

Comparison: Terrorist Financing, Money Laundering, and Financing the Proliferation of Weapons of Mass Destruction

This table displays differences and similarities between critical concepts in combatting financial crime. These are:

- › Terrorist Financing (**TF**)
- › Money Laundering (**ML**)
- › Financing the Proliferation of Weapons of Mass Destruction (**PF**)

It is designed to assist Industry in its understanding of the differences and similarities between TF, ML and PF, supporting our common efforts to identify and mitigate these activities:

- › Anti-Money Laundering (**AML**)
- › Countering the Financing of Terrorism (**CFT**)
- › Countering Proliferation Financing (**CPF**)

| | Terrorist financing | Money laundering | Financing the proliferation of weapons of mass destruction |
|------------------------|---|--|---|
| Motive | Support acts of terrorism, terrorists, and terrorist organisations. | Enable the proceeds of crime to appear legitimate. | Enable the proliferation of weapons of mass destruction. |
| Source of Funds | <p>From illegitimate/legitimate activities</p> <p>Numerous funding streams, including, for example:</p> <ul style="list-style-type: none"> › Sponsored by financier/benefactor sympathetic to the cause › Self-funded › Funds raised via commercial activities (e.g. web shops, music festivals) › Funds raised via organised fund-raising activities (e.g. via non-profit sector, social media, crowdfunding platforms, groups’ own magazines) › Exploitation of natural resources in conflict zones (e.g. ISIL – Oil in the Middle East; Al-Shabaab – Gold in West Africa and Daesh – Timber in East Africa) | <p>From illegitimate activities.</p> <p>Funded via the illicit activity of the criminal/criminal organisation. For example, corruption, tax evasion, the sale of drugs, robberies, ransomware attacks, illegal arms trade, prostitution etc. The crime may not have been committed in Jersey</p> <p>Organised crime groups may collaborate with terrorists and may also be classified as proscribed terrorist organisations.</p> | <p>From illegitimate/legitimate activities.</p> <p>May ultimately be State sponsored but may also emanate from non-State actors, often utilising proliferation networks. Funding may, for example, emanate from ransomware attacks.</p> |

| | Terrorist financing | Money laundering | Financing the proliferation of weapons of mass destruction |
|-------------------------------|---|---|--|
| | <ul style="list-style-type: none"> › Looting and sale of cultural artifacts › Real estate (generating income, acting as an investment, and which certain terrorist groups use as club houses etc.) <p>It is not unusual for terrorists to be involved in, or operating in close proximity to, conflict zones and criminal methods to raise funds tend to emerge, either in isolation or working with criminal groups (e.g. illicit smuggling, human trafficking, extortion, drugs trafficking and kidnap for ransom).</p> <p>The United Nations reports that during the COVID-19 pandemic cash smuggling to territories where Daesh was active became less prominent, whilst crypto transfers increased (e.g. using personal crypto wallets).</p> | | |
| Money trail and stages | <p>Linear – funds are used to promote and finance terrorists and their activities, as well as their infrastructure, by <i>raising, storing, moving and using funds</i>. None of these stages need to be associated with violence.</p> | <p>Circular – the funds eventually tend to end up with the person who generated them, once the funds have been sufficiently distanced from the crime (e.g. via self-laundering, professional money laundering or third-party laundering by enablers/facilitators) by <i>converting, concealing and disguising</i> the true nature and source.</p> | <p>Linear – funds tend to be used to purchase materials and goods from manufacturers, traders etc.</p> |

| | Terrorist financing | Money laundering | Financing the proliferation of weapons of mass destruction |
|---------------------------------------|---|--|--|
| | | The more traditional model of money laundering stages refers to <i>placement, layering and integration</i> , however, this model does not take into account circumstances which do not require all those stages, e.g. tax evasion. | |
| Monetary value | Both small and large sums. Small in order to fall below reporting thresholds and limited expenses are often required to carry out an attack. Typologies, for example, show use of low-limit pre-paid cards. | Tends to be larger sums. On a risk-based approach smaller sums may sometimes be considered to present limited money laundering risk. | Both small and large sums. |
| Financial activity and sectors | Multiple, varied methods, e.g. formal banking system, informal value transfer systems, smuggling of valuables (precious metals and stones, antiquities) and cash. Exposure to all sectors. For example procurement of weapons (including knives) and vehicles (including car hire businesses). | Complex structuring and web of transactions which may involve using front companies, i.e. businesses set up to provide a plausible cover for illicit activities. Including, for example, cash-intensive businesses (such as restaurants, convenience stores and nail bars), bearer shares and secrecy havens. Exposure to all sectors. For example purchase of luxury items with tainted/criminally obtained funds. | Complex structuring – structured to hide the origin of the funding as well as what funds/assets are ultimately intended to be used for. Exposure to all sectors. For example purchase of dual use items such as engine parts. |
| Conduits | Tends to favor formal/regulated financial | Tends to favor formal/regulated | Tends to favor formal/regulated |

| | Terrorist financing | Money laundering | Financing the proliferation of weapons of mass destruction |
|--|--|---|--|
| | system, however may also use other means (e.g. crypto assets). | financial system, however may also use other means provided the final stage of the laundering process creates the perception of untainted, legitimate funds/assets. | financial system, however may also use other means (e.g. crypto assets). |
| Examples of red flags | Suspicious relationships such as wire transfers between seemingly unrelated parties. | Suspicious activities/transactions which appear uncharacteristic when compared with prior knowledge and expectations. | Often sophisticated – individuals, entities, States, goods, materials, activities. May involve false accounting/invoicing or other falsified documentation. |
| Cross-jurisdictional complexities? | Yes, this is not uncommon. | Yes, this is not uncommon. | Yes, this is not uncommon. |
| Differences in timing of criminal event | Combatting financing of terrorism requires vigilance as it may include preventing a <i>future</i> terrorist act from happening, however, TF does not require an act of terror to occur, e.g. it includes providing financial support to a terrorist or terrorist organization. | The criminal activity (predicate offence) has already taken place by the time that money laundering occurs. | Combatting financing of proliferation requires vigilance as it may include preventing a <i>future</i> act from happening, however, it suffices to provide financial support to a Proliferator. |