

Guidance on Detecting and Reporting Proliferation Financing Cases for Reporting Entities

Overview

Proliferation financing (PF) refers to the movement or provision of funds or financial services that support the development, acquisition, or transportation of weapons of mass destruction (WMD) and their delivery mechanisms. As part of its international obligations, the Republic of Armenia (RA) is committed to identifying and preventing such financial activity.

In line with Recommendation 7 of the Financial Action Task Force (FATF), the RA is required to implement targeted financial sanctions against individuals and entities involved in PF, based on United Nations (UN) Security Council resolutions. This guidance is intended to assist reporting entities (RE) in meeting these obligations. It outlines key responsibilities, practical red flag indicators (behavioural, transactional, and contextual), and step-by-step instructions for conducting due diligence, transaction monitoring, sanctions screening, and internal reporting or escalation.

By consistently applying these measures, REs in the RA play a vital role in upholding national security and contributing to global efforts to prevent the spread of weapons of mass destruction.

Core Responsibilities under PF Controls

1. Enforcing Targeted Financial Sanctions

REs must strictly comply with PF-related targeted financial sanctions. FATF Recommendation 7 requires the immediate freezing of assets and the prohibition of any financial services or resources being made available to sanctioned individuals or entities. In practice, this means screening all customers and transactions against the most recent UN sanctions lists and freezing any assets tied to listed persons without delay. No business should be conducted with individuals or organizations appearing on these lists.

2. Customer Due Diligence (CDD) and Risk Assessment

Thorough customer due diligence must be conducted at the start of the business relationship and maintained throughout. This includes identifying and verifying the identities of all beneficial owners and controllers. It's critical to understand the customer's line of business and assess whether it may present exposure to PF risks—such as involvement in the trade of dual-use goods or links to high-risk jurisdictions. Enhanced due diligence is required for customers with elevated risk factors, particularly those with potential ties to countries, sectors, or goods associated with PF.

3. Transaction Monitoring for PF Risks

Monitoring systems should be in place to detect unusual or potentially high-risk transactions, particularly those that may involve PF. This includes monitoring trade

finance activity, wire transfers, and other forms of payment. Transactions that involve sensitive goods, sanctioned destinations, or complex structures (such as the use of intermediaries or convoluted payment routes) warrant additional scrutiny. Both automated monitoring rules and manual reviews should be calibrated to detect red flags—for example, a customer unexpectedly transacting with a sanctioned country or engaging in activity inconsistent with their known profile.

4. Sanctions Screening

All relevant parties must be screened against current sanctions lists—not just at onboarding, but on an ongoing basis. This includes customers, beneficial owners, transaction counterparties, and, where applicable, associated agents, shipping vessels, or intermediaries. Screening should cover UN sanctions regimes such as those under UNSCR 1718 (Democratic People’s Republic of Korea). Sanctions lists must be updated promptly in line with new designations by the UN. Advanced screening techniques, including fuzzy matching, should be used to detect variations or aliases of sanctioned names. Any potential matches must be escalated immediately in accordance with the RE’s internal procedures.

5. Internal Controls and Staff Training

REs must maintain internal policies and procedures to manage PF risks in accordance with RA legislation and FATF Standards. Staff across all functions—such as client-facing roles, compliance, AML teams, and trade finance—should be trained to recognize red flags and understand their obligations under sanctions regimes. Training programs should include real-life case examples of proliferation financing methods and stress the importance of adherence to legal and regulatory requirements. Training must be kept up to date as new threats and typologies emerge.

6. Cooperation with Authorities

REs are expected to work closely with national authorities on matters related to AML/CFT/CPF. For example, bodies represented in the Interagency Committee on Combating Money Laundering, Terrorism Financing, and Financing of Proliferation of Weapons of Mass Destruction play a central role in shaping national policies, conducting risk assessments, and facilitating cooperation. Compliance teams must fulfil their responsibilities by reporting suspicious transactions promptly to the Financial Monitoring Center of the Central Bank of Armenia (FMC).

Behavioral Red Flags

Compliance staff should be attentive to customer behaviour that may signal underlying PF risks. While a single red flag may not, on its own, confirm suspicious activity, patterns of concerning behaviour—or a particularly strong individual indicator—should trigger closer examination and potentially enhanced due diligence.

1. Evasive or Reluctant Behaviour

A customer who avoids providing complete or clear information, or who appears unusually secretive about their operations, warrants extra scrutiny. For example, clients who refuse to identify the end-users of goods or withhold details about beneficial ownership raise immediate concern. Vague or inconsistent responses during the KYC process, the use of misleading statements, or the submission of obviously fake documentation should be treated as serious warning signs.

2. Negative Background or Known Associations

If a customer—or one of their beneficial owners—has a history of involvement in sanctions breaches, illicit trade, or other financial crimes, the PF risk is elevated. Open-source media reporting on attempts to smuggle sensitive goods, for instance, is a red flag. Similarly, if a client appears on an export control authority's denied-party list, this should prompt further investigation and may justify enhanced monitoring or restrictions.

3. Mismatch between Business Profile and Activity

An inconsistency between the customer's stated business and their actual transactions may suggest concealment. For example, a newly incorporated company with no verifiable track record that suddenly engages in high-value international trade of technical equipment beyond its declared scope is suspicious. Likewise, a family-run food trading firm inexplicably shipping chemicals or electronic components should raise questions about the true nature of the business.

4. Opaque or Complex Ownership Structures

The use of shell companies, multiple layers of ownership, or nominee shareholders without any clear business justification may be a deliberate attempt to obscure a sanctioned person's involvement. If identifying the ultimate beneficial owner (UBO) is difficult—or if shares are held by entities based in secrecy jurisdictions—compliance officers should consider the possibility of a hidden link to a designated individual. Armenian legislation treats companies owned or controlled, directly or indirectly, by listed persons as subject to sanctions.

5. Excessive Secrecy or Unusual Urgency

Clients who push for rapid execution of transactions—especially those involving high-risk countries—or who pressure staff to bypass normal due diligence protocols should be treated with caution. A sense of urgency without a legitimate explanation, especially when paired with secrecy, can be a tactic to move funds or goods before sanctions screening catches up. This behaviour may indicate an attempt to avoid detection or enforcement measures.

Transactional Red Flags

Certain transaction patterns may indicate a link to PF, especially when they are inconsistent with a customer's business profile or involve jurisdictions, goods, or

behaviours associated with WMD procurement networks. Below are key transactional red flags that should prompt closer scrutiny:

1. Dealings with High-Risk Jurisdictions

Transactions involving countries subject to PF-related targeted financial sanctions—or those known to be used as transshipment hubs by sanctioned actors—warrant immediate attention. This includes direct or indirect payments involving sanctioned areas, as well as transfers routed through third countries where sanctioned entities are known to operate. Even if the immediate counterparty is based in a neutral jurisdiction, if they are known to procure goods on behalf of a sanctioned state, the transaction should be considered high risk.

2. Use of Shell or Front Companies

Payments routed through multiple companies or accounts with no clear economic rationale may indicate efforts to disguise the true beneficiary. Shell or front companies—particularly newly created firms with minimal capital or no operational footprint—can be used to conceal a proliferator’s involvement. When funds flow through several unrelated businesses or offshore entities with no transparent commercial purpose, this may signal an attempt to obscure a sanctions connection.

3. Trade Involving Dual-Use or Controlled Goods

Transactions that reference goods with both civilian and military applications—commonly referred to as dual-use goods—or items found on export control lists should raise concern, especially if such products are inconsistent with the customer’s usual line of business. This includes commodities such as specialized metals, high-performance electronics, or chemical precursors. If such transactions are directed toward high-risk destinations, the likelihood of PF involvement increases significantly.

4. Sanctioned or Embargoed Goods

Deals involving explicitly prohibited goods are among the clearest indicators of PF risk. These include weapons, certain petrochemical products, and luxury items banned under regimes like those targeting Democratic People’s Republic of Korea. If trade documentation—such as a letter of credit or wire transfer instructions—suggests the movement of embargoed items (e.g. military-grade technology or luxury goods destined for sanctioned countries), the RE should treat the transaction as suspicious and potentially linked to sanctions evasion.

5. Irregularities in Trade Documents

Falsified or suspicious trade finance documentation is a strong PF warning sign. Examples include fake or altered Bills of Lading, invoices, or customs documents, or paperwork with unusual inconsistencies—such as mismatched fonts, missing data, or unexplained amendments. Vague or misleading product descriptions (e.g. labelling advanced electronics as “spare parts”) are often deliberate attempts to disguise the true

nature of the transaction. Any such irregularities should trigger efforts to verify the documents' authenticity and the legitimacy of the trade.

6. Unusual Payment Patterns

Payment activity that defies commercial logic may signal PF. This includes “smurfing” techniques, where large payments are split into multiple smaller ones across different accounts or jurisdictions to avoid detection. A sudden spike in wire transfers by a previously low-activity account, or funds being routed through a series of intermediaries for no clear business reason, may also be cause for concern. Roundabout or circuitous payment paths often indicate attempts to mask the origin or destination of funds.

7. Mismatched Values or Over/Under-Invoicing

Discrepancies between the value of goods and the declared financial amounts in related transactions can point to PF. For example, if the reported shipment value is well below market rates—or even less than the cost of shipping—it may suggest that the true purpose of the transaction is being concealed. Similarly, an account belonging to a small, low-revenue business processing multi-million-dollar transactions labelled as generic purchases (e.g. “construction equipment”) should raise questions. Such anomalies may be efforts to move value on behalf of proliferators under the guise of legitimate trade.

8. Third-Party Payments and Use of Cash

When payment for goods or services is made by a third party with no apparent link to the transaction, this may indicate an attempt to conceal the true buyer or beneficiary. Similarly, the use of cash in international trade—where electronic payments are the norm—is highly unusual and may signal efforts to avoid financial traceability. Large or structured cash deposits followed by outbound international transfers should also be treated as potential indicators of PF-related activity.

Contextual Red Flags

Beyond customer behaviour and transaction activity, certain contextual elements can also indicate a heightened risk of proliferation financing. These factors provide important background that may not be obvious at first glance but can significantly alter the risk profile of a transaction or relationship. Compliance teams should remain alert to the broader context surrounding clients, counterparties, goods, and jurisdictions.

1. Links to Proliferation-Risk Jurisdictions

If a customer, beneficial owner, or transaction counterparty is based in—or maintains strong business connections with—a country of proliferation concern (such as the DPRK), this should trigger enhanced scrutiny. Even if the party is not directly listed under sanctions, their jurisdictional ties alone increase the likelihood of indirect involvement in sanctioned activities.

2. Unusual End-Use or End-User

In trade finance, understanding who the final recipient of goods is—and what those goods will be used for—is essential. A red flag arises when the stated end-user is a military or research entity in a high-risk jurisdiction, or when the customer is unable to credibly explain the end-use of dual-use items. For example, a client claiming to ship “laboratory equipment” to a newly formed firm in a third country—when in fact the items are highly specialized instruments—could be concealing diversion to a WMD-related program. A mismatch between the technical sophistication of the goods and the capabilities of the receiving country’s civilian industry should also raise concern.

3. Denied Parties and Export Control Lists

In addition to standard sanctions lists, many governments maintain export control watch lists that include individuals and entities denied export privileges due to prior proliferation-related activities. If a customer or related party appears on such a list—or has previously been refused an export license—that history should be treated as a serious red flag. It signals that the entity has already been identified as a potential risk by authorities.

4. Activity in High-Risk Sectors

Certain industries are inherently more vulnerable to proliferation financing, including arms manufacturing and trade, aerospace technology, chemicals, and nuclear materials. If a customer operates in—or suddenly enters—these sectors, their transactions should be monitored more closely. Additional contextual risk arises from transactions involving freight forwarders or shipping firms with a history of operating in grey areas—such as frequent changes in vessel flags, transit through sanctioned ports, or routing via conflict zones.

5. Use of Concealment Tactics

Proliferators often go to great lengths to hide their involvement in financial and trade transactions. Watch for indicators such as businesses registered under the names of family members or associates, sudden changes in ship names or ownership before carrying sensitive cargo, or the involvement of intermediaries (e.g. lawyers, brokers) in unusual roles. If a deal features an overly complex chain of intermediaries or routes through multiple secrecy jurisdictions without a clear commercial rationale, it may be an attempt to mask the participation of a designated entity.

In summary, contextual red flags provide crucial background insight and should not be overlooked. The presence of one or more of these indicators should trigger a more in-depth review of the relationship or transaction. Where concerns persist, enhanced due diligence, close monitoring, or formal reporting procedures should follow, as outlined in the next sections.

Enhanced Due Diligence and Screening Measures

When a potential PF risk is identified—or when dealing with clients who fall into higher-risk categories—compliance teams should follow a structured enhanced due diligence (EDD) process. These measures go beyond standard customer due diligence and are designed to uncover hidden risks, clarify suspicious activity, and ensure regulatory compliance.

1. Conduct a Thorough Know-Your-Customer (KYC) Review

Reassess and update the customer's identity, ownership structure, and business activities. Ensure you have the latest, most accurate information on all beneficial owners and controllers. For legal entities, obtain clear documentation outlining the ownership structure and screen each individual involved against current sanctions lists.

Keep in mind that sanctioned individuals may not appear as named clients—they might be concealed as directors, shareholders, or silent partners. RA law considers entities owned or controlled, directly or indirectly, by designated persons as subject to sanctions. Therefore, uncovering indirect control is essential. Use corporate registries, publicly available information, and third-party intelligence to determine who is ultimately behind the business.

2. Clarify the Purpose and Nature of Transactions

Ask the customer to explain the intended use of their account and provide details about specific transactions. If the activity involves goods or international trade, request documentation such as contracts, invoices, end-user certificates, and relevant import/export licenses.

For example, if a client is sending funds to purchase industrial machinery, confirm exactly what is being bought, who the end-user is, and whether the destination country poses any risks. A legitimate customer should be able to provide clear, consistent documentation demonstrating lawful end-use, especially if the transaction involves controlled or dual-use items. Ambiguous or inconsistent information should be treated as a potential red flag.

3. Perform Additional Sanctions and Watch List Screening

For all high-risk transactions and clients, conduct extra screening steps before proceeding:

- **Sanctions Lists:** Screen all involved parties—including customers, recipients, agents, shipping firms, and intermediaries—against UN sanctions lists related to WMD proliferation, particularly those concerning Democratic People's Republic of Korea, and other relevant regimes. Use a reliable, up-to-date screening tool. If a party is an exact or close match to a designated individual or entity, pause the transaction and escalate internally.
- **Other Watch Lists:** Check additional PF-related targeted financial sanctions lists, including denied persons lists from export control authorities, entities flagged in

FATF or UN typology reports, and domestic lists issued by Armenian regulators. These sources can reveal risky connections not found on standard sanctions lists.

- **Adverse Media Screening:** Conduct a brief open-source search for any news reports, academic publications, or expert panel findings that link the client or transaction parties to proliferation networks, illicit trade, or sanctions evasion. Such references—while not always definitive—can provide valuable context and should inform your risk assessment.

4. Apply Risk-Based Controls for High-Risk Clients or Transactions

If a customer or transaction is deemed high risk from a PF perspective, consider applying one or more of the following enhanced measures:

- Increase the frequency and depth of transaction monitoring.
- Require sign-off from senior management for any high-value or unusual transactions.
- For trade finance clients, verify the authenticity of transport documentation (e.g. bills of lading) using trusted shipping databases.
- Regularly compare the customer's activity—especially in relation to dual-use goods—with their declared business profile to spot inconsistencies early.
- Restrict certain high-risk services (e.g. transfers involving sensitive products or high-risk jurisdictions) unless additional checks are completed and approved.

5. Maintain Ongoing Monitoring and Update Risk Profiles

A customer's risk level is not static—it must be reviewed and updated as new information emerges. For example, if a new director joins the company and is later found to be linked to a sanctioned entity, or if the client begins transacting with unfamiliar or high-risk jurisdictions, the compliance team must reassess the risk and update due diligence records accordingly.

Ensure your system performs continuous sanctions screening—nightly batch screening of the entire customer database is a recommended practice. This allows you to detect if a current client is added to a sanctions list and take action without delay. RA legislation requires sanctions to be implemented “without delay,” so your RE's systems and procedures must be capable of responding immediately to new designations announced by the UN or RA authorities.

Detecting Indirect Links to Sanctioned Persons or Entities

Sanctioned individuals and entities frequently attempt to circumvent financial controls by operating through intermediaries, shell companies, or affiliates that do not appear on official sanctions lists. This practice is a common method of sanctions evasion, and detecting these indirect connections is essential to effective PF risk management.

In line with FATF Recommendation 7, REs are obligated to prevent funds or services from reaching designated persons **either directly or indirectly**. That means your

responsibilities extend beyond basic list-checking—into identifying hidden relationships that may not be obvious at first glance.

What Constitutes an Indirect Link?

Indirect connections to sanctioned individuals or entities can take various forms, including:

- **Ownership:** A sanctioned person directly or indirectly owns 50% or more of a company. Under UN guidance—such entities are treated as sanctioned, even if not explicitly named.
- **Control:** A sanctioned individual exercises influence over a company through board seats, veto powers, contractual arrangements, or by shaping business decisions—regardless of their ownership share.
- **Close Associates:** Friends, family members, business partners, or employees acting on behalf of a designated person. The involvement of known associates should be treated as a high PF risk indicator.
- **Shared Identifiers:** Commonalities such as addresses, phone numbers, email domains, or IP addresses shared with a sanctioned entity suggest a potential hidden connection.
- **Shell Companies:** Firms with no substantive operations, often set up for the sole purpose of disguising the involvement of a designated party.
- **Third-Party Intermediaries:** Lawyers, agents, consultants, or service providers who act as proxies for sanctioned persons—either knowingly or unknowingly.

How to Detect Indirect Links: Practical Measures

1. Beneficial Ownership Checks

- Investigate multi-layered ownership structures to determine the true ultimate beneficial owners (UBOs).
- Screen all individuals and controlling parties against applicable sanctions lists.
- Escalate any client who refuses to fully disclose ownership details or provides incomplete information.

2. Advanced Screening Tools

- Use tools with fuzzy logic capabilities to detect spelling variations, aliases, and transliterations.
- Go beyond name screening: include addresses, emails, domain names, IP addresses, and vessel identification numbers.
- Ensure your screening systems incorporate “ownership and control” data from reliable sources.

3. Open-Source Intelligence (OSINT) and Adverse Media

- Regularly search open sources—such as news outlets, company registry leaks, sanctions-related publications, and investigative databases—for links between clients and known proliferators.
- Pay attention to repeated associations with sanctioned entities, such as shared contact details or business networks.

4. Red Flags

Be alert for indicators that may point to indirect involvement, such as:

- Sudden changes in ownership shortly after a sanctions designation.
- Multiple companies sharing identical contact details or addresses.
- Complex corporate structures involving secrecy jurisdictions or nominee ownership.
- Unexplained third-party payments or intermediaries unrelated to the underlying business.
- Customers who are evasive or unwilling to provide supporting documents when requested.

5. Ongoing Monitoring

- Re-screen clients and associated parties on a periodic basis.
- Update beneficial ownership records regularly, especially for high-risk industries or cross-border operations.
- Treat changes in a client's ownership, control, or business model as triggers for enhanced due diligence.

Key Reminder

A company or individual **does not need to be named on a sanctions list to be subject to sanctions**. If they are owned or controlled by a designated person, they are legally considered sanctioned under most frameworks. When in doubt, treat the case as high risk until you can confirm otherwise.

Identifying indirect links is not just a regulatory formality—it's a critical step in preventing sanctioned actors from exploiting the financial system through deceptive means. Your diligence in this area plays a direct role in disrupting global proliferation networks.

This guidance should serve as a practical reference for daily operations. When faced with uncertainty, it is always better to err on the side of caution and consult with the MLRO or competent authorities.

By staying alert, REs not only protect themselves from regulatory or reputational harm—they contribute meaningfully to national security and global peace. Compliance in this space isn't just about avoiding penalties; it's about preventing the catastrophic consequences that can arise when proliferators gain access to financial resources.