions). $Z\ a/k \rightarrow_{MAX} SD_{ML/FT}$.

The FIU is bound by the direction of the OI vector, but can amplify it with its own scalars, which may differ from the

scalars available to the OI. The OI does not have a set of operational instruments, but only a risk-based analysis, which can be defined as intelligence analysis (reconnaissance analysis). The purpose of analytical activities at an OI is not to prove a crime but only to demonstrate a) circumstances that may indicate a suspicion of money laundering or terrorist financing, or b) a reasonable suspicion that a specific transaction or specific assets may be related to money laundering or terrorist financing. Therefore, this type of activity falls under attributive activities (searching for risk characteristics within the axiom and associating them in the SAR/STR).

This condition (W), however, does not justify forwarding an incorrect or empty SAR, assuming that $W_{SAR} \in SAR$ is $SAR \neq \emptyset$, by the OI handover to the FIU. Therefore, the effect of these actions is not to directly report a suspected crime to the prosecutor's office, but to forward the SAR/STR to the FIU. Therefore, the use of the AFCC method does not limit decision-makers' activities but only aims to characterize events classified as ML/FT criminal offenses, both for their prosecution and for the identification of their symptoms at the OI/FIU stage. This approach can also be used by the AFCC to undertake predictive actions regarding the possibility of a crime. At the same time, the AFCC provides the opportunity for targeted intelligence analysis in the OI, focused solely on identifying suspicions, anomalies, and irregularities related to ML/FT. The magnitude of the factor constructed based on the statistical analysis of the original crimes should not dominate the overall calculation results for k', as the purpose of AFCC is primarily to reveal the characteristics of the ML/FT act itself, without identifying the original prohibited act. In the case of FT, this is sometimes impossible when the original funds originate from legal sources. AFCC can be supported by technical analytical tools based on artificial intelligence (AI/AML) due to the sheer volume of data requiring processing, especially within OI and open information sources. AFCC reasoning – as a methodological module – should translate not only into human reasoning ($d \in D = \{OI/FIU/CU\}$) but also into the use of AI tools.

When assessing the feasibility of CFCC application, it can be stated that in the vast majority of cases, we are dealing with a fixed "scene" (perhaps rather a platform for information about the event), ‖ Xi ‖, where the OI can conduct a "forensic assessment" of various types of criminal activities. This space can be expanded, for example, by offering new OI products or modifying existing ones. This expansion of "scenes" can be implemented at the level of the institution itself or in relationships with other OIs that share the same scope of activity or require product-related cooperation (e.g., a bank and an insurer). In the case of the forensic characterization of crimes, as represented by A. N. Kolesnichenko and V. E. Konovalova, the aim is to support and direct future actions, which should be combined with "investigation planning." The aim is rather to link the development of forensic tactics with other sciences, such as social sciences, psychology, linguistics, etc., associating criminal events with elements of the investigation and its tactics. In the case of AFCC, the OI decision-maker also takes on the role of heuristic thinking, creating algorithms (models of behavior) that allow him to solve problems effectively [4]. The construction of the AFCC method must fit into the scheme: "criminal proceeds" - "legalization costs" - "pure criminal profit" - "investing legalized assets" (ML) or in the case of (FT) "criminal/legal proceeds" - "legalization/camouflage costs" - "assets with a terrorist beneficiary", as a potential subject of the typed crime. The k' indicator is proposed to be created as a result of metric research on the manner in which ML/FT crimes are committed and on the behavior of clients identified in OI as potential perpetrators. After constructing the matrix, it will be possible to adopt a numerical scalar that can be used in subsequent stages of the CFCC method.

4. AFCC Methodology

Let there be a specific decision maker d z OI, belonging to the set of decision-makers of the set D ={OI/FIU/CU}, where $d \in D_{OI/FIU/CU}$. Let there be a given space in IO, ‖ X ‖ defined by information – Xi. Information will be any type of signal that can be interpreted (given the characteristics of a value). Let the features k' be given, defined by the determination of classifying (axiomatizing) events as committing a crime ML or FT (metrically calculable). It should be assumed that the elements of ‖ X ‖ and its complements ‖ O" ‖ were moving towards S set $D_{ML/FT.}$ [$SD_{ML/FT}$] where the obtained state $S_{ML/FT}$ is the basis for the construction of the directional action vector in OI - SAR/STR. Most events in ‖ X ‖ remain measurable; the scoring of these events must be developed by OI itself. Their measurability can also be used to identify the measurability of elements in ‖ O" ‖ as complements of ‖ X ‖. However, there is no guarantee that all the elements available to d will participate in the measurement, but d strives for this state. It is important to ensure the completeness of ‖ X ‖ and to bring ‖ O" ‖ to a "sufficient state" for the purpose of obtaining elements with k' features from it. The effect of the measurability process [must be to assign the resulting elements attributive-forensic features k'. Measurability becomes a necessary process for determining the position of elements in relation to other elements and determining their "size" in k'. Therefore, the assumption is to extract from ‖ X ‖ such elements "i" that will have the property k' [$SD_{ML/FT}$ set of elements with property k', $SD_{ML/FT}$ (i)]. The property k' is the vector of suspiciousness (α) of "i" forensic features of ML/FT crimes (β), which can also be represented as a matrix.

It is also assumed that every specific human behavior (including activation the movement of assets) is reflected in the information space Xi (a trace in space). This reflection occurs in this space for both ordinary behaviors (positively normalized) and those that public authorities (customarily) classify as reprehensible (negatively normalized). Therefore, the ‖Xi‖ space can contain representations of both negative and positive behaviors (data structuring). This allows for combining

negative risk assessments in OI with the identification of "criminal" characteristics of information that shapes the risk assessment, resulting in the creation of a "comprehensive trace" through their axiomatization. The decision-maker's task is to identify and classify negative behaviors that exhibit characteristics of two crimes, ML or FT (alternatively or jointly). In this case, "negative behavior" represents an unfavorable assessment of the OI from the perspective of the adopted "pattern" of handling the product or transaction. It also indicates a suspicion of characteristics criminally classified - as symptoms of an ML/FT crime. Reprehensible behaviors possess negatively axiomatic characteristics k', from the perspective of their code (legal) assessment or the assessment of suspiciousness attributes. Deviant behaviors are also an indirect reflection of behaviors in the information space, which can be classified as criminal symptoms, or merely as mistakes, errors, misunderstandings, lack of skills, or ignorance. Such elements should also be analyzed to see if they possess the characteristics of a "comprehensive trace" k'. $E_{k'}$= {i1, i2, …in}, where "i" is an element of the set E marked by the axiom k'. So, such an element is soug $E_{k'} = i_{k'} \in \| Xi \|$ where simultaneously $\| Xi \| = \{i: i \in Xp \wedge i \in Xn\}$, whereby $i_{k'} \in Xn \wedge i_{k'} \notin Xp$, $Z\, i_{k'} = \{f: f \in Zn\}$.

Let us consider a space ‖ O" ‖ as its complement –which means that any of its elements will be qualified by axiomatic properties but can be found in undefined regions (open spaces). ‖ O" ‖ is the complement of ‖ X ‖ [for the algebra of sets it could be defined as —X]. Due to greater complexity, ‖ X ‖ and ‖ O" ‖ could be defined as subspaces of some space ‖ Ω ‖ provided that ‖ X ‖ ∽‖ O" ‖ = ‖ Ω ‖. Its axiomatic classification reduces a given element h to being an element of the space ‖ O" ‖, h ∈ ‖ O" ‖ and the set O, neutral with respect to the results of axiomatization, also belongs to the space – ‖ O" ‖, O ∈ ‖ O" ‖, $h_{k'} = i_{k'} \in \| O" \| \wedge i_{k'} \notin O$. The element under study may be - unconditionally significant - when it directly qualifies as an element of space by having strong axiomatic features (properties), "→ k'". Or being conditionally significant, when its initial evaluation does not give it the feature of unconditionality, but over time it may become an element that is unconditionally axiomatically significant. $i_{k'} \notin O \rightarrow h_{k'}$, when $i_{k'} \neq i_p$. All those elements that do not fall into these ranges will constitute a set of elements – axiomatically irrelevant $i_p \in Op \wedge i_p \notin On$ [p- axiomatically positive, n- axiomatically negative]. To comprehensively organize the actions undertaken by the decision-maker d, it is possible to introduce a definition – a series of activities, that occur when the decision-maker undertakes such a course of action. This involves adopting an internal instruction – an algorithm for handling events, information, and knowledge in the IO.

Features - when there is a set of elements where each element E in the set has a feature k', $E_{k'}$, which is adequate to the features contained in the set, features of suspiciousness and features characteristic for the elements of the adequate set Z_A is an adequate element. The element $O_{k'}$ as measurable with the feature k' also belongs to the adequate set, $O_{k'} \in Z_A$. Moreover, the gauge of the element E can also be performed by means of the features k' obtained from the environment ‖ O" ‖, where $O"_h = \{ h: h \in On \wedge \notin Op\}$ creating an element $h_{k'}$, where $h_{k'} = i_{k'} \in \| O" \| \wedge i_{k'} \notin Op$ so it will not belong to the data set that does not meet the condition of being an element of the adequate set. $E_{k'} \in On \wedge E_{k'} \in Z_A$ at is, elements that meet the this condition sought: $E_{k'} = \{i_{k"} \in \| Xi \|$ where $i_{k'} \in Xn \wedge \notin Xp \wedge i_{k"} \in On \wedge i_{k"} \in Z_A\}$. The adequate set contains only elements that meet the condition $Z_A = \{f: f \in Zn\}$. Zn is only a set of adequate elements that have received negative action towards the element identified with ML/FT. Wanted set Z a/k attributive-forensic is a set that meets the condition for the element that: Z a/k = [e: e ∈ {Z $i_{k'} \cup O"_h \cup Z_A$}]. Each element value result obtained in this way is included in the recognized elements of the space ‖ X ‖ and should be assessed in terms of its axiomatic value for the purpose of selecting other elements towards the evaluation of k' (and be included in the training set in the future).

The adequate set Z_A is built based on directional experience, e.g., FATF examples, but also as a training set using AI, or constructed based on other analytical and information activities. Set O consists of various subsets, e.g., social media, discussion media, classified messaging applications, etc., element e will belong to set O if the gauge elements taken from the adequate set allow for a radical assessment of them as potential "evidence" of suspicion (directionally positively attributive). Only such feature representation is taken into account that will strengthen the set of axiomatic features for the purposes of typing (multiplying) the assessment of suspiciousness. Especially the one selected as the directional axiomatic feature for the established deviant event established with suspiciousness characteristics in OI. In this respect, a complementary element is sought, but it is not "homeomorphic". This makes it innovative $E_{k'}$ after positive verification, it can be included in the set of axiomatic features Z a/k. It should be borne in mind that beyond the action space OI ‖ X_i ‖, there are other wider spaces ‖ O" ‖, however, the decision-maker d is particularly interested in obtaining the potentially most effective features k' from the entire set of available features, where i∈ Wn elements (and narrow the space by eliminating non-attributive elements Wp), which will identify the suspiciousness and in the future the evidentiary nature of the behavior of the designated perpetrators, ultimately creating such a set Z a/k, when Z a/k ={i: i∈ Wn ∧ i ∉ Wp} [i ∈ Wn — Wp ⇔ i∈ Wn ∧ i ∉ Wp] [13]. As an assumption for action it can be assumed that each element, A ∈ $E_{k'}$, by $E_{k'}$ space ‖ Xi ‖ considered by the decision-maker d, d ∈ $D_{OI/FIU/CU}$, remains convergent, or tends to establish the maximum number and quality of features of one of the elements $P1_{ML}$ or $P2_{FT}$, PN_{ML}, PM_{FT} …. A max → $F_{max\ E\ k'}$ ($E_{k'} \in \| Xi \|$) where $F_{max\ E\ k'}$ takes on characteristics C' ∈ C {$P1_{ML}$, $P2_{FT}$, PN_{ML}, PM_{FT}…}. In addition $f_{C'}$: ($Z_{E\ k'}$) → (Z a/k) and $f_{C'}$: (Z

$_{E\,k}$') → (Z_A), $f_{C'}$: ($Z_{E\,k}$')= $Z_{E\,k}$'. Set C = {$P1_{ML}$, $P2_{FT}$, PN_{ML}, PM_{FT}…} is a set of suspiciousness attributes (analytical recognition and forensic features associated with ML/FT crimes) [14, 15].

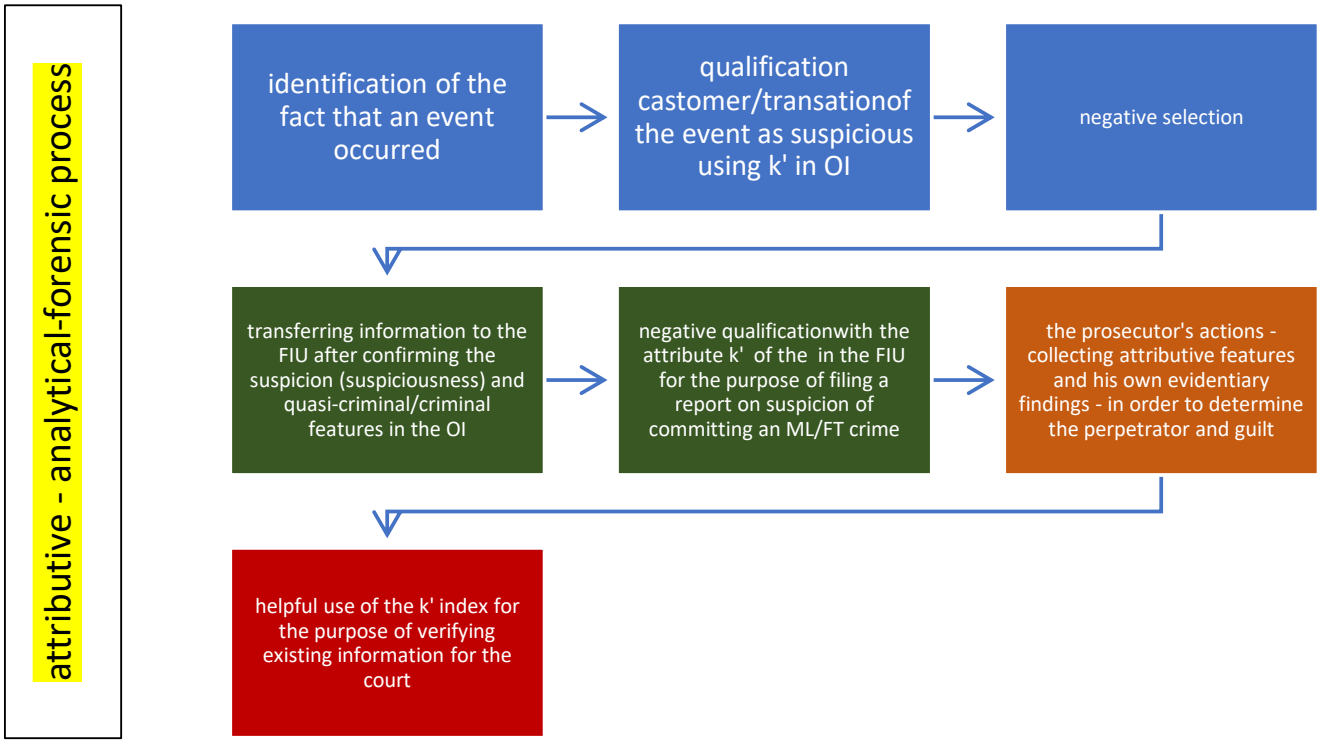
Thus, from the entire defined space ‖ Xi ‖ and the complement ‖ O" ‖, the elements that have axiomatic features consistent with the features of the indicated P_{ML} or P_{FT} elements should be generated. This means that the search for $E_{k'}$ elements in the subject space is related to the function they perform in the entire criminal procedure defined by the target P_{ML} or P_{FT} elements. Consequently, it is important that the overall process of detection, analysis and reconnaissance analysis is completed with such a state (set) of established features of elements that qualify a given element for the subsumption of the crime (suspicion) of money laundering (AML) or terrorism financing (PFT). Each of the elements with characteristics k' typed in OI should remain tending to a specific convergent state (set of elements) $SD_{ML/FT}$, {$Z_{a/k\,1}$, $Z_{a/k\,2}$ … $Z_{a/k\,N}$} ∈ $SD_{ML/FT}$ unconditionally assessed negatively, which would be the basis for building in OI - SAR/STR (extracting negative features consistent with the symptoms of the indicated crimes). The approach pattern in OI may be repeated at the FIU level, and in this case the convergent state will be – submitting a notification of a suspected crime to the prosecutor's office or forwarding information (not for proceedings) to the CU/foreign FIU. As a consequence we get that $y_{SAR/STR} = f(x_{SDML/FT})$, where y is an element of the set {SAR/STR} and x belongs to the set { $SD_{ML/FT}$}. Taking into account the indicated stages of creating a set{ $SD_{ML/FT}$} it can be determined that f:{ $SD_{ML/FT}$}→{SAR/STR}.

5. Applying the AFCC Method to Counteract ML/FT

In the analytical and administrative area, IOs play a significant role in the ML/FT countermeasures system. Based on established risk analysis results or existing states, IOs must acquire data and information from their own systems and external administrative systems. The goal is to identify individual or complex facts that may indicate ML/FT. This constitutes a constitutive search for negative indicators. Based on the established results of preliminary risk analyses or existing conditions, they must acquire data and information from their own systems and external administrative systems to identify individual or complex facts that may indicate ML/FT. This constitutes a search for negative indicators of k'. These initial risk assessments can be undertaken at the on-boarding level, but also as chat-GPT for potential future clients. The next step is monitoring customer behavior and ordered transactions for any suspicious behavioral patterns. This approach shapes the "characteristics" of behavior. This should result in a vector-based, structured set of information that can be further analyzed. Consequently, the informational construction of the SAR/STR report—as an analytical result—can be profiled based on the "characteristics" of behaviors captured as a result of the IO-client (transaction) relationship, as well as the forensic characteristics of ML/FT crimes. Both of these "characteristics" of A/C should be intertwined and complementary, hence the proposed AFCC method. This goal will focus on obtaining data that allows for confirming a threat, not just a risk, by obtaining a state of suspicious circumstances or a reasonable suspicion that a specific transaction or asset may be related to ML/FT. However, information may be transferred from the OI to the FIU in a persistently high state of uncertainty. This, in turn, creates the possibility of submitting premature, uncertain, or empty SARs. The AFCC method aims to ensure that "reasonable suspicion" is as closely aligned as possible with the "criminal characteristics of a crime." This can be achieved by using the AFCC method by identifying: the client or the transaction originator as a potential suspect; identifying the characteristics of the suspicious transaction or the client's behavior toward other clients or the IO itself; identifying the similarity of the behavior with patterns of "suspicious behavior" available to the IO; and finally, demonstrating the circumstances under which the suspicious behavior occurred. The AFCC does not force IO decision-makers to act "like a prosecutor" but rather reduces the activities (specifies actions) to the targeted identification of suspicious behavior as identifying the perpetrator's behavior that can be considered "constituting conduct covered by a prohibited act." The result should be a "comprehensive trace" of the forensic characteristics of the crime. In addition, the AFCC should influence the adoption of specific tactics within the OI to generate SARs and neutralize risks. A "comprehensive trace" becomes a "continuous trace" from the IO to the identification of the perpetrator's guilt in criminal proceedings.

Obtaining such a result provides the basis for referring the SAR to the FIU, which can assign additional features that fit the forensic characteristics of the ML/FT crime (secondary axiomatization). The subject of this stage of analysis – financial information – collected from the SAR/STR, i.e., a set of elements interconnected with varying degrees of probability, may indicate the existence of another, as yet undetermined attribution element, determine the direction and method of searching for it, or further refine the characteristics of existing connections. Using only instruments that enable indirect event characterization results in an incomplete picture of the forensic characteristics of the crime, but it can be identified differently than through operational intelligence. AFCC allows for the creation of associations, connections between individual elements, and characterization as individual, but especially as related to other elements, to build a picture of criminal behavior. The tactics of event characterization in OI differ from those in CU. The AFCC concept allows for inferences from established elements about other elements that have not yet been revealed. This allows for the creation of a forensic image of the crime, i.e., the components and connections between them, as if a pattern of the prohibited act existed

(including identifying which components are missing, and an evidentiary matrix of the perpetrator's guilt). The use of AFCC also allows for the assumption of a specific version of the perpetrator's behavior, both when we have knowledge of the entire time frame from the creation of the crime to its completion, and when all the components are missing to prove their behavior and bring charges in criminal proceedings. This action will utilize the findings and knowledge retained by the OI, FIU, and, at a later stage, by the CU as part of the criminal procedure. This is especially true if the STR report submitted to the FIU has resulted in its transformation into a notification of suspected crime. The CFCC method "selects" only those features of anomalous behavior that are identical to the subject matter of the crime (criminalization) and the subject of the act specified in the provision—that is, the subject of the enforcement action. The AFCC method recognizes that certain ML/FT processes correspond to the stage of development of the criminal mechanism—interactions between direct and indirect participants in a criminal event and their environment, which in turn naturally determines the formation of appropriate material and intellectual traces. At the same time, it is important to remember that each criminal action has its own individual characteristics, constituting its own forensic characteristics. Furthermore, behavioral imitation also occurs, maintaining the same mechanism of action by a given perpetrator (which individualizes them), or benefiting from already existing (successful) criminal behavior.



Scheme 1. *The process of using the k' factor for the purpose of identifying negative analytical and forensic features of ML/FT crimes.*

6. Summary

The use of AFCC is possible at any stage of the diagnosis assessment analysis in order to correct its results/lack of results in a purposeful manner → $_{MAX}$ $SD_{ML/FT}$. The purpose of using the AFCC method is to uncover attributive and forensic symptoms of ML/FT. Its use is worthwhile when assessing an event's suspiciousness predicts the securing of k' traces of complex criminal actions undertaken to commit the ML/FT crime. The AFCC method neutralizes the problem of attribution and interpretation, achieving strong correlation between events. The flexible AFCC procedure model allows for adaptation to individual ML/FT countermeasure modules assigned to the OI as a result of the duties imposed on OI. Given the diversity of OI, AFCC organizes the information image and determines suspiciousness analyses to identify the characteristics of ML/FT crimes. AFCC is a targeted search for forensically significant ML/FT characteristics, which are revealed in the characteristics of the methods, mechanisms, and environment of its implementation, structuring the understanding of these crimes. AFCC should also identify the preparatory and execution levels of the targeted ML/FT perpetrator. This issue is crucial because these crimes can be committed both directly and through multi-stage elements of the supply chain from initiator to beneficiary. Indirect use of AFCC will also allow for the identification of criminal activity, allowing for the rejection of other illegal behaviors or

symptoms of anomalies that are not illegal. The close connection between quasi-forensic and forensic activities refines and directs the information vectors used by the OI. Consequently, the method allows for obtaining an "investigative situation" [16]. That is, a situation constituting a set of results from the investigator's search and cognitive activity, reflecting the current state of the investigative process and serving as the basis for making informational, tactical, and organizational-management decisions. This set is expanded not only by the investigator's activity but also by the results resulting from the activities of the analyst at the OI and the FIU analyst. An example where the presented AFCC methodology would be helpful is the case of asset seizure in a drug and cryptocurrency trafficking investigation [17]. It would enable the provision of forensic evidence already at the analytical stage in the OI/FIU for the purposes of the ongoing legal proceedings. ML/FT proceedings have evolved into two main approaches, each reflecting a distinct legal philosophy: the "follow the money" principle and the classical criminal approach [18]. The "follow the money" principle emphasizes that asset recovery is the primary goal, with restitution of losses incurred as a result of the crime prioritized over the perpetrator's criminal conviction. The AFCC method, on the other hand, offers the potential to strengthen the evidentiary process of "suspicious activity" identified analytically and then procedurally by the ML/FT perpetrator. For these purposes, it is crucial to develop a suspiciousness attribute within the IO that will identify suspicious behavior, transactions, and relationships between the client and the institution. Actions undertaken using this factor can contribute to establishing both a monetary and criminal trail.

In summary, the following advantages of using the AFCC method can be identified:

1) Early, temporally-initial stage of event information analysis;
2) Interpreting the event from the outset to identify "suspiciousness" within the reconnaissance analysis in the AML/CFT system based on risk assessment attributes and the adequacy of financial security measures;
3) Integrating the above-mentioned assessments with attributes resulting from the forensic characteristics crime of money laundering and terrorist financing;
4) Using the axiomatic factor k' of numbers assigned to the qualitative attributes of the system based on SAR/STR and notifications to the CU (prosecutor's office) in the metric assessment – to build conversion matrices in data sets and linear functions;
5) Obtaining a selected set of axiomatically characterized attributes as "hard" evidence in criminal proceedings.

Author Contributions

Matthias Alexander Kędzierski is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflict of interest.

References

[1] Wektory, przestrzenie wektorowe (2022), Matematyka na Wydziale Mechaniki i Inżynierii Środowiska Akademii Górniczo-Hutniczej, Kraków, wykład nr 2. [Vectors, vector spaces, Mathematics at the Faculty of Mechanics and Environmental Engineering, AGH University of Science and Technology, Cracov - lecture no. 2. (2022.)], Available from: https://home.agh.edu.pl/~rudol/M_2Srodow/Sr4.pdf (accessed: 5 December 2024).

[2] Granados, O. M., Vargas, A. The geometry of suspicious money laundering activities in financial networks. EPJ Data Sci. 11, 6 (2022), Available from: https://doi.org/10.1140/epjds/s13688-022-00318-w (accessed: 5 December 2024).

[3] Vagaská, A.; Gombár, M.; Korauš, A. Mathematical Modeling and Nonlinear Optimization in Determining the Minimum Risk of Legalization of Income from Criminal Activities in the Context of EU Member Countries. Mathematics 2022, 10, 4681.). Available from: https://doi.org/10.3390/math10244681 (accessed: 5 December 2024).

[4] Коновалова, В. Е., Колесниченко, А. Н. (1984). Теоретические проблемы криминалистической характеристики. Криминалистическая характеристика преступлений, (14), 16-23. С. 7—16. [Theoretical problems of forensic characterization. Forensic characterization of crimes, (14), 16-23. P. 7-16].

[5] Веренич И. В., Кустов А. М., Прошин В. М. Криминалистическая теория механизма преступления: моногр., [Forensic theory of the mechanism of crime: monograph]/ И. В. Веренич, А. М. Кустов, В. М. Прошин; Под науч. ред. А. М. Кустова, 2014. — s. 640. Available from: http://lawlibrary.ru/izdanie2296104.html (accessed: 31 October 2024).

[6] Колесниченко А. Н. Актуальные проблемы тактики и методики расследования преступлений [Current issues in tactics and methods of crime investigation]/ А. Н. Колесниченко, В. Е. Коновалова // Проблемы социалистической законности [Problems of socialist legality]. – Харьков: Вища шк., 1978. – Вып. 3. – С, s. 96, Available from: https://dspace.nlu.edu.ua/jspui/handle/123456789/4325 (accessed: 31 October 2024).

[7] Valentina, Korzh. "Forensic Characterization of Economic Crimes Committed by Organized Groups with Corruption Relations." *Theory and Practice of Forensic Science and Criminalistics* 35, no. 2 (2024): pp. 44-57. Available from: https://doi.org/10.32353/khrife.2.2024.04 (accessed: 5 December 2024).

[8] Korchagin, A., O. Bespechniy, and A. Sokolov. "Forensic characterization of the judicial investigation: the concept and meaning." *International Conference on Sustainable Development of Cross-Border Regions: Economic, Social and Security Challenges (ICSDCBR 2019)*. Advances in Social Science, Education and Humanities Research, volume 364. Atlantis Press, 2019. pp. 570-573 Available from: https://www.atlantis-press.com/proceedings/icsdcbr-19/125922350 (accessed: 5 December 2024).

[9] Malewski H., 2010, Kryminalistyczna charakterystyka przestępstwa – ważny element metodyki kryminalistycznej czy sztuka dla sztuki? [Forensic characterization of a crime – an important element of forensic methodology or art for art's sake?] [w:] Gruza E., Goc M., Tomaszewski T. (red.), Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości?, Warszawa, s. 127 [What's new in criminology – an overview of issues related to combating crime?, Warsaw, p. 127].

[10] P. Gilmour, B. Omondi, H. Feyza Alkaç B. Han, A. Carre, D. Kapardis, C. Halfpenny, Reexamining the 'Placement–Layering– Integration' Model of Money Laundering Available from: https://brianforensics.com/wp-content/uploads/2024/11/Institute-Report-Reexamining-the-PLI-Model-of-Money-Laundering.pdf (accessed: 28 November 2024).

[11] Schott P. A., Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, 2006, Available from: https://documents1.worldbank.org/curated/pt/982541468340180508/pdf/634980WP0Refer00Box0361517B0PUBLIC0.pdf (accessed: 1 December 2024).

[12] Kędzierski M. A., Informacja, ryzyko i taktyka w kontekście przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, Wydawnictwo Adam Marszałek, Toruń 2024, s. 971. ISBN: 978-83-8180-766-1; [monografia], s. 70-71; Kędzierski M. A., [Information, risk and tactics in the context of counteracting money laundering and terrorism financing, publishing house Adam Marszałek, Toruń 2024, p. 971. [monograph], pp. 70-71].

[13] Bloemkolk I. C., 2015, The European Fight Against the Financing of Terrorism, A study of the European Union's Third AML/CFT Directive, University of Twente.

[14] Rasiowa H., Wstęp do matematyki współczesnej, Wydawnictwo Naukowe PWN, Warszawa 2012, Wydanie XIV. [Introduction to Modern Mathematics, PWN Scientific Publishing House, Warsaw 2012, 14th Edition].

[15] Elementarna teoria mnogości, Rozdział 2 (2011) Zbiory i działania na zbiorach, [Elementary Set Theory, Chapter 2 Sets and Operations on Sets], Available from: https://www2.im.uj.edu.pl/LeszekPieniazek/DU/ELTM/test-2.html (accessed: 29 November 2024).

[16] Бахтеев Д. В. Ситуационный характер процесса расследования преступлений: проблемные ситуации и подходы к их разрешению // Российский Юридический Журнал. 2013. №1. [Bakhteyev D. V. Situational nature of the crime investigation process: problem situations and approaches to their resolution // Russian Law Journal. 2013. No. 1] [w] . Бахтеев Д. История развития теории следственных ситуаций в отечественной криминалистике/ Дмитрий Валерьевич Бахтеев// Российский юридический журнал.- 2018.- № 1.- С. 193 – 202. [History of the development of the theory of investigative situations in domestic forensic science / Dmitry Valerievich Bakhteev // Russian Law Journal. - 2018. - No. 1. - P. 193 - 202.] Available from: https://www.calameo.com/read/00601769599f9131a2ab3

[17] Sądowy impas wokół 1, 4 mld zł. Pieniądze z narkobiznesu czy depozyty klientów? Portal: Money. pl, 2025, Court Deadlock Over PLN 1.4 Billion. Drug Deal or Customer Deposits? Portal: Money. pl, 2025, Available from: https://www.money.pl/gospodarka/sadowy-impas-wokol-1-4-mld-zl-pieniadze-z-narkobiznesu-czy-depozyty-klientow-7216764622801504a.html (accessed: 8 November 2025).

[18] Efendi Lod Simanjuntak, Trinaili, Y.., Purwono, & Md Said, M. H.. (2025). The Convergence of Classical Punishment in Money Laundering: Follow the Money Principle Using Blockchain Approach. *Lex Publica*, *12*(1), pp. 264–290. Available from: https://doi.org/10.58829/lp.12.1.2025.298 (accessed: 8 November 2025).