TYPES OF CRIMES

2024

MINISTERIO
DE ECONOMÍA, COMERCIO
Y EMPRESA

COMMITTEE ON THE PREVENTION
OF MONEY LAUNDERING AND
MONETARY OFFENSES

INTRODUCTION

This document outlines some of the most commonly used methods for money laundering and terrorist financing (hereinafter ML/TF), classified according to the primary underlying crime to which they are typically linked.

The purpose of this document is to assist entities subject to compliance with Law 10/2010 of April 28 on the prevention of money laundering and terrorist financing. A better understanding of the ways in which threats manifest in this area (drug trafficking, organized crime, corruption, etc.) can help improve the systems implemented by regulated entities to prevent and detect money laundering transactions.

The proposed list is not exhaustive. The methods used for money laundering can be extraordinarily diverse. Furthermore, they are highly dynamic, varying in form and content depending precisely on the actions that the regulated entities' prevention system adopts to prevent, detect, and combat them. However, the most important ones are likely represented.

For each money laundering scheme, a brief explanation is provided of the objectives the perpetrators seek to achieve by using each one in money laundering processes, to facilitate a better understanding. This is followed by a description of the money laundering scheme, tracing the process from start to finish. Many of the schemes include steps that may take place in other countries, but the explanation focuses in greater detail on the parts of the process that are typically carried out in Spain.

The descriptions of the money laundering schemes include important aspects that regulated entities must take into account when preventing and detecting each of the money laundering processes listed in the typologies. Only the distinguishing features of each typology are mentioned; there are a number of general measures that are expressly identified in Law 10/2010 of April 28 as obligations to be fulfilled by regulated entities and which are not repeated here (proper customer identification, information collection, appropriate categorization, etc.).

Most of the typologies explained here require the involvement of more than one type of regulated entity for their execution.

Finally, a section is included with general considerations regarding the financing of terrorism.

TYPES OF CRIMES RELATED TO ORGANIZED CRIME AND DRUG TRAFFICKING

Cryptoassets

Cryptoassets have certain characteristics that make them highly attractive for money laundering schemes. Their anonymity allows, in certain cases, for the concealment of value without revealing the owner's identity. Their ease of transfer, which occurs via a global blockchain, enables funds to be moved between jurisdictions simply by purchasing them in one country and selling them in another. Finally, the sector comprises both a regulated segment, which operates within the prevention system money laundering, and another arm that operates

independently of the first, which can also be exploited for money laundering purposes.

In some cases, criminal organizations receive their proceeds directly in cryptocurrency, knowing how difficult it is to trace. This is what happens, for example, in ransomware cases, where criminals typically demand ransom payments in cryptocurrency.

However, in most cases, these organizations generate their proceeds in cash or other forms of payment. In such cases, a common money laundering scheme involves converting funds of illegal origin—received in cash or other forms of payment—into cryptoassets, serving as an intermediate step toward subsequent placement processes, thereby severing the link to the funds' illegal source.

This method begins with the possession of cash derived from drug trafficking or other serious criminal activities. The next step is to purchase cryptoassets, which can be done in various ways. Some methods involve using the financial system, while others bypass it through peer-to-peer exchanges.

Among the processes that use the financial system, one possibility is to use multiple accounts to deposit the illegal funds into them in small individual amounts and then transfer them to a crypto-asset service provider. It is therefore possible to use networks of mule accounts for these purposes, which receive the funds and transfer them to the provider. It is also possible to take an intermediate step, by interposing a account that acts as centralizing entity, receiving funds from the other accounts via transfer and then diverting the funds to the cryptoasset service provider.

In transactions where cryptoassets are bought and sold between individuals, peer-to-peer (P2P) tools are used. The agreement between the seller and the buyer is reached through social media or specialized, unregulated platforms. The seller of the cryptoassets will generally receive payment for their cryptocurrency in cash, either handed over in person by the buyer or deposited into their account by the buyer.

It is also possible to convert cash into cryptoassets through the intervention of unregulated professionals operating on the deep web who match individuals with cash who wish to acquire cryptoassets with those who wish to sell them.

Once cryptocurrencies have been acquired, the next steps take place within the crypto world. As a first step, the funds are transferred to wallets managed by unregulated providers or to wallets not held in custody by a provider. Then, transactions are carried out to break the traceability of the operations through various mechanisms, including: The use of cryptocurrency mixers, which combine transactions from different users to make it difficult to trace the origin and destination of each individual transaction; CoinJoin services, which achieve the same objective as the previous method by combining multiple transactions into a single one; conversion to cryptocurrencies specifically designed to hinder traceability, such as Monero (XMR), Zcash (ZEC), Dash (DASH), Verge (XVG), Beam (BEAM), and others; or the use of swapping services that allow users to exchange one type of cryptoasset for another without having to go through a centralized exchange.

Finally, they would follow a reverse process to convert cryptoassets into fiat currency and use it to make investments, presenting the returns from previous cryptoasset investments as the source of the funds—even though such investments may not have actually taken place (on the contrary, many criminals prefer stablecoins for their operations). It is very common for the conversion to take place in a foreign country.

Front companies

Criminal organizations often obtain their profits in cash. For example, organizations involved in drug trafficking collect cash from buyers for the sale of drugs, and that cash continues to circulate among the various levels of suppliers, where it is stored and accumulated until, at some point, it must be moved out. Furthermore, many of these organizations are transnational in nature, and it is very common for profits obtained in one country (in this case, Spain) to be transferred to another, often the country where the narcotic substance is produced.

This scheme aims to introduce the cash into the financial system and subsequently transfer it abroad. The deposit of large amounts of cash without justification is a clear indication of money laundering; therefore, to avoid arousing suspicion, the organizations use the front of businesses or companies that, on the surface, sell products or services to the general public, providing a justification for the deposit of cash.

The scheme described here involves the use of a business or commercial activity that, in principle, is suitable for collecting cash from its customers. The money is deposited into a bank account as if it were proceeds from the sale of products or goods. Subsequently, the funds are transferred abroad, as if they were payments to supposed suppliers.

The process begins with the recruitment of a self-employed individual or small business engaged in some form of commercial activity, however minimal. Businesses or companies can vary in type, ranging from retail sales to restaurants. Generally, the business or company will have some form of commercial premises, located in downtown areas, shopping centers, or industrial parks.

It is also possible to establish a new company and launch a business—even if only ostensibly or in a purely formal sense—such as a supermarket, an electronics store, a used cell phone shop, or other similar ventures.

The cash will be presented as originating from the company's retail sales of goods. However, it is also possible for several of these companies to act in coordination, with all of them depositing cash into their accounts and transferring funds back and forth between one another, pretending to be suppliers to one another.

Cash deposits will be recorded in the business or store accounts, either in person at bank branches or via ATMs. The individuals making the deposits will generally be the business owner and people in their inner circle. The organizations will hand over cash to those in charge of these businesses, who will then deposit it into their accounts.

Once the money is deposited into the accounts, it is transferred to other accounts, usually abroad. The payment will be disguised as being made to a supplier, but other mechanisms are possible, such as repayment of a fictitious loan, payments for fictitious or inflated property rentals, etc.

Since cash is not received from a variety of customers but rather depends on the arrival of a shipment from a criminal organization, cash receipts will not follow the usual temporal/seasonal pattern seen in businesses that serve a real customer base subject to typical patterns (days of the week that consistently see higher activity than others; times of the year with higher activity than others; a decline in activity during holidays; etc.)

Likewise, it is very common for sudden increases in business volume to occur once the viability of the business has been established, which is inconsistent with the reality of commercial activities.

The absence of other payment methods used by customers may also be striking. For example, the absence of card payments.

If the cash brought into the business is very large relative to its actual activity—which can make it seem suspicious—the organization decides not to continue the operation for long, replacing the business with a new one. When the business has consistent actual activity (for example, a restaurant) and the amount of cash injected into it is not disproportionate, the money laundering operation can continue for a longer period until it is detected.

In operations like these, certain red flags may be observed, such as the presence of large amounts of cash being disproportionate to the company's infrastructure—including the number of employees, payments for supplies, etc. Tax returns filed with the Spanish Tax Agency, Agencia Estatal de Administración Tributaria (hereinafter, AEAT) may be fabricated.

Offsetting with commercial transactions

Criminal organizations operating in Spain generally attempt to channel a portion of the profits they generate to other countries. Many of these organizations have an international presence and move funds between countries. These countries may be drug-producing nations, for example, or the countries where the criminal organization originated.

One strategy these organizations use to transfer funds internationally is to enter into agreements with importers of goods in the destination countries. These agreements allow for the receipt of local currency from importers in exchange for

paying exporters for the products that the importers receive in their respective countries.

When the exporter is a Spanish company, payment for the goods can be received in various ways. Sometimes, members of the organization deposit cash directly into the exporter's account. On other occasions, the cash is deposited into the account of a front company that acts as an intermediary and then transfers the funds to the exporter.

In the case of organizations engaged in fraud, it is even possible that the payment to the exporter is made by the fraud victim themselves, either from Spain or, more frequently, from abroad. For example, scammers may provide the victim with the exporter's account number, leading them to believe it belongs to a different company (one of the tactics observed in scams targeting businesses that are deceived by altered account numbers on supplier invoices, for instance).

Regardless of the form and geographic origin of the payment to the exporter, these transactions can be detected through the inconsistency arising from the fact that the exporter receives payment from a country other than the one where the goods were delivered, and that the payment is not made by the company to which the goods were sold, but by a different person or company.

Once the exporter receives payment for the exports, the importer in the destination country will deliver the agreed amount to the organization in the destination country, thereby completing the transfer of funds. Payment in the foreign country is generally made in cash. This type of transaction benefits the importer, who can thus pay for goods that subsequently enter the country undeclared or undervalued (contraband), without the payment for said goods appearing in the financial

transactions subject to review by the authorities in their country.

In schemes like these, Spain may also play a role other than that of the exporter's country. For example, payments can be made from Spain for goods exported from another country, regardless of whether or not they are received in Spain. When these types of payments are made, there is a discrepancy between the destination of the funds (payment for goods) and the profile of the person or company making the payment (who is not the importer of the goods).

Money Transfers

There are large clandestine financial flows driven by organized crime. For example, drug trafficking generates a continuous flow of illegal goods from producing countries to consuming countries and also generates another continuous financial flow moving in the opposite direction, with money flowing from consuming countries to producing countries. These illegal financial flows sometimes attempt to disguise themselves among other legal financial flows moving in the same direction. A typical example is the type of scheme we are discussing here: drug money is attempted to be camouflaged and mixed in with the remittances that immigrants in consumer countries (for example, Spain) send to their countries of origin, which sometimes coincide with drug-producing countries or countries involved in drug distribution.

In these money-laundering schemes, drug proceeds are broken down into small amounts and handed over to immigrants, who, in exchange for a commission, arrange money transfers to the countries and individuals specified by the criminal organization.

The money may also be handed over directly to rogue agents at payment service providers, who then split it into multiple transfers, each of a small amount. Each transfer is attributed by the agent to customers who have occasionally used their services—and whose identity information they retain—or to false identities. Furthermore, these agents typically distribute such transactions across different payment service providers, so that the activity appears less suspicious to each individual provider with which they have an agency agreement.

In either case, the transfers will reach the destination country, where other individuals—whether members of the organization listed as the beneficiaries of the transfers or others with powers similar to those of the rogue agents who initiated the operation—will receive the funds and hand them over to the criminal organization.

Through schemes such as these, and given that the transfer will have been made in the names of multiple individuals—thereby concealing the true identity of the person who authorized the transfers—and by splitting the total amount into several smaller transfers, the requirement to provide information on the source of the funds (mandatory above a certain amount) will have been circumvented.

When these transfers are examined individually, it can be seen in many

transactions that do not exhibit some of the typical characteristics of this type of operation. For example, it may sometimes be observed that the sender of the transaction is not sending money to their country of origin, as is usually the case; or that the alleged recipient, based on their last name, does not appear to be related to the sender (generally, these transfers are made to relatives in the immigrant's country of origin); or that the amount of the transaction is higher than what the same sender has sent on previous occasions; or that the name of the beneficiary listed on the transfer does not match the one provided by the same sender on previous occasions.

In the case of agents involved in this type of money laundering operation, an analysis of their overall operations will reveal that the destination country predominates over others, that transfers to that country have the highest average value, and that some of the transfers may share common details, such as the same contact phone number for the sender. It is also common for the agent themselves to appear as the sender of some of the transfers, or to use the identities of their relatives, or to use the identities of other clients who have previously ordered legal transfers.

Foreign currency exchange

Due to its geographical location, Spain serves as a hub for various drug trafficking routes. In this context, criminal organizations from other countries come to Spain to procure narcotics. Sometimes, they transport cash from their home countries in local currency and exchange it for euros in Spain, which they then use to purchase the narcotics.

This operation is observed primarily in tourist areas where there are a large number of currency exchange establishments

The operation is generally carried out with the collusion of an established currency exchange office, whose staff collects the cash of illegal origin from the organization seeking to make the exchange. In the office's ledger, the total amount received is broken down into multiple small-amount transactions, each attributed to a different person, so that the operation does not attract attention.

Subsequently, the currency exchange office staff deposits the collected foreign currency at a financial institution and withdraws the same amount in euro banknotes. Finally, these euro banknotes are delivered to the organization that initially provided the foreign currency banknotes.

The credit institution may detect these transactions due to the unusual increase in the volume of transactions at the currency exchange office conducting such operations. Even when the office carries out several such transactions over time, it can be observed that the currency exchange transactions are not distributed over time in the same way as tourism, which has a strong seasonal component.

For smaller amounts, this type of transaction can be carried out without the currency exchange office's complicity. In that case, the cash is distributed among several people who visit various different currency exchange offices to carry out the exchanges in small transactions over time.

The currency exchange office may detect this scheme in various ways: Sometimes, the person exchanging currency is not a national of the country whose currency they are attempting to exchange; or it may be evident that they are being assisted by another person at the time of the exchange transaction. Ultimately, if the scheme is repeated, there will be an increase in the number and frequency of transactions involving the same foreign currency.

Money laundering as a service

In certain cases, criminal organizations do not carry out money laundering processes themselves but instead turn to specialized professionals. These professionals provide outsourced money laundering services, which can be utilized by any type of organization, group, or criminal who wishes to do so or lacks their own money laundering infrastructure. In short, these professionals offer money laundering as a service (money laundering-as-a-service) in exchange for a commission.

The services provided can vary widely, but it is common to use companies through which funds will flow. Pre-incorporated companies are often used, or those that undergo frequent changes in management, or even changes in their corporate purpose. Typically, they are structured in several tiers: some companies with the most visible operations, which remain active for a short time, and other companies that operate behind the former and remain active for a longer period.

For the representation of these companies, front men are used for “disposable” companies, while other companies that remain active for longer periods are managed by the professionals themselves.

The services offered include acting on behalf of the company before third parties—many of whom are regulated entities—or before the authorities themselves. This approach aims to prevent criminals from having direct contact with regulated entities and to ensure that funds with illicit origins and/or destinations pass through financial instruments controlled by the organization.

As for their operations, the structure typically aims to collect cash, deposit it into the financial system, simulate some form of business activity, and then transfer it out of the organization without raising suspicion among regulated entities.

To achieve this without triggering alerts, they require both a stable infrastructure in economic sectors compatible with the type of transactions requested by their clients, as well as a vast number of individuals and legal entities acting as frontmen and “disposable” instruments, thereby making financial tracing difficult.

The introduction and final disposition of the funds are carried out by the shell companies and their frontmen at the helm, but in between, a stable structure capable of managing large volumes of funds operates.

The presence of this type of structure is observed in economic sectors involving

the exchange of opaque goods or services, in terms of verifying the actual value of the goods or services being managed, for example, all types of second-hand items (clothing, cars, electronic products, etc.), high-value products (precious metals or jewelry), consulting or advertising, etc.

TYPES OF CORRUPTION

International bribery

Economic globalization has expanded the scope of business operations, with many companies now competing against one another in a global market. Corrupt officials and government employees may take advantage of this situation to demand illegal payments from the foreign companies with which they negotiate, in exchange for influencing their contracts. The widespread prevalence of these corrupt practices can hinder the development of the countries affected, but it also undermines free competition among companies, as it favors those that pay over those that do not. For these and other reasons, international bribery is strictly prosecuted and is considered a predicate offense to money laundering that requires special attention.

The patterns observed in relation to international bribery include preparatory acts to justify the transfer, from the company's treasury, of funds that will later be used to make illegal payments; and the execution of such payments to the foreign official or authority, generally through shell companies or intermediaries. Subsequently, the foreign authority or official will launder the funds received in order to benefit from them and incorporate them into their assets.

As for the process of securing funds to make payments, there are several options. If the company conducts part of its business in the underground economy, it can use funds previously collected under the table for illegal payments, and in such cases, payments are typically made in cash. If the company does not have funds that are not reported to the tax authorities, a process is required to transfer those funds out of the company's cash flow. To do this, the most common practice is to simulate the payment of services to a supposed supplier who, in reality, is under the company's own control. The company will pay the invoices issued by the fake supplier, and then those funds—whether withdrawn in cash or transferred abroad—will be set aside to later make payments to the authority or official.

These companies acting as fake suppliers provide justification for the outflow of funds from the company through the corresponding invoices, typically disguised as payments for consulting services, software, or other services that are difficult to verify. These fake companies exhibit a significant disparity between the revenue they receive and their business infrastructure (which is usually nonexistent or practically nonexistent). Given the illegal nature of their activity, they can only operate for short periods of time, which is why multiple companies are sometimes created to succeed one another. In this way, the true purpose of the payments remains hidden not only from the authorities but also from the company's own internal control bodies, as well as from auditors and advisors.

As for the payment itself, it can be made in cash or by other means. Cash is used for payments up to a certain amount, but when payments are large and ongoing, it is more common to make payments through the banking system, using front companies, such as the aforementioned service providers mentioned above.

These payments are generally routed to countries other than both the paying company's country and the country of the corrupt authority or official.

Sometimes, payments are made through professionals who act as intermediaries between the company and the corrupt authorities and officials. These intermediaries set up the corporate structures and necessary infrastructure, both to facilitate the movement of funds and to give the payments the appearance of legality.

There are many other ways in which benefits are provided to foreign officials or government authorities. In some cases, the benefit granted by the foreign company to the local authority takes the form of a stake in the joint venture that will carry out business activities in the country, entitling the authority to receive dividends from the joint venture without having previously contributed capital. On other occasions, benefits are granted by performing work beyond what was agreed upon in the contract, which benefits the authority or official. It is also possible for the company to recognize individuals or entities related to the authority or official for the provision of non-existent services, thereby creating a credit claim that they can claim in cash or as shares in the company.

In any case, due to their international nature—involving different actions across various jurisdictions and the involvement of professionals who design and execute them—these types of transactions pose significant challenges for the competent authorities in the different countries involved to gain a comprehensive understanding of the operation for the purpose of preventing and prosecuting corruption.

Investments Derived from Corruption Abroad

Typically, corrupt officials and public servants invest most of their illicit gains in countries other than the one where they reside and perform or have performed their political duties or work as public servants. In this way, their wealth can go more unnoticed in the face of the controls established in their home country. Furthermore, this protects a portion of their assets from legal proceedings that might arise from the discovery of acts of corruption and from potential political changes in their home country that could harm them.

Corruption can affect all countries, but it is far more serious and far more frequent in undemocratic societies.

The methods used to invest funds derived from corruption abroad in Spain typically involve holding illicit proceeds either in cash or deposited in third countries. It is also possible to hold these proceeds in cryptoassets.

As for the ownership of the assets they subsequently acquire, there are various possibilities. Sometimes, the corrupt official or agent may make the investment in their own name. This is particularly common in cases involving individuals who hold public office in their country and who, in addition to being politicians, are also engaged in some form of business activity. More often, however, the individuals listed as the beneficial owners of the investments are people close to the official or authority, such as their spouse or descendants.

Finally, complex corporate structures can also be created in an attempt to conceal both the identity of the ultimate owner and the origin of the funds. Such structures are designed and managed by professionals and may involve the use of front men to formally hold the beneficial ownership.

The funds entering Spain may be directed directly to sellers for the purchase of real estate, or to professionals, or to intermediaries. Accounts and companies may also be opened in Spain to receive the funds, with payments made subsequently.

As for the purpose of the investment, there are various possibilities. The most common is the purchase of real estate, preferably in tourist areas or major cities.

It is also possible to invest these illicit proceeds in companies by purchasing a stake or participating in capital increases.

TYPES OF TAX FRAUD

Value-Added Tax (VAT) Fraud Schemes

The predicate offense underlying money laundering involves the creation of an artificial chain of companies in transactions involving the importation of goods from other European Union (EU) countries. The companies involved in the scheme, acting in concert, pretend to be suppliers to one another, and one of them (the one acting as the importer of the goods) fails to pay the tax, thereby committing tax fraud.

The VAT regime for commercial transactions between European Union (EU) countries provides for the refund to exporting companies of the input VAT on the goods they export and ensures that importing companies do not incur VAT when purchasing goods from other EU countries. Tax evasion can be attempted in various ways. On the one hand, an export of goods can be simulated, so that the exporting company's VAT return results in an undue refund of the theoretically input VAT. On the other hand, an importing company may fail to meet its tax obligations by either (i) failing to file a return, (ii) including in its returns VAT input that is not real for an amount equal to the VAT passed on, (iii) requesting a deferral and failing to pay the debt, or (iv) simply failing to pay the VAT that would otherwise be due. The most common type of fraud is the latter,

involving intra-Community acquisitions, which is the type to be discussed here.

These frauds are carried out by forming a chain or network of companies that act as suppliers to one another, interposing themselves between the actual supplier of the goods or an intermediary and the company to which the products are to be sold. The companies in the network formally appear as theoretically independent entities, but actually, they are under the same management.

The company in the network that acts as the importer does not pay VAT on its purchases abroad but does charge VAT on its sales in Spain. When this company files its tax return, a high tax liability will result, which it will not, however, pay to the Tax Agency. Typically, the importing company's failure to pay the tax leads to a reduction in the price at which the product is sold to the rest of the scheme, resulting in the product being sold to third parties at prices lower than the competition. This translates into greater market penetration for the scheme and may even lead to the expulsion from the market of intermediaries who comply with their tax obligations.

These fraud schemes have primarily taken root in the importation of high-demand, small-sized, and relatively high-value goods (traditionally, computer and electronic components), but they have spread to other sectors such as household appliances, tires, and machine tools. Similar schemes are also used in the trade of used vehicles between EU countries.

The hydrocarbons sector deserves special mention. In this sector, the product is collected from tax warehouses by a distributor's first-tier company without incurring VAT, in a manner similar to the goods importers described above. This has led to the creation of new VAT fraud schemes in this sector, operating similarly to those explained above, by creating artificial chains of suppliers from the initial seller down to service stations and gas stations. Although these schemes have been particularly significant in recent years, recent legislative changes are expected to lead to their prompt eradication. Another form of fraud very similar to the one described above involves alcoholic beverages, where their removal from the tax warehouse also triggers the accrual of VAT and excise tax.

There are several distinctive features in VAT fraud schemes that can be used to detect them. The companies inserted into the supply chain are mere fronts, with no actual business activity. Their sole function is to receive and issue invoices, and to handle the corresponding collections and payments for the other members of the scheme.

- They typically have the profile of recently incorporated limited liability companies with minimal capital contributed to the form of non-monetary assets. Occasionally, they may be older companies that have been recently acquired, which is evident in the change of representatives.
- They do not have large facilities. They may be registered at abandoned premises, professional offices, or shared workspaces.

- The individuals representing them are generally front men who lack even the most basic training or experience to handle the commercial activity they claim to be engaged in. They are often accompanied by other individuals who are the ones truly pulling the strings.
- Large movements of funds in a relatively short period of time.

As for the operations of the network's members, a key characteristic is the immediacy between collections and payments, leaving almost no balances in the accounts. Given that their function, as already mentioned, is merely to issue invoices, it is also characteristic in many cases that they maintain only one or a few suppliers and one or a few customers (depending on how extensive the chain of fraudulent companies is). They have no business relationships outside their own companies.

If they are asked to provide documentation supporting their business activities, a review of such documentation may reveal irregularities, such as a lack of specificity regarding the goods traded, rounded prices, or documents that appear unprofessional, etc.

Tax-Opaque Funds

The non-payment of taxes levied on the profits of companies or individuals—particularly corporate income tax for companies and income tax for individuals—results in amounts (the evaded tax liability) that are improperly retained in the assets of the tax evader and may be subject to subsequent money laundering.

The simplest way to conceal these evaded amounts is to hold them in cash. This cash is then used by the evader to pay for goods and services, whether for everyday expenses or for more special purchases.

Attempts to make large cash payments may be indicative of holding tax-evaded funds.

There are tax measures prohibiting cash payments exceeding a certain amount (currently 1,000 euros) for goods or services provided by businesses or professionals. However, there are also sellers and service providers who attempt to circumvent the prohibition through various mechanisms, such as splitting payments or using intermediaries.

Tax-evaded cash can also be used to pay part of the price when purchasing real estate. Generally, these transactions are carried out through a private agreement between the seller and the buyer, in which they agree to reflect in the deed of sale only the price covered by other means of payment. These transactions can be detected because, first, the transaction price will generally be lower than the market price, since the portion paid in cash has not been taken into account. As for the seller, it can be detected if they deposit cash into their accounts on dates after the sale of the property.

Another method of concealment is to transport cash abroad and deposit it there into the financial system. To do this, they seek out countries with lax legal systems

toward tax evasion and financial firms that are lax (if not fully complicit with the tax-evading client). For example, employees of these firms travel to Spain, collect cash from tax evaders who wish to deposit it abroad, and deliver it to other clients in Spain—also tax evaders—who wish to withdraw in cash part of the money they previously deposited abroad.

The funds that have been sent abroad may, at some point, return to Spain, depending on the owner's needs. Typically, they will arrive via a bank transfer ordered by a foreign company, most often from a non-cooperative jurisdiction for tax purposes. The arrival of the funds may coincide with or immediately precede a transaction such as the purchase of real estate or the execution of an investment opportunity. Therefore, if information and explanatory documentation are requested in such situations, special attention must be paid to whether the client justifies the origin of the funds and whether the funds or the stake in that foreign company were declared to the Spanish tax authorities.

A relatively recent method of concealing evaded taxes is investment in cryptoassets. The opacity of this market allows tax evaders to park those funds in virtual assets. Special attention must be paid to the moment when virtual assets are acquired, as well as to the moment when they are sold and converted into fiat currency.

It is also common for fraudsters to divert funds from the business to their own personal accounts or those of related third parties (usually family members)

so that, from those accounts, they can withdraw the funds or pay for personal goods or services.

Finally, tax-evaded funds can also be invested abroad in more or less complex investment products, such as unit-linked funds. This type of activity almost always involves professionals who design and execute the transactions with varying degrees of awareness that the funds originate from tax evasion.

TYPES OF ACCOUNTS LINKED TO SCAMS AND OTHER TYPES OF FRAUD

Mule accounts

The digitalization process and the rise of e-commerce have led to an increase in fraudulent transactions, particularly those committed via electronic means (cyberfraud). In many of these fraud schemes, the perpetrators need to have a network of accounts to provide to their victims—whom they deceive in various ways—so that the victims will send the stolen money to those accounts.

Naturally, to appear as the account holders, they use identities that have nothing to do with the perpetrators of the scam, so that the latter remain hidden. This is achieved by using forged documents or the genuine documents of other people without their knowledge (identity theft). More commonly, scammers collude with other people who open accounts in their names and then provide them with the necessary login credentials to operate them remotely (account lending).

Once the account is opened, a small transaction is usually made as a test, and then the account remains inactive for a while until it is made available to the scammers to provide to victims as a destination for their payments.

Apparently, there are groups that specialize in setting up these types of accounts and then selling them to the scammers. When this is the case, it can be verified that the devices and IP addresses used for the account opening process and for carrying out transactions are different.

As for the transactions recorded in these types of accounts, with regard to deposits, they receive transfers from fraud victims. Most often, the victims are individuals, and the amounts sent to the account are not large, although the latter depends on the type of fraud. The victims of these frauds may be in Spain or abroad. Transfers may also be received from other money mule accounts, artificially increasing the complexity of the operation to make it more convoluted.

As for the destination of the funds received in this way, immediacy is a key factor. Destinations for the funds may include traditionally, cash withdrawals (often made at ATMs abroad); payments to crypto-asset service providers, with a preference for those not established in Spain; and transfers to other money mule accounts, in Spain or other countries.

In general, these are accounts with a limited lifespan, since the victim of the fraud will sooner or later, the victim will realize that they have been defrauded and will try to recover their money by alerting the financial institutions involved.

Typically, once the account is opened, it takes some time before it begins to be used, and it then remains active for only a short period (days or weeks, depending on the specific case). However, the victim may take time to discover the deception, or may find it difficult to file a claim, or may not file a claim at all, either because the amount involved is small or because they do not want to admit they were deceived. All of these are factors that delay or limit such claims and allow for an extension of the operational lifespan of the type of accounts described here.

Furthermore, given the increasingly frequent interconnection between various criminal activities, money mule accounts are also used to launder funds originating from other more serious criminal activities (human trafficking and smuggling, in particular).

Limited Liability Company Accounts

Scams and other forms of fraud sometimes use personal bank accounts to receive money from victims. When the amount defrauded is large, its passage through personal accounts is highly conspicuous. In contrast, if large sums pass through a corporate bank account, they may go more unnoticed, since, in principle, companies have a higher volume of transactions than individuals. Furthermore, it is in the fraudsters' interest for transactions to pass through several different jurisdictions, in order to make it more difficult to trace them (typically, a victim is selected in one country, payment is demanded in another, and the funds are then sent to a third country). For these reasons, some organizations involved in the most sophisticated fraud schemes invest resources in establishing Spanish limited liability companies and in opening accounts in our country, attempting to create a

façade of supposed business legitimacy for the transactions and adding an artificial step between the fraud committed and the final destination of the funds obtained.

To incorporate these companies, the organizations turn to professional firms that are typically commissioned indirectly, through another foreign professional firm.

The profile of the individuals forming the companies is that of a foreign citizen with no business experience and who, in many cases, has no known connection to Spain that would justify the purported business venture in our country. Eventually, they will claim a lack of knowledge of the language to avoid providing explanations.

Companies are sometimes incorporated in groups, with several individuals guided by the same professional to incorporate multiple companies, each one of them. The share capital paid up at the time of incorporation is generally the minimum amount and is contributed through the transfer of assets to the company (computer, furniture, etc.).

The founding partner typically serves as the sole partner and sole manager.

Once the companies are incorporated, bank accounts are opened in the name of each one at different financial institutions and branches. In-person service is preferred. During the account opening process, the new client will be assisted by a professional. The new company's business activity will be listed as brokerage in some form of international trade, supposedly without the need for facilities, staff,

or the transit of goods through Spain.

Once the bank account is opened, it will be managed remotely by the organization. The founding partner may disappear from the scene, so if the bank wishes to contact him, it will be unable to do so, or any supposed contact will be via email or through intermediaries.

As for the operational profile of these accounts, the main incoming transactions will be transfers ordered from abroad. In many cases, the victims of the fraud are the transfer originators themselves, sometimes repeatedly (the victim remains unaware of the fraud for a period of time). In these cases, it is highly likely that the transfer message will contain inconsistent information; for example, the beneficiary's name listed in the transaction may not match that of the company holding the account, or the text messages referenced in the transfer may be unrelated to the business activity declared by the account-holding company when the account was opened.

The accounts may also receive other transfers ordered by other shell companies used by the same criminal organization, whether these are initiated from Spain or, more commonly, from abroad.

The main types of outgoing transactions are transfers to exporting companies in other countries. This creates a balance between the fraudulent transactions and legitimate business transactions: the importer of the goods pays the organization behind the fraud, in cash or cryptocurrency, for the payments made from the bank accounts.

Those managing the accounts ensure there is no balance in them to prevent them from being frozen, disposing of the received funds immediately upon receipt.

Occasionally, the scheme is detected through a complaint from another country regarding a transfer received from one of the victims.

In general, it should be noted that these are accounts with no real activity, so there is an absence of the transactions one would expect in a business operation. Furthermore, since transactions that are independent of one another are combined, there is an obvious inconsistency between the profiles of the inflows and outflows (for example, inflows from foreign individuals and outflows to large heavy machinery export companies…). Additionally, underlying the scheme is the absence of a genuine link justifying the conduct of the scheme in Spain.

Although it may not always be obvious, it is common for a single financial institution to hold accounts for several companies that are theoretically independent of one another but are, in practice, under the same management. These corporate networks can be identified through factors such as the origin and destination of recorded transfers, contact information, or the devices and IP addresses from which the accounts are operated.

TYPES OF TERRORIST FINANCING

Terrorist financing can take many different forms, depending on multiple factors, such as the specific terrorist organization in question or the type of needs it is intended to meet (ranging from carrying out a terrorist attack to maintaining the organization's structure).

Terrorist financing can originate from states and governments, companies, associations and organizations, or individuals. Although in some cases it involves large-scale transactions, most financing activities involve small amounts. Virtually any type of payment method can be used for financing (cash, transfers, money transfers, card payments, fintech products, crypto-assets, etc.).

Furthermore, the funds used for financing may have a completely legal origin, or they may be the proceeds of criminal activities. In the latter case, it is said that a "hybridization" occurs between criminal activities and terrorist activities.

For all these reasons, it is extraordinarily difficult to identify indicators, patterns, or general typologies from the specific cases of terrorist financing observed in reality.

However, the following are three types of transactions involving financial flows that have repeatedly been observed in the context of terrorist financing:

- The use by terrorist organizations of solidarity campaigns that call for fundraising for a specific purpose, subsequently diverting part of the funds toward terrorist activity. In turn, these campaigns can take many different forms: ranging from more traditional ones, involving in-person events and primarily using cash; to the use of new technologies, websites, social media, crowdfunding platforms, or crypto-assets for fundraising. They may be organized by organizations and associations as well as by individuals.
- The transfer of funds to areas vulnerable to terrorism, primarily those where armed conflicts have broken out in which one of the warring parties is supported by terrorist organizations. These areas attract terrorist elements that require on-the-ground support, and these transfers serve to finance them. Again, all forms of fund transfers are possible, although not all of them can reach the destination area directly, as local financial systems are typically suspended. For this reason, funds are usually directed to the nearest countries and, from there, continue via human couriers to the conflict zone.
- The execution of settlement operations, or the use of pre-established payment systems, such as hawala.

Finally, it is worth noting other elements from which indications of terrorist financing can be drawn, such as: messages included in transactions, when they contain words or phrases related to terrorism; social media profiles; or the connection of transactions to other cases of financing or to investigations by authorities.

September 2024

www.tesoro.es

secretariaICMC@economia.gob.es

Paseo del Prado 6, 28014, Madrid