

AML/CFT GUIDANCE FOR THE ART SECTOR

PURPOSE AND CONTENTS

The Financial Intelligence Unit of Trinidad and Tobago (“the FIU”) provides this sector specific guidance to entities collectively referred to as ‘the art sector’ on their legal obligations under the Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) laws of Trinidad and Tobago. In this guidance, these entities collectively referred to as ‘the art sector’ include any individual or company that buys and sells works of any category of art.

This guidance uses plain language to explain the most common situations under the specific laws and related regulations which impose AML/CFT obligations. It is provided as general information only. Because AML/CFT obligations are contained in several laws, amendments and regulations, it is our aim that the entities within the art sector would find this guidance useful as a reference to the relevant provisions pertaining to their legal obligations. It is provided for general information only. It is not legal advice, and is not intended to replace the AML/CFT Acts and Regulations.

The use of the word “**must**” indicates a mandatory requirement, “**should**” indicates a best practice and the word “**may**” indicates an option for you to consider.

This guidance, is divided into ten (10) parts and includes:

1.	Do these obligations apply to you? - Clarification on the specified business activities which apply to the Art Sector.
2.	What is a Listed Business?
3.	The role and function of the FIU in the AML/CFT regime.
4.	What is Money Laundering?
5.	What is Financing of Terrorism?
6.	Why are entities in the Art Sector designated as a Listed Business?
7.	Examples of Money Laundering using the Art Sector.

8.	What are your AML/CFT legal Obligations? - An explanation of the main AML/CFT legal obligations, how they should be applied and Best Practices.
9.	Offences & Penalties.
10.	Additional Resources.
	Appendix – Suspicious Transactions/Activities Indicators

PART I

DO THESE OBLIGATIONS APPLY TO YOU?

Clarification on the specified business activities which apply to the Art Sector

These obligations apply to all types of Listed Business in the art sector that satisfy the criteria below. If you are an employee of a Listed Business, these obligations are the responsibility of your employer except with respect to reporting suspicious transactions and terrorist property, which is applicable to both.

The Art Sector

An art dealer is a Listed Business described in the First Schedule to the Proceeds of Crime Act Chap. 11:27 (“the POCA”) as ‘*an individual or company that buys and sells works of any category of art*’.

Therefore, if you buy and sell works of any category of art or own or operate a company which does so, the AML/CFT obligations detailed herein apply to you.

Accordingly, this guidance applies to you if you are a buyer, vendor, or intermediary involved in the sale of art works as professionals and includes for example auction houses, galleries, museums and art fairs and other art market operators.

Art includes works of drawing, painting, sculpture, engraving, lithography, photography and tapestry.

PART 2

WHAT IS A LISTED BUSINESS?

Anti-Money Laundering and Counter-Financing of Terrorism (“AML/CFT”) is everyone’s responsibility. It is important to note that all citizens of Trinidad and Tobago are subject to the Proceeds of Crime Act (“the POCA”) and the Anti-Terrorism Act (“the ATA”), however, further obligations are imposed on business sectors which face a greater risk of coming across crime proceeds and terrorist property than others. Business sectors which have been identified as more vulnerable include Attorneys-at-Law and Accountants when performing certain specific functions, Real Estate agents, Dealers in precious metals and precious stones dealers(s) and Trust and Company service providers and Art Dealers among others. These business sectors are identified as “Listed Businesses” under the First Schedule to the Proceeds of Crime Act, Chap. 11:27. If you carry on the business activities described in **Part 1** you are a Listed Business. Your business falls under the supervisory remit of the FIU. You have to comply with legal obligations under the AML/CFT laws of Trinidad and Tobago and the FIU as your Supervisory Authority monitors your compliance.

The AML/CFT laws of Trinidad and Tobago in which you will find your obligations are:

- (1) **Proceeds of Crime Act, Chap. 11:27 (“the POCA”)** as amended by Act No. 15 of 2014 - applies to all persons, but certain offences such as failure to report suspicious transactions only apply to Listed Business and Financial Institutions.
- (2) **Anti-Terrorism Act, Chap. 12:07 (“the ATA”)** as amended by Act No 15 of 2014 - establishes several offences for engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. The ATA applies to all persons but certain offences such as the failure to report suspicious transactions only apply to Listed Business and Financial Institutions.
- (3) **Financial Intelligence Unit of Trinidad and Tobago Act, 2009, Chap. 72:01 (“the FIU Act”)**as amended by Act No. 15 of 2014;
- (4) **Financial Obligations Regulations 2010**; as amended by The Financial Obligations (Amendment) Regulations, 2014 (LN No.392);

- (5) **Financial Intelligence Unit of Trinidad and Tobago Regulations 2011** as amended by the Financial Intelligence Unit of Trinidad and Tobago (Amendment) Regulations, 2014 (LN No. 403); and
- (6) **Financial Obligations (Financing of Terrorism) Regulations 2011.**

These laws are available on the FIU's website <http://www.fiu.gov.tt/>

PART 3

THE ROLE AND FUNCTION OF THE FIU IN THE AML/CFT REGIME

The FIU is Trinidad and Tobago's Financial Intelligence Unit. The FIU was established under the FIU Act pursuant to Recommendation 29 of the 40 Recommendations of the Financial Action Task Force (the FATF). Recommendation 29 mandates all its member jurisdictions to have a FIU to serve as the information related arm in efforts to combat Money Laundering, Financing of Terrorism and related crimes.

The FIU was created as an administrative type FIU, in that it does **not** have law enforcement or prosecutorial powers. Rather, it is a **specialised intelligence agency** which is legally responsible for **producing financial intelligence** for Law Enforcement Authorities ("LEAs"). The FIU became operational in 2010 upon the proclamation of the FIUTT Act. It is an autonomous department within the Ministry of Finance.

The FIU works in very close partnership with individuals and entities that have obligations under the AML/CFT laws. Those entities within the art sector have such obligations and are therefore also reporting entities.

WHAT THE FIU DOES

(1) Analyses and Produces Intelligence Reports

Essentially, the FIU is responsible for **producing financial intelligence** that is then disclosed to law enforcement agencies (LEAs) for investigation. To do this, the FIU receives suspicious transaction or suspicious activities reports (STRs/SARs) and requests financial information from various reporting entities such as banks, credit unions and other financial institutions, accountants, attorneys-at-law, money services businesses, art dealers, motor vehicle sales, real estate, private members' clubs. A total of seventeen (17) different reporting sectors **must** make (STRs/SARs) to the FIU.

The FIU receives many reports of suspicious transactions/activities from reporting entities, but within those reports are legitimate transactions. The FIU's analysis is therefore, to ensure that only those transactions on which there are reasonable grounds to suspect are related to money laundering or terrorist financing are disclosed to LEAs. Only transactional information and information relating to the suspicion of money laundering and terrorist financing are contained in the Intelligence report. For example, the name and other information on the person who actually submitted the report would not be provided to LEAs.

(2) Supervises for AML/CFT Compliance

Another important function of the FIU is to ensure compliance with obligations under the POCA, the ATA, the FIU Act and the Regulations made under those Acts. The FIU is the Supervisor for Listed Businesses and non-regulated financial institutions which have obligations under those Acts and Regulations and is responsible for making sure that they are meeting those obligations.

Activities related to the FIU's compliance mandate include educating and providing guidelines (such as this one), and enhancing public awareness of Money Laundering and Financing of Terrorism to allow entities who have AML/CFT obligations to be aware and know exactly what they need to do with regard to meeting their obligations. The FIU also conducts on-site inspections and takes action to ensure that the law is being complied with by the entities it supervises.

PART 4**WHAT IS MONEY LAUNDERING?**

The offence of money laundering is the process by which illegally obtained funds are given the appearance of having been legitimately obtained. Money laundering begins with the commission of criminal activity which resulted in benefits/gains (illegal funds) to the perpetrator. The perpetrator will then try to disguise the fact that the funds were generated from criminal activity through various processes and transactions which may also involve other individuals, businesses and companies. There is no one single method of laundering money. Methods can range from the purchase and resale of a luxury item (e.g., art, cars or jewellery) to passing money through legitimate businesses and “shell” companies or as in the case of drug trafficking or other serious crimes. The proceeds usually take the form of cash which needs to enter the financial system by some means.

There are three (3) acknowledged methods in the Money Laundering process. However, the broader definition of Money Laundering offences in POCA includes even passive possession of criminal property.

(1) Placement

‘Placement’ refers to the process by which funds derived from criminal activity are introduced into the financial system. In the case of drug trafficking, and some other serious crimes, such as robbery, the proceeds usually take the form of cash which needs to enter the financial system. Examples of Placement are depositing cash into bank accounts or using cash to purchase property/assets. Techniques used include Structuring or ‘smurfing’- where instead of making a large deposit transaction and in order to avoid suspicion or detection the illegal receipts are broken up into smaller sums and deposited into single or multiple accounts sometime using other persons are used to deposit the cash.

(2) Layering

Layering place after the funds have entered into the financial system. It involves the movement of the money. Funds may be shuttled through a complex web of multiple accounts, companies, and countries in order to disguise their origins. The intention is to conceal, and obscure the money trail in order to deceive LEAs, to make the paper trail very difficult to follow and to hide the criminal source of the funds.

(3) Integration

The money comes back to criminals “cleaned”, as apparently legitimate funds. The laundered funds are used to fund further criminal activity or spent to enhance the criminal's lifestyle such as investment into real estate and the purchase of luxury assets.

Successful Money Laundering allows criminals to use and enjoy the income from the criminal activity without suspicion which is why the AML/CTF legislative and compliance regimes are important crime fighting tools.

As traditional money laundering techniques have come under closer scrutiny persons with illegally obtained funds have increasingly turned to the art market. The Basel Art Trade Guidelines have estimated the global art trade to be in the region of 30 to 40 billion Euros annually.ⁱ

Studies have found that certain characteristics peculiar to the art sector make it susceptible to illegal activity such as:ⁱⁱ

1. It is characterized by discreet, confidential transactions, often of a high value.
2. The art sector is an extremely diverse market area bringing together a wide range of highly diverse players. Market participants can assume the multiple roles of auctioneers, dealers and collectors which, in other markets, would involve conflicts of interest.
3. The art sector is dominated by a few auction houses and a myriad of art-dealers. These in turn are organised in a variety of trade associations which may subscribe to a great range of different ethical standards.
4. The art sector largely operates independently of the financial markets and the fluctuations of share prices, yet displays comparable characteristics by exposing its trade objects to often dramatic and sometimes inexplicable changes in value.
5. Akin to the real estate sector, the art sector has the reputation of a ‘*refuge de valeur*’, which means that the more tightly the financial sector is regulated and controlled, the more copiously funds flow into the art world.

6. Apart from the use of art sales for the purpose of money laundering the volume of illegal or legally questionable transactions encompasses looted art, professional counterfeiting and fake certificates.

The art market has other advantages for launderers apart from the difficulty in accurately discerning a work's worth, and that is of the highly mobile and informal nature of exchanges. Art works are often highly valuable and readily transported, and may be privately sold without respecting the correct formalities.

Though there are no hard statistics on the amount of laundered money invested in art, law enforcement officials and scholars agree they are seeing more of it.

Therefore, as an entity in the Art Sector you are part of the national safeguard efforts to prevent money laundering and financing of terrorism as you and your business are at risk of becoming an unwitting party to these crimes.



PART 7**EXAMPLES OF MONEY LAUNDERING USING THE ART SECTOR****Case 1: Fake Auction**

The process involves a launderer putting a work up for auction which will be bought by an accomplice paying the auctioneer in cash using dirty money. The launderer/seller then receives a cheque from the auctioneer, and the money has thus been successfully laundered. The same technique can be used to the benefit of a dealer.

In August of 2000, the client entered a contract with a Swiss art dealer to buy and sell a well-known piece of art. The art dealer obtained the painting from a renowned European gallery for USD 10 million. The art dealer then sold the painting to an overseas company for USD 11.8 million. This company was acting as the exclusive agent of yet another overseas company. The two end buyers of the painting were the beneficial owners of that company. For their services rendered, the persons involved in the deal were to share the difference between the purchase price and the sales price; the client should receive USD 1.5 million, and the art dealer USD 100,000. Those involved in the deal did not know each other, nor were they aware of how much money each would receive. A few days after it had been bought, the painting was turned over to an auction house for further sale.

In May 2001, the Swiss art dealer learned that one of the end-buyers was allegedly entangled in an international corruption and money-laundering scheme. A high-ranking dignitary and fellow countryman of the person were reportedly also involved in this affair. Considering these circumstances, it was likely that the money used to buy this painting was of criminal origin. The Swiss art dealer notified MROS about his suspicions. The case has been passed on to law enforcement.

Source: Egmont Group, The Role of Financial Intelligence Units in Fighting Corruption and Recovering Stolen Assets, An Egmont Group White Paper

Case 2: Gallery Curator sells counterfeit works of art and transfers profits to himself

Over the course of several years Mr. T, a gallery curator sold more than 60 never-before exhibited and previously unknown works of art that he claimed were painted by some of the most famous artists of the 20th century. Mr. T sold these works of art to two prominent galleries for approximately \$10 million. In selling some of the paintings to the two galleries, he purported to represent a client with ties to France who had inherited the paintings and wanted to sell them, but who also wished to remain anonymous (the “purported French client”). For the remainder of the paintings, he purported to represent a Spanish collector (the “purported Spanish collector”). Mr. T also claimed that a portion of the price paid by the Manhattan galleries would be his commission for selling the paintings and that the remainder would be passed along to his clients.

In fact, as an investigation would later reveal:

- The paintings Mr. T sold were fake, that is, not by the hand of the artists that he represented them to be;
- Mr. T knew that the paintings were counterfeit and that the statements she made about their provenance were false;
- The purported French client on whose behalf he purported to sell most of the paintings to the Manhattan galleries never existed;
- The purported Spanish collector on whose behalf he claimed to sell the remainder of the paintings to the Manhattan galleries never owned the paintings;
- Instead of passing along a substantial portion of the proceeds of the sale of the various paintings, he kept all or substantially all the proceeds and transferred substantial portions of the proceeds to an account maintained by his family relative; and
- Mr. T concealed and disguised the nature, location, source, ownership, and control of the proceeds of sales of the fake works by causing the galleries to transfer substantial portions of the proceeds of the sales to foreign bank accounts, and by transferring, and causing to be transferred, proceeds of the sales from foreign bank accounts to accounts maintained in the his country of origin.

*Extracted with minor alterations from: Long Island Art Dealer Indicted in Massive Art Fraud, Money Laundering, and Tax Scheme
Glafira Rosales Charged with Knowingly Selling Fake Artworks Purportedly by Renowned Artists in \$30 Million Scheme – The
Federal Bureau of Investigation, U.S.*

Attorney's Office, July 17, 2013

<http://www.fbi.gov/newyork/press-releases/2013/long-island-art-dealer-indicted-in-massive-artfraud-money-laundering-and-tax-scheme>

WHAT ARE YOUR AML/CFT LEGAL OBLIGATIONS?

The AML/CFT laws of Trinidad and Tobago impose obligations on you to:

- i. Register with the FIU;
- ii. Submit Reports to the FIU;
- iii. Not to “Tip-off”;
- iv. Keep Records;
- v. Ascertain client identity;
- vi. Ascertain whether the client is acting for a Third Party;
- vii. Appoint a Compliance Officer and Alternate Compliance Officer;
- viii. Develop a written effective Compliance Programme; and
- ix. Implement your Compliance Programme and conduct periodic reviews.

I. REGISTRATION WITH THE FIU

You **must** register with the FIU for the purpose of identifying yourself as an entity which is supervised by the FIU if you perform any of the specified activities. You **must** also notify the FIU of a change of address of your registered office or principal place of business within six (6) months of such change.

You must register with the FIU within three (months) of commencing business activity or incorporation as a company, whichever is the earlier date.

You must also notify the FIU where there is a change of Directors, Owners, Partners or Compliance Officer within six (6) months of such change.

(1) How to Register

The registration process is very simple and free of charge. On-line pre-registration is available through the FIU’s website however you must download the form and print the completed registration form. To complete the registration process you must sign your printed pre-registration form and **manually submit this to the FIU.**

Register on **the FIU Registration Form** which you may access by [clicking here](#).

(2) **Offences**

- Failure to register within the time stipulated is an offence and you are liable on summary conviction to a fine of \$50,000 and to a further fine of \$5,000 for each day the offence continues.
- Failure to notify the FIU of a change of address of your registered office or principal place of business is an offence and you are liable on summary conviction to a fine of \$20, 000.
- Failure to notify the FIU of a change of Directors, Owners, Partners or Compliance Officer within six (6) months will be an offence and you will be liable on summary conviction to a fine of \$20,000.

II. SUBMITTING REPORTS TO THE FIU

You are required to send to the FIU two (2) types of reports:

- (1) reports of Suspicious Transactions or Activities (STRs/SARs) ; and**
- (2) reports of Terrorist Funds in your possession.**

The relationship between reporting entities and the FIU is a key one, because the FIU can only perform its analytical function to produce financial intelligence if the various reporting entities report the critical information they have.

Failing to report to the FIU knowledge or suspicion of crime proceeds or terrorist property is a criminal offence. If you continue to deal with such a transaction or funds knowing or having reasonable grounds to believe that the funds are crime proceeds or terrorists' funds and you do not report it to the FIU then you may have committed the offence of Money Laundering or Financing of Terrorism.

a) Reports of Suspicious Transactions/Activities

i. You must submit a Suspicious Transaction Report or Suspicious Activity Report (STR/SAR) to the FIU where you know or have reasonable grounds to suspect:

- that funds being used for the purpose of a transaction are the proceeds of a crime; or
- a transaction or an attempted transaction is related to the commission or attempted commission of a Money Laundering offence; or
- that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organizations or those who finance terrorism.

The STR/SAR must be submitted **within fourteen (14) days of the date the transaction was deemed to be suspicious.**

- ii. You **must also** submit a STR/SAR to the FIU **immediately** if a terrorist entity* attempts to enter into a transaction or continue a business relationship. You must not enter into or continue a business transaction or business relationship with such entity.

***A terrorist entity means any individual or entity and their associates designated as terrorist entities by the Security Council of the United Nations or any individual or entity listed on the consolidated list circulated by the FIU.**

Report using the **STR/SAR Form** which you may access by [clicking here](#).

You may access the **Security Council of the United Nations List** ("the UN list") by [clicking here](#).

[Click Here](#) for **STR Reporting Standard No 1 of 2011** to guide you in completing the STR/SAR form.

- iii. ***Defining Knowledge and Suspicion***

The first criterion provides that, before you become obliged to report, **you must know or have reasonable grounds for suspecting**, that some other person is engaged in Money Laundering or Financing of Terrorism.

If you actually 'know' that your client is engaged in Money Laundering, then your situation is quite straightforward – the first criterion is met. However, knowledge can be inferred from the surrounding circumstances, for example, a failure to ask obvious questions may be relied upon by a jury to imply knowledge.

You are also required to report if you have 'reasonable grounds' to suspect that the client or some other related person is engaged in Money Laundering or Financing of Terrorism. By virtue of this second, 'objective' test, the requirement to report will apply to you if based on the facts of the particular case, a person of your qualifications and experience would be expected to draw the conclusion that those facts should have led to a suspicion of Money Laundering or Financing of Terrorism. The main purpose of the objective test is to ensure that the Art Sector (and other regulated persons) are not able to argue that they failed to report because they had no conscious awareness of

the Money Laundering activity, e.g. by having turned a blind eye to incriminating information which was available to them or by claiming that they simply did not realise that the activity concerned amounted to money laundering.

iv. ***Attempted Transactions***

You also have to pay attention to **suspicious attempted transactions**. If a client attempts to conduct a transaction, but for whatever reason that transaction is not completed, and you think that the attempted transaction is suspicious, you must report it to the FIU.

Example of suspicious attempted transaction: a visitor walks into your art gallery. He says he would like to buy a painting for his living room; he has \$ 10,000 in cash to spend. He says his name is John X but when you ask him for identification he replies that he left it in his car. You insist he provide it. He goes away to get it but does not return. If you think from all the information you have that this is unusual or the transaction is related to some crime you have to report that attempted transaction to the FIU.

Therefore, an attempt is only when concrete action has been taken to proceed with the transaction.

NOTES:

It is only when *you know or reasonably suspect* that the funds are criminal proceeds or related to Money Laundering or Financing of Terrorism that you have to report: you do not have to know what the underlying criminal activity is or whether illegal activities have actually occurred.

Money Laundering can take place with any amount of money/cash. If you think a \$ 1,000 transaction is suspicious, you must report it to the FIU.

You must report suspicious transactions/activities and attempts by a terrorist entity* to enter into a transaction or continue a business relationship **on the STR/SAR Form which you may access by [clicking here](#).**

[Click here](#) for Guidance Note on Suspicious Transaction/Activity Reporting Standards to guide you in completing the STR/SAR form.

v. Identifying a Suspicious Transaction/Activity

You must determine whether a transaction or activity is suspicious based on your knowledge of the customer and of the sector. You are better positioned to have a sense of particular transactions which appear to lack justification or cannot be rationalized as falling within the usual methods of legitimate business. While general indicators may point to a suspicious transaction, sector-specific indicators would also help you and your employees to better identify suspicious transactions whether completed or attempted.

What are the risk indicators for the Art Sector?

The art sector can be used to facilitate money laundering through each of the three money laundering stages: placement, layering and integration and/or the financing of terrorism.

The following circumstances may pose a higher risk of money laundering or terrorism financing:

- **Large cash Transactions**
Cash is the mainstay of much organised criminal activity. For the criminal, it has the obvious advantage of leaving no discernable audit trail. Cash is also a weakness for criminals. Whilst they hold cash they are more at risk of being traced to the predicate offence. They will therefore often seek to dispose of cash into high value goods.
- **High Value goods**
Money launderers normally want to move funds quickly in order to avoid detection. This is more easily done in one-off transactions. The purchase of high value goods, paid for in cash, with good portability represents an attractive area for money launderers. Goods purchased with cash that can easily be sold on (even for a loss) for 'clean money' are especially attractive. High value goods are also a useful store of value and may form part of a criminal lifestyle. Goods purchased would generally be luxury items that could be potentially sold on through the black market, for example, jewellery, antiques and high performance cars.
- **Customer's behaviour**
Risk can be indicated by a customer's behaviour. For example, where a customer initially proposes to pay for goods by credit/debit card/cheque and then at the last minute presents cash as the means of payment prior to taking ownership of the goods.

- Provenance

Unclear or doubtful or incomplete provenance of the goods.

- Requests for non-disclosure to third parties.

See the [Appendix](#) for a list of red flags and suspicious indicators of which you should be cognizant.

(b) Reports of Terrorist Property/Funds

- i. You **must report immediately** to the FIU the existence of funds within your business where you know or have reasonable grounds to suspect that the funds belong to an individual or legal entity who:

commits terrorist acts or participates in or facilitates the commission of terrorist acts or the financing of terrorism; or is a terrorist entity; or

- ii. You **must report immediately** to the FIU where you know or have reasonable grounds to believe that a person or entity named on the UN list or the consolidated list circulated by the FIU has funds in Trinidad and Tobago; or

- iii. Is a Listed Entity as included in the [Trinidad & Tobago Consolidated List of Court Orders](#).

Report the existence or suspicion of terrorist funds on the **Terrorist Funds Report - FIU TFR Form** which you may access by [clicking here](#).

III. NO TIPPING-OFF

When you have made a suspicious transaction report to the FIU, you or any member of your staff must not disclose the fact or content of such report to any person. It is an offence to deliberately tell any person, including the customer, that you have or your business has filed a suspicious transaction report about the customer's transactions.

You must also not disclose to anyone any matter which may prejudice Money Laundering or Financing of Terrorism investigation or proposed investigation.

IV. RECORD KEEPING

You are required to keep a record of each and every transaction for a specified period. Record keeping is important for use in any investigation into, or analysis of, possible Money Laundering or Financing of Terrorism offences. Records must be kept in a manner which allows for swift reconstruction of individual transactions and provides evidence for prosecution of Money Laundering and other criminal activities.

You must keep the following records in electronic or written format *for at least six (6) years* or such longer period as the FIU directs. The records must be kept for six (6) years after the end of the business relationship or completion of a one-off transaction:

- (1) All domestic and international transaction records;
- (2) Source of funds declarations;
- (3) Client identification records;
- (4) Client information records;
- (5) Copies of official corporate records;
- (6) Copies of suspicious transaction reports submitted by your staff to your Compliance Officer;
- (7) A register of copies of suspicious transaction reports submitted to the FIU;
- (8) A register of all enquiries made by any Law Enforcement Authority or other competent authority;
- (9) The names, addresses, position titles and other official information pertaining to your staff;
- (10) All Wire transfers records (originator and recipient identification data); and
- (11) Other relevant records.

V. ASCERTAINING IDENTITY – KNOW YOUR CLIENT

If you are unable to identify and verify a client's identity or obtain sufficient information about the nature and purpose of a transaction, you must **NOT** carry out a transaction for that client or enter into a business relationship with the client and you must terminate any business relationship already established. You should also consider submitting a STR/SAR to the FIU.

The art sector's main difference from other business is found in the necessity to subject almost every transaction to two questions. Firstly, 'Is the ownership of an art object up for sale traceable?' (provenance

of the object); secondly, 'Are the buyers and their sources of funds identifiable?' (provenance of the funds).

While "provenance of the funds" applies to all sectors which have AML/CFT obligations, disclosure of the "provenance of the object" may be an issue due to the conflicting priorities of transparency and discretion.

Some sellers and buyers may have reasonable grounds to prefer to remain anonymous to third parties (discretion) while the need to ensure clarity on the provenance of art objects and funds has to be adequately addressed (disclosure).

Consequently, the identity of the seller and the buyer must be known to each other, and to all intermediaries involved, including to third parties with a legitimate legal interest (e.g., insurers).

Identifying the seller reduces the risks resulting from any ambiguity regarding provenance, illicit trade and forbidden exportation. Identifying the buyer reduces the risks of money laundering and illicit enrichment and serves to preserve the records on provenance of the art object. The art market operator therefore has to ensure full identification and documentation of the seller and the buyer ('know your customers' rule).

The Customer Due Diligence (CDD) obligations are designed to make it more difficult for you or your company to be used by criminals for money laundering or terrorist financing.

CDD involves determining the customer's identity. Where there is a business relationship i.e., a formal or an informal arrangement between the business and the customer that anticipates an ongoing relationship between the two parties (regular customer) it will also be necessary to ascertain the intended nature and purpose of the business relationship.

To understand the purpose and intended nature of the relationship may include some or all of the following:

- 1) Details of the customer's business or employment;
- 2) The expected source and origin of the funds to be used in the relationship;
- 3) Copies of recent and current financial statements;
- 4) The relationships between signatories and underlying beneficial owners;
- 5) The anticipated level and nature of the activity that is to be undertaken through the relationship.

High Risk Clients/Transactions

There are circumstances where the risk of money laundering or terrorist financing is higher, and Enhanced Due Diligence (EDD) measures have to be taken. You must take specific measures to identify and verify the identity of the following high risk persons (individuals or entities):

- (1) Any person who conducts a **large cash transaction** i.e. equal to or over TTD 90,000;
- (2) Domestic and Foreign Politically Exposed Persons (PEPs);
[Click here](#) for **Customer Due Diligence Guide No. 1 of 2011** for the categories of persons who are PEPs and see also the PEP Guidance Note [Click here](#) ;
- (3) Any client or transaction or service or product type that you have identified as posing a higher risk to your business e.g., transactions which involve high levels of funds or cash;
- (4) Any individual or entity who conducts complex, unusual large transactions, (whether completed or not), unusual patterns of transaction and insignificant but periodic transactions which have no apparent economic or visible lawful purpose;
- (5) Any individual or entity who conducts business transactions with persons and financial institutions in or from other countries which do not or insufficiently comply with the recommendations of the Financial Action Task Force ("the FATF");
[Click here](#) for **FATF High Risk and Non-Cooperative Jurisdictions**.
- (6) Any individual or entity for whom you have to send a suspicious transaction report to the FIU (reasonable measures and exceptions apply e.g. to avoid **tipping-off**).

You must apply **EDD measures** to high risk customers and situations which include, but are not limited to:

- (1) Obtaining additional information on the customer e.g., additional form of Government issued identification;
- (2) Obtaining details of the source of the client's funds and the purpose of the transaction if relevant;
- (3) Verifying the source of funds for the transaction e.g., if client states the cash is from his bank account, ask for proof;
- (4) Obtaining approval from a senior officer to conduct the transaction;
- (5) Applying supplementary measures to verify or certify the documents supplied or requiring certification by a financial institution;
- (6) Ongoing monitoring (e.g., monthly, quarterly, annually or on a transaction basis) of the client's account throughout the relationship; and
- (7) Implementing any other customer identification policies and procedures to prevent money laundering and financing of terrorism.

VI. Is the Client acting for a Third Party?

You must take reasonable measures to determine whether the client is acting on behalf of a third party especially where you have to conduct EDD.

Such cases will include where the client is an agent of the third party who is the beneficiary and who is providing the funds for the transaction.

In practice, this means that if the art market operator knows, or has reasonable suspicion to believe that the other party to a transaction is, in fact, acting on behalf of someone else (e.g. another buyer or seller), the art market operator must establish the identity of the true beneficial owner and their relationship with the client. This identification of the beneficial owner should take place even if the identity is to ultimately remain unknown to third parties.

[Click here](#) for Customer Due Diligence Guide No. 1 of 2011

VII. DESIGNATE A COMPLIANCE OFFICER

You must designate a senior employee or other competent professional as approved in writing by the FIU as a designated Compliance Officer (“CO”) for your business/firm. The individual you appoint will be responsible for the implementation of your compliance regime. Where an external party is the designated CO the responsibility for compliance obligations will be that of the business.

You must also appoint an alternate for the CO (“ACO”) who shall be a senior employee or such other competent professional as approved in writing by the FIU. The alternate shall discharge the functions of the CO in his absence.

You must obtain the approval of the FIU for the person chosen as the CO and ACO. If you change your CO or ACO you must inform the FIU immediately and get the FIU’s approval for the new CO and ACO.

Your CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. Depending on your type of business, your CO should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator.

If you are a small business, employing five (5) persons or less, the CO must be the person in the most senior position. If you are the owner or operator of the business and do not employ anyone, you can appoint yourself as CO.

If you are a business employing over five [5] persons, the CO should be from a senior management level and have direct access to senior management and the board of directors. Further, as a good governance practice, the appointed CO in a large business should not be directly involved in the receipt, transfer or payment of funds.

Your CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. The CO must:

- (1) have full responsibility for overseeing, developing, updating and enforcing the AML/CFT Programme;

- (2) have sufficient authority to oversee, develop, update and enforce AML/CFT policies and procedures throughout the company; and
- (3) be competent and knowledgeable regarding AML/CFT issues and risks.

Depending on your type of business, your CO should report, on a regular basis, to the board of directors or senior management, or to the owner or chief operator of the business.

The CO's responsibilities include:

- a) Submitting STRs/SARs and TFRs to the FIU and keeping relevant records;
- b) Acting as Liaison officer between your business and the FIU;
- c) Implementing your Compliance Programme;
- d) Directing and enforcing your Compliance Programme;
- e) Ensuring the training of employees on the AML/CFT; and
- f) Ensuring independent audits of your Compliance Programme.

For consistency and ongoing attention to the compliance regime, your appointed CO may choose to delegate certain duties to other employees. For example, the CO may delegate an individual in a local office or branch to ensure that compliance procedures are properly implemented at that location. However, where such a delegation is made, the CO retains full responsibility for the implementation of the compliance regime.

VIII. DEVELOP AND IMPLEMENT A COMPLIANCE PROGRAMME

After you have registered with the FIU as a reporting entity, you **must** develop a written Compliance Programme ("CP"). If you are an organization the CP also has to be approved by senior management [Click here](#) for the CP Check list.

The CP is a written document which includes a risk assessment of your particular business and which sets out your system of internal procedures, systems and controls which are intended to mitigate the vulnerabilities and inherent risks identified by you which can be exploited by money launderers and terrorism financiers. Your CP will contain measures that ensure that you comply with your reporting, record keeping, client identification, employee training, and other AML/CFT obligations. These policies,

procedures and controls, must be communicated to employees, and when fully implemented, will help reduce the risk of your business being used for money laundering or to finance terrorism.

It is advisable to revise the CP on a regular basis say every 2 years, to ensure that measures in place remain commensurate with the risks posed to the business and are current with legal obligations.

A well-designed, applied and monitored regime will provide a solid foundation for compliance with the AML/CFT laws. As not all individuals and entities operate under the same circumstances, your compliance procedures will have to be tailored to fit your individual needs. It should reflect the nature, size and complexity of your operations as well as the vulnerability of your business to money laundering and terrorism financing activities.

The following five (5) elements must be included in your compliance regime:

- (1). the appointment of a staff member as CO and his/her responsibilities;
- (2). internal compliance policies and procedures such as reporting suspicious transactions to the CO; application of CDD, EDD and record keeping;
- (3). your assessment of your risks to money laundering and terrorism financing, and measures to mitigate high risks;
- (4). ongoing compliance training for all staff at the level appropriate for their job duties; and
- (5). periodic documented review/audits of the effectiveness of implementation of your policies and procedures, training and risk assessment.

[Click here](#) to access the **Guide to Structuring an AML/CFT Compliance Programme**

IX. IMPLEMENT AND TEST YOUR COMPLIANCE PROGRAMME

Your obligations include implementing your written CP. The FIU may conduct an onsite examination to determine the effectiveness of implementation of the measures outlined in your CP.

All employees involved in the day-to-day business should be made aware of the policies and procedures in place in the business to prevent Money Laundering and Financing of Terrorism.

You must conduct internal testing to evaluate compliance by your staff with your CP, in particular, CDD record keeping and suspicious transactions reporting.

In addition, you must conduct internal testing and external independent testing to evaluate the effectiveness of your systems and controls and implementation of same. Such reviews must be documented.

PART 9

OFFENCES & PENALTIES

Non-compliance with your obligations under the AML/CFT laws and regulations may result in criminal and or administrative sanctions.

[Click here](#) to access a summary of the Offences and Penalties under the AML/CFT laws and regulations of Trinidad and Tobago.

This summary is intended to guide you in fulfilling your legal obligations under the AML/CFT laws. You may access the laws on the FIU's website, www.fiu.gov.tt under "Legal Framework". [Click here](#) to access the laws.

PART 10

ADDITIONAL RESOURCES

This summary is intended to guide you in fulfilling your legal obligations under the AML/CFT laws.

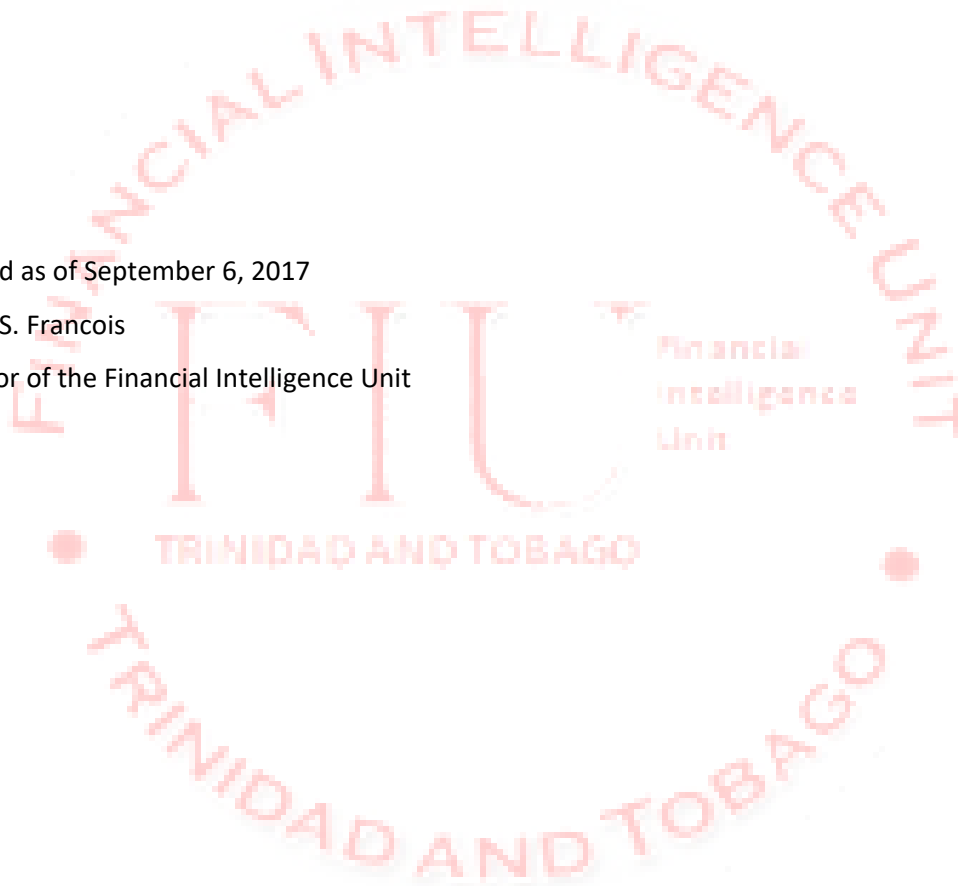
Additional reference materials include:

- I. The AML/CFT laws available on the FIU's website, www.fiu.gov.tt under "Legal Framework".
- II. The FATF recommendations at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

Revised as of September 6, 2017

Susan S. Francois

Director of the Financial Intelligence Unit



APPENDIX**AML/CFT Suspicious Indicators for the Art Sector**

Cash is the mainstay of much organised criminal activity. For the criminal, it has the obvious advantage of leaving no discernable audit trail. Cash is also a weakness for criminals. Whilst they hold cash they are more at risk of being traced to the predicate offence. They will therefore often seek to dispose of cash into high value goods.

Money launderers normally want to move funds quickly in order to avoid detection. This is more easily done in one-off transactions. The purchase of high value goods, paid for in cash, with good portability represents an attractive area for money launderers. Goods purchased with cash that can easily be sold on (even for a loss) for 'clean money' are especially attractive. High value goods are also a useful store of value and may form part of a criminal lifestyle. Goods purchased would generally be luxury items that could be potentially sold on through the black market, for example, jewellery, antiques and high performance cars.

- 1) There are no genuine reasons for paying large sums of money in cash.
- 2) Customer identification issues such as -
 - a) The customer refuses or appears reluctant to provide information requested;
 - b) There appears to be inconsistencies in the information provided by the customer;
 - c) The customer purchases are inconsistent with other profile details such as employment, area of residence;
 - d) The customer is in a hurry to rush a transaction through, with promises to provide the information later.
- 3) The goods purchased, and/or the payment arrangements are not consistent with normal practice for that type of transaction Businesses where the level of cash activity is higher than the underlying business would justify.
- 4) The customer is paying in used notes or in small denominations.
- 5) The customer will not disclose the source of cash or there appears to be inconsistencies in the information provided by the customer

- 6) In the case of regular or established customers, there is a sudden increase in the frequency/value of transactions of a particular customer without reasonable explanation
- 7) The customer is buying from an unusual location in comparison to their location.
- 8) The method of delivery is unusual, for example, a request for immediate delivery, delivery to an address other than the customer's address, or the loading of high volume/bulky goods immediately into the customer's own transport.
- 9) Cash payment is only mentioned by the customer at the conclusion of the transaction.
- 10) Instruction on the form of payment changes suddenly just before the transaction goes through.
- 11) Customer's behaviour ; for example, where a customer initially proposes to pay for goods by credit/debit card/cheque and then at the last minute presents cash as the means of payment prior to taking ownership of the goods.
- 12) Goods that are purchased and subsequently returned. (Returning high value goods paid for in cash and obtaining a refund by way of cheque enables the laundering of 'dirty money' by exchanging it for a legitimate retailer's cheque).
- 13) In the case of refunds, the customer:
 - a) Enquires about the business's refund policy;
 - b) Seeks a refund for spurious reasons;
 - c) Seeks the repayment in the form of a cheque.

Please note that this is not an exhaustive list of suspicious indicators.

Published on May 9, 2014

Revised August, 2017

ⁱ Basel Art Trade Guidelines, Working Paper series No 12, Thomas Christ, Claudia von Selle, 2012

ⁱⁱ *Ibid*