Annex 1: False positives in AML/CFT compliance: their nature and consequences

General definition: **legitimate transactions flagged as suspicious by financial compliance systems** (e.g. banks, cryptocurrency exchanges, crowdfunding platforms). They can occur *accidentally* or be the result of *malicious (targeted)* actions against the person or entity in question by undermining their reputation. Upon further review, if carried out diligently (taking into account the sources of information in question), nothing suspicious would be found.

As indicted in the research paper published by the Italian Economic Journal (May 2022), apart from the detriment of the interests of law-abiding customers, they lead to ***Excessive and useless reporting****, known as the "crying wolf effect" (Takats 2011), is a crucial shortcoming that any anti-money laundering (AML) design aims to address and fix. The "crying wolf effect" harms the informational value of reports that banks and other professionals are obliged to file to comply with AML regulations.*[54]

Type	Description	How it works (examples)	Case study
Random	Unusual commercial transactions	Transfers for not provided services or undelivered goods, despite previous arrangements, are returned to the sender	Priorité Energie, which helps low-income families in Paris to insulate their homes under a government initiative, had its funds frozen and was told by Revolut that it would no longer offer services to the company. After Priorité transferred money to one of its suppliers in Czechia, he supplier was unable to deliver the goods and returned the money (the situation was reported in 2020).
Random	Crowdfunding and other fundraising actions	Regular cash deposits (as result of fundraising/charity actions - money collected to boxes during charity events) or bank transfers flagged as suspicious activity due to their frequency, varying/unusual transaction amounts or their form (cash). It may also stem from associations with specific, flag-raising context and keywords (support for Ukraine's military, body armours, helmets etc.)	Open Dialogue Foundation, other pro-Ukraine individuals and initiatives collecting funds and donating to the Ukrainian military or war-related humanitarian causes

[54] https://link.springer.com/article/10.1007/s40797-022-00195-2

Malicious	Smear campaign - fake news or overall negative publicity in the media/social media (even indirect - related to actual or perceived associates)	Politically motivated press and social media attacks accusing the customer of criminal activity, bogus commercial interests, links to sanctioned countries etc. carried out by non-democratic (e.g. Kazakhstan) and hybrid regimes as well as Western companies acting on their behalf to influence journalists and business intelligence firms (e.g. Refinitiv, Dun & Bradstreet)	Retaliatory attacks on Open Dialogue Foundation for criticism of human rights and rule of law violations in Kazakhstan, in Plahotniuc's Moldova and Poland since 2017; the same *modus operandi* in the cases of Kazakh, Belarusian, Russian and Turkish activists in exile
Malicious	Political prosecution by home or third countries and legal assistance requests	Dubious, politically motivated criminal investigations into alleged fraud, money laundering, extremism, terrorism, espionage etc. publicised in the media or transmitted to local law enforcement via mutual, European or bilateral legal assistance frameworks requesting banking data under a pretext of seeking evidence. Once a bank is approached by police or prosecutor's office with a request to disclose information on a person/entity in question, it flags the customer as highly suspicious and, subsequently, the bank terminates the customer's accounts	Retaliatory attacks on Open Dialogue Foundation for criticism of human rights and rule of law violations in Kazakhstan, in Plahotniuc's Moldova and Poland, included legal assistance requests from Poland (as European Investigative Orders) and from Moldova to Belgian authorities in 2019-2022;the same *modus operandi* in the cases of Kazakh, Belarusian, Russian and Turkish activists in exile

Malicious	Arbitrary designation as security threat	Secret opinions issued by special/security/intelligence services labeling customers as security threat for obscure reasons, which leads to their data being included in the national and European (Schengen Information System) databases of undesirable persons for political purposes - if publicised by e.g., the spokesperson of special services, they result in red flags at financial institutions. Also, as a part of politically motivated persecution, security and law enforcement services from different countries may exchange information concerning the customers and, request banking data flagging the customer. In the process of fulfilling this request, the bank may flag the customer as suspicious and trigger AML/CFT monitoring procedures.	Lyudmyla Kozlovska and Open Dialogue Foundation controversially labelled as security threat by rule-of-law rogue Poland in 2018 Ismail Sezgil, an exiled Turkish opposition political commentator had his accounts blocked and funds frozen in the UK and EU when Turkey's government published his data on the list of the Fethullahist Terrorist Organisation (FETO) alleged members. Kazakhstan, Belarus, Russia also abuse accusations of extremism, being a threat to the national security with the same pattern of targeting the activists in exile and those associated with them. The details are in the testimonials.
Random	Legitimate transactions involving high-risk country flagged as suspicious, based solely on their location or customers' countries of origin or customers'names	Geographic location of the transaction serve as the only indication of suspicious transaction, without considering the actual transactional activity (e.g. support for opposition movements or family members)	Navalny's Foundation, Interim Government of Venezuela, BYSOL Foundation supporting anti-corruption and opposition activities, as well as supporting politically persecuted persons and their families in Russia and Belarus. Migrants and refugees from sanctioned countries or occupied territories (Donbas, Crimea)

Random	Use of crypto-assets	Donations received by an NGO from anonymous donors via its self-hosted wallet are transferred to the NGO's account on the cryptocurrency exchange - donors' anonymity raises compliance flags. Transfers from accounts on cryptocurrency exchanges to bank accounts deemed high-risk by banks due to the very use of crypto-assets, despite their intended purpose (donations for legitimate purposes), and difficulty of identifiying each donor.	Open Dialogue Foundation and emergency donations for Ukraine's support, Navalny's Foundation, Interim Government of Venezuela, BYSOL Foundation