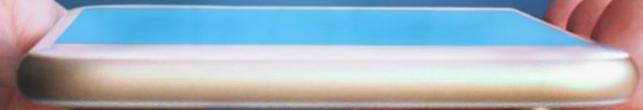


Re-Vision

Guideline
for the NEW



CDD and
AML/CFT



Why do we have to apply CDD and AML/CFT

policies and procedures in the NEW





Cryptocurrency is here to stay!

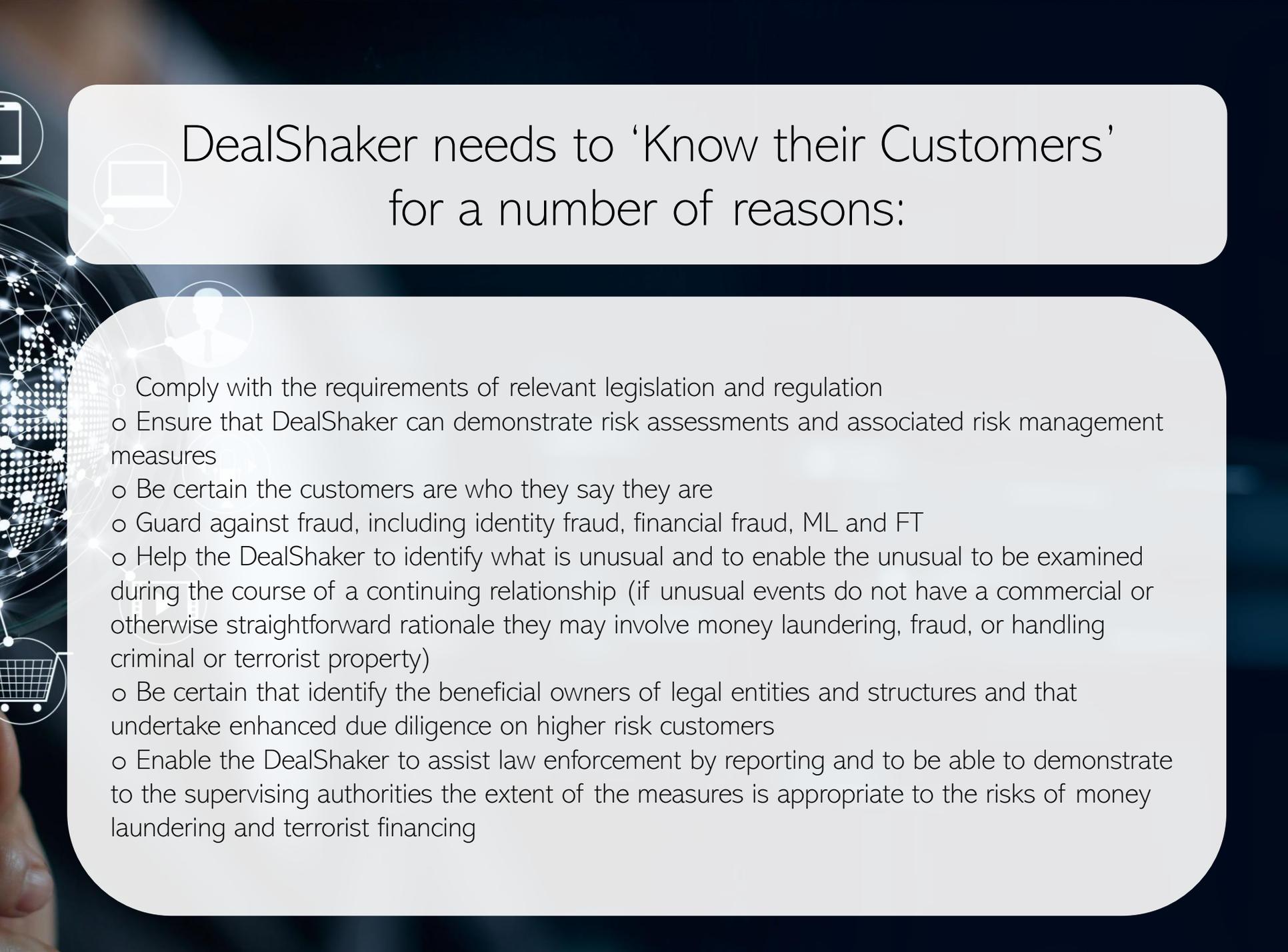
Thus regulations had to be applied.

The **G20** (or **Group of Twenty**) is an international forum for the [Governments](#) and [Central bank](#) governors from 19 countries and the European Union. On 02nd December 2018 they have decided:

Financial Action Task Force is going to Issue its Crypto Guidelines by Mid-2019 (June)

The move would be an upgrade from guidelines currently in place, which were first adopted by the FATF in June 2015 for global regulators to monitor cryptocurrencies. As we have been having a clear vision for the ways the regulations will change, we have been able to communicate them, to implement them and to use them in our daily work.

As professionals we have seen these implementations coming and we had applied them years ago.



DealShaker needs to 'Know their Customers' for a number of reasons:

- Comply with the requirements of relevant legislation and regulation
- Ensure that DealShaker can demonstrate risk assessments and associated risk management measures
- Be certain the customers are who they say they are
- Guard against fraud, including identity fraud, financial fraud, ML and FT
- Help the DealShaker to identify what is unusual and to enable the unusual to be examined during the course of a continuing relationship (if unusual events do not have a commercial or otherwise straightforward rationale they may involve money laundering, fraud, or handling criminal or terrorist property)
- Be certain that identify the beneficial owners of legal entities and structures and that undertake enhanced due diligence on higher risk customers
- Enable the DealShaker to assist law enforcement by reporting and to be able to demonstrate to the supervising authorities the extent of the measures is appropriate to the risks of money laundering and terrorist financing

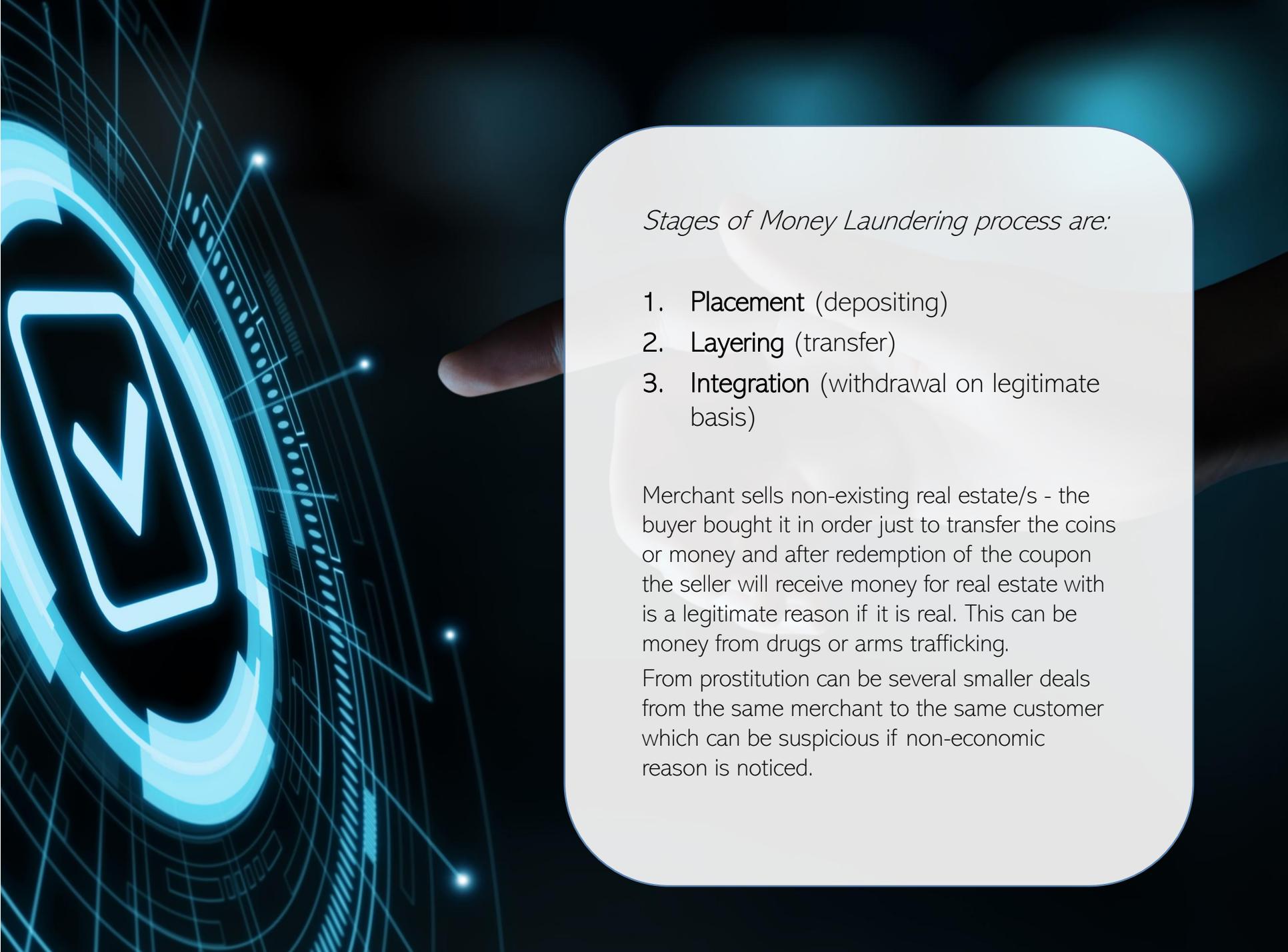
What is 'money laundering'?

Definition:

'Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.'

The nature of functioning of the Dealshaker (namely managing, controlling and possessing money and coins) means that it is vulnerable to abuse by money/coin launderers. Money laundering requires an underlying, primary, profit-making crime (such as corruption, drug trafficking, market manipulation, fraud, tax evasion), along with the intent to conceal the proceeds of the crime.





Stages of Money Laundering process are:

1. **Placement** (depositing)
2. **Layering** (transfer)
3. **Integration** (withdrawal on legitimate basis)

Merchant sells non-existing real estate/s - the buyer bought it in order just to transfer the coins or money and after redemption of the coupon the seller will receive money for real estate with is a legitimate reason if it is real. This can be money from drugs or arms trafficking.

From prostitution can be several smaller deals from the same merchant to the same customer which can be suspicious if non-economic reason is noticed.

Legitimate products and services can be used to mask illegal origins of funds

Example 1: MP from drugs and arms trafficking

1. Placement (depositing)

Placing a big amount of fiat or crypto in DealShaker

2. Layering (transfer)

The merchant sells a non-existent real-estate
The buyer purchase the non-existing property

3. Integration (withdrawal on legitimate basis)

Redemption of the coupon for the non-existing property. Money transfer for a large amount

Example 2: ML from prostitution

1. Placement (depositing)

Placing a small amount of fiat or crypto in the DealShaker platform

2. Layering (transfer)

Placing small deals on the DealShaker platform (furniture, gold, cars)

3. Integration (withdrawal on legitimate basis)

Redemption of the purchased coupons

Legitimate products and services can be used to mask illegal origins of funds

Illegal activities are difficult to be distinguished due to the irregular activities on the DealShaker platform.

Such as:

- Sale of coins and or transfer of coins
- Targeted purchase of goods/services for coins with the sole purpose of a subsequent sale for fiat

!NB Please be informed that irregular activities on the DealShaker platform are strictly forbidden!

What is 'financing of terrorism'?

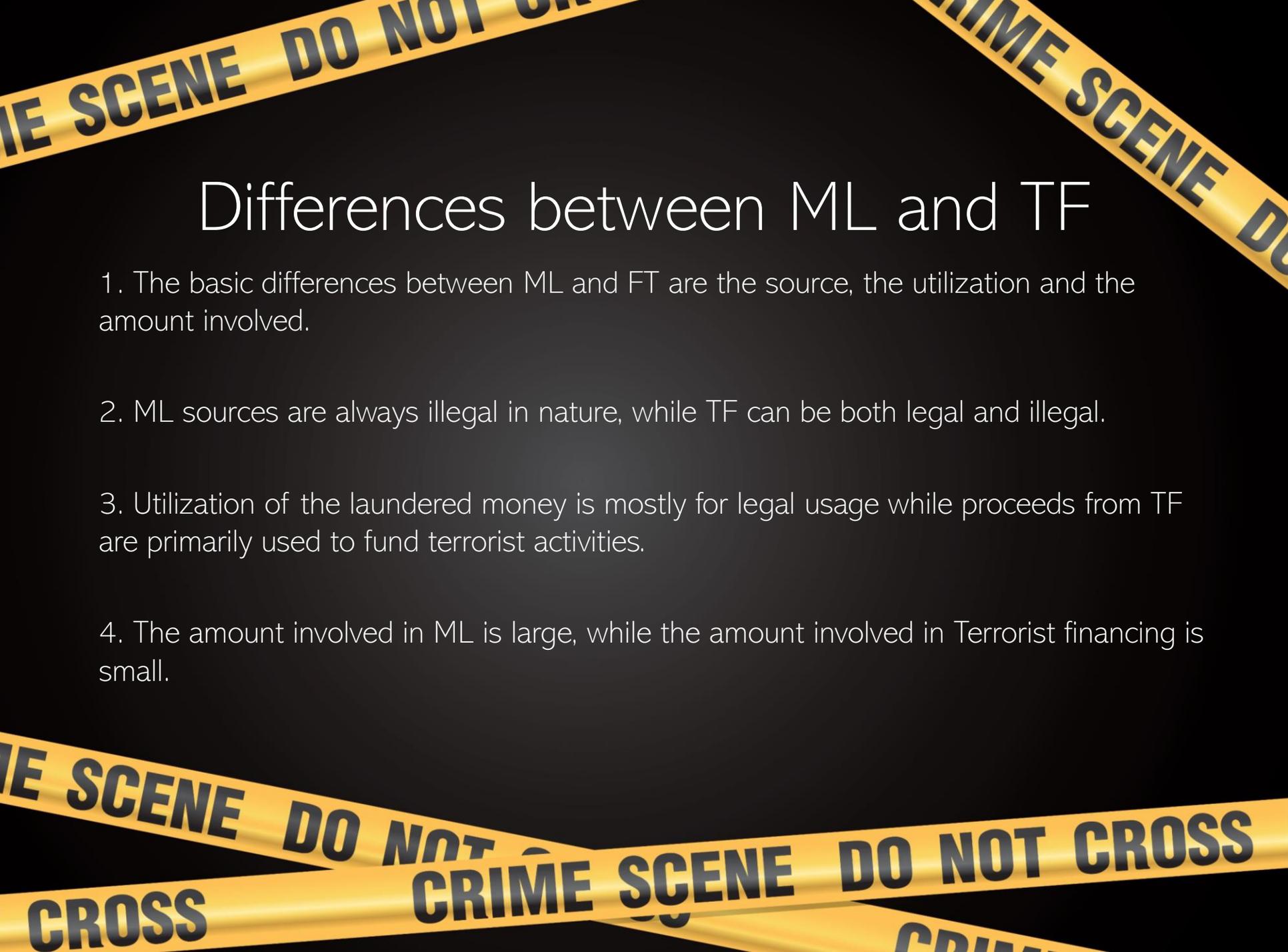
A person wearing a black balaclava and black gloves is holding a stack of gold bars. The person's face is partially visible through the balaclava, showing a serious expression. The background is dark, and the lighting highlights the gold bars and the person's hands.

The **financing of terrorism** involves providing finance or financial support to individual [terrorists](#) or [non-state actors](#).

Individuals and organizations who finance terrorism need to conceal how the money will be used and where it is originated. The funds may come from legal sources, such as legitimate religious or cultural organizations, or from illegal sources, such as drug trafficking and government corruption. The funds may also come from an illegal source but appear to come from a legal source through money laundering.

Example:

Car sale deal between two FATF restricted or offshore countries.



Differences between ML and TF

1. The basic differences between ML and FT are the source, the utilization and the amount involved.
2. ML sources are always illegal in nature, while TF can be both legal and illegal.
3. Utilization of the laundered money is mostly for legal usage while proceeds from TF are primarily used to fund terrorist activities.
4. The amount involved in ML is large, while the amount involved in Terrorist financing is small.

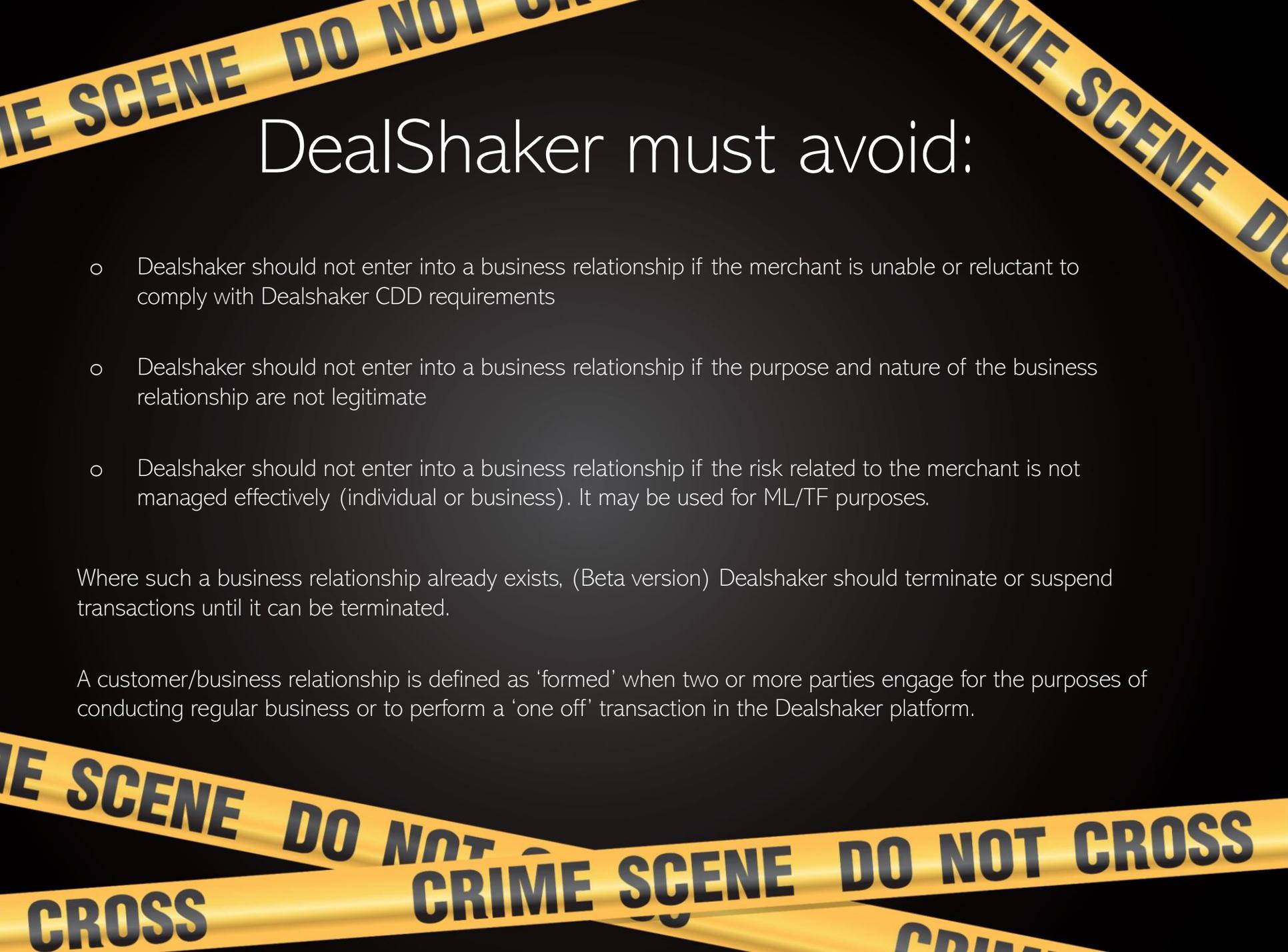
How Much Does A Terrorist Attack Cost?

A Lot Less Than You'd Think

Back in 2006, when Germany was hosting the World Cup soccer tournament, a terrorist attack was narrowly averted.

Two men plan to execute a terrorist attack. They carried two bombs hidden in 2 suitcases which were meant to blow up on a train, create a huge amount of damage and public anxiety. The bombs were fairly simplistic: a propane tank, alarm clock, batteries and a plastic bottle filled with gas. One of the men used part of his school tuition money to pay for all the supplies. All the necessary materials for the bombs cost less than \$500.





DealShaker must avoid:

- Dealshaker should not enter into a business relationship if the merchant is unable or reluctant to comply with Dealshaker CDD requirements
- Dealshaker should not enter into a business relationship if the purpose and nature of the business relationship are not legitimate
- Dealshaker should not enter into a business relationship if the risk related to the merchant is not managed effectively (individual or business). It may be used for ML/TF purposes.

Where such a business relationship already exists, (Beta version) Dealshaker should terminate or suspend transactions until it can be terminated.

A customer/business relationship is defined as 'formed' when two or more parties engage for the purposes of conducting regular business or to perform a 'one off' transaction in the Dealshaker platform.

Who is the merchant and what does

- 'Risk-sensitive basis'
- 'Company legal name'
- 'Type of activity'
- 'Sales volume per year'
- 'Nature of the transaction or activity' **mean?**

The risk-based approach to CDD

The best risk insurance is PREVENTION.

International standards require a risk-based approach applied to CDD.

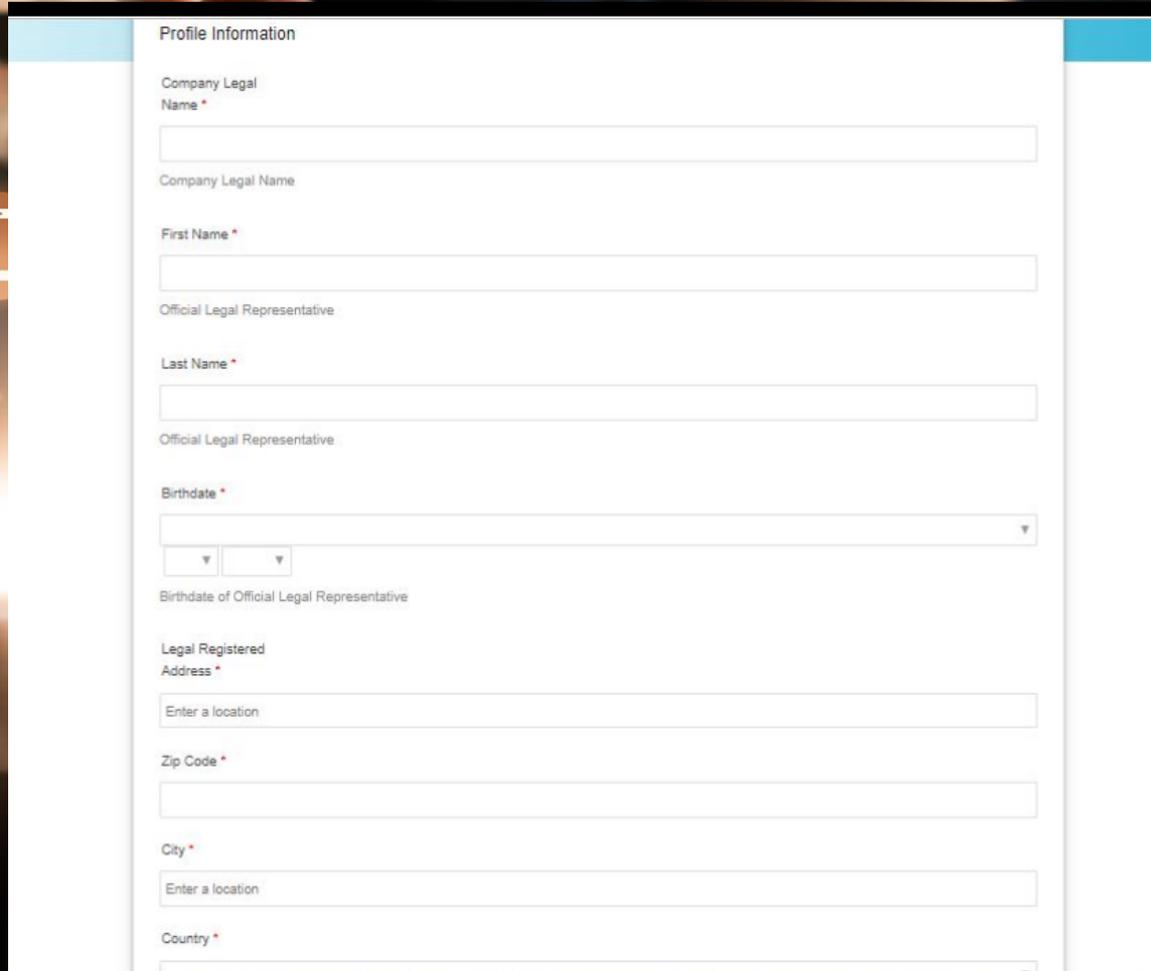
Consequently, measures should be applied on a risk-sensitive basis depending on the type of *customer, business relationship or nature of the transactions or activity*. Higher risk categories should be subject to enhanced due diligence (ECDD).

The risk assessment will determine how much of the information collected needs to be independently verified, as the following examples indicate.

- Only simplified or basic account opening information may need to be collected for companies with low-turnover annual income, not from countries in the FATF list/offshore, not with complicated company structure and not risk activity. Furthermore, UBO or the legal representative names must not be on PEP/Sanction lists.
- For standard-risk customers individual, i.e. those who are permanently resident in the country, with a salaried job or other transparent source of income, not in PEP or Sanction lists only the standard information provided may need to be verified.
- Enhanced due diligence should be applied to higher-risk customers/clients. Enhanced due diligence must also be applied to the beneficial owners or controllers of higher-risk companies or structures. **Enhanced Due Diligence** is a higher level of **due diligence** and is required in specific cases to mitigate the increased risk. A high-risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing.

During the ECDD process further documents are required: UBO identity documents and source of wealth/source of funds

Let`s see what information we require for entities and how they have to be used to determine the risk level?



The image shows a web form titled "Profile Information" with the following fields:

- Company Legal Name ***: A text input field.
- Company Legal Name**: A label for the field above.
- First Name ***: A text input field.
- Official Legal Representative**: A label for the field above.
- Last Name ***: A text input field.
- Official Legal Representative**: A label for the field above.
- Birthdate ***: A date selection field with a dropdown arrow.
- Birthdate of Official Legal Representative**: A label for the field above.
- Legal Registered Address ***: A text input field with the placeholder "Enter a location".
- Zip Code ***: A text input field.
- City ***: A text input field with the placeholder "Enter a location".
- Country ***: A text input field.



'Company legal name' gives you the entity type

Risky entity types are:

- LLC Limited liability company
- LLP Limited liability partnership
- Holdings/Trust
- JV Joint venture

Risky entity types

Examples:

LLC/LLP

Closely held business types - Has more than 50% of the value of its outstanding stock owned (directly or indirectly) by 5 or fewer individuals at any time during the last half of the tax year
a [corporation](#) in which more than half of the shares are held by just a few individuals has a more informal operating structure, which allows some decisions to be made without the board of directors approval.

Holdings/Trusts

Privately owned companies and other entities such as trusts, are generally assessed as higher risk than quoted companies because they are exposed to a lower level of external scrutiny than those that are publicly owned.

For such relationships, the identities of the beneficial owners UBO (not just legal representative) must also be verified in addition to verifying the identity of the corporate entity and the legal representative.



What QUESTIONS may arise:

Is the customer's ownership and control structure transparent and does it make sense?

Is there an obvious commercial or lawful rationale when the customer's ownership and control structure is complex or opaque?

Is there a sound reason for changes in the customer's ownership and control structure?

Is the customer a new undertaking without an adequate business profile or a track record?

'Address of the individual/company'

First step - During the registration period of a merchant

Please check the country of origin! Jurisdictions associated with higher ML/TF risk come from FAT/offshore countries. These FATF/offshore countries have strategic deficiencies in their AML/CFT regime which impose a significant threat.

When identifying the risk associated with countries and geographical areas, Dealshaker should consider risk related to:

- a) The jurisdictions in which the customer and beneficial owner are based;
- b) The jurisdictions that are the customer's and beneficial owner's main places of business;
- c) The jurisdictions to which the customer and beneficial owner have relevant personal links.
- d) Has the country been identified by FATF as having strategic deficiencies in its AML/CFT

Second step – During redemption

Please check where the money comes from! If the funds used are from FATF/offshore countries this should give reason to suspicion, based on what the firm knows about the purpose and nature of the business relationship.

Let`s see what information we require for entities and how they have to be used to determine the risk level?

Company

Registration Number *

*

Type of Activity *

Sales Volume per
year *

Last Name *

Last Name of Ultimate Beneficial Owner

First Name *

First Name of Ultimate Beneficial Owner

VAT number

Add your VAT number if you have one

Save

'Type of activity'

'Type of activity' is a field which gives you information where we could find out if the merchant is risky. Have in mind that in non-face-to-face environment (such as DealShaker) most of the relations are risky.

Types of risky business activities by definition are:

- Cash-intensive business (restaurants, Retail stores, liquor stores, vending machine operators, parking garages)
- Non-bank ATM (operators)
- Money services businesses
- Third party payment processors
- Foreign import export activities
- Non-profit organisations whose activities could be abused for terrorist financing purposes (foundations)



What QUESTIONS may arise:

Does the merchant or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defense, the extractive industries or public procurement?

Does the customer or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?

Does the customer or beneficial owner have links to sectors that involve significant amounts of cash?

Is it possible to justify or prove the customer's or beneficial owner's source of wealth or source of funds easily?

For instance, a secure source of funds or wealth could be occupation, inheritance or investments.

Is the explanation plausible?

'Sales volume per year'

Low Risk < 25 000 Euro Turnover

High Risk \geq 25 000 Euro Turnover = ECDD



Examples of EDD measures, firms should apply in a high-risk situation include:

- Obtaining additional customer information during identification such as the source of funds
- Applying additional verification measures from a wide variety of reliable and independent sources (e.g. checking against online databases) in order to verify the customer's or beneficial owner's identity
- Applying identity fraud checks to ensure that the customer is who they claim to be
- Applying enhanced monitoring to the customer relationship and individual transactions

Establishing the source and/or the destination of funds.

- 'Source of funds' means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, the customer's salary for instance. Applies in case of single/bulk transactions.
- 'Source of wealth' means the origin of the customer's total wealth, for example inheritance or savings.

How can you verify merchant's claim/s for source of funds:



1. Savings/ Salary

- Savings are regular small payments from an income source such as a salary, pension or an annuity. The best evidence for this will be 6 months' bank statements showing you gradually paid from your employer/pension/annuity and the money slowly growing in your bank account.
- If the merchant has multiple bank accounts for their savings then provide 6-months bank statements for each of the bank accounts.

2. Release of pension

A copy of the merchant pension release documentation and a copy of his bank account statement showing the money being received from the pension company.

3. Sale of shares

A copy of the share release schedule and a copy of the merchant bank account statement showing the money being received from the company.

How can you verify merchant`s claim/s for source of funds:



4. Sale of another property

A copy of the completion statement from the merchant solicitor, or the notary act and a copy of the bank account statement showing the money being received from the solicitor following completion/the seller.

5. Inheritance

A copy of the letter from the executors stating how much the merchant are being paid as a beneficiary and a copy of the merchant bank account statement showing the money being received from the solicitor/executor's bank account.

6. Dividends from a company

A copy of the merchant dividend certificate, a copy of the company's accounts and a copy of their bank account statement showing the money being received from the company.

How can you verify merchant`s claim/s for source of funds:



7. Gambling winnings

A copy of merchant receipt proving their winnings and a copy of the merchant bank account statement showing the money being received from the gambling company.

8. Compensation award

A copy of merchant letter confirming their compensation settlement from a solicitor and/or court and a copy of their bank account statement showing the money being received from the third party/court/solicitor.

9. Chain transactions

If the merchant claims that receive money to buy the good/services on behalf of a group of friends. They should consider writing down details of the names, personal data like ID/Passport number, date of birth, addresses of the friends and the amounts to be transmitted and the grounds for that transfers and their explanations for source of funds that transfer until Dealshaker has proof that the source is from legitimate activity.

The source of funds for company (or wealth) can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports.

REMEMBER!

The documents about the company are necessary if online search is not applicable!

The AMLD4 specifies that businesses must collect relevant official documents directly from official sources like government registers and public documents, rather than from the organization/merchant in question.



REMEMBER!

The company has to consider encrypted way of gathering documents such as:

1. Certificate of good standing
2. Article of association
3. The ownership structure document
4. A copy of the document by which the persons are empowered/ authorized to dispose with the balance on the Company's accounts/A power of attorney if applicable/.
5. Additional documents upon request.

Do not forget to constantly monitor merchant behavior!



What are the signs of suspicious behavior?

- The customer is reluctant to provide CDD information or appears deliberately to avoid face-to-face contact
- A business is reluctant to provide documents for establishing a new account, complete information about the nature and purpose of its business, anticipated account activity, prior DealShaker relationships, names of its officers and directors, or information on business location
- The customer's evidence of identity is in a non-standard form for no apparent reason.
- The customer's behaviour or transaction volume is not in line with that expected from the category of customer to which they belong, or is unexpected based on the information the customer provided at the beginning.

What are the signs of suspicious behavior?

Dealshaker should use the findings from its business-wide risk assessment to make a decision on the appropriate level and type of CDD that will apply to individual business relationships and occasional transactions and put in place adequate policies and procedures.

Follow our professional acumen
which sets us apart from all
OTHERS.

