Scurdex Capital

Anti-Money Laundering and Counter Financing Terrorism Policy

NICHIE

Non-adherence to any part of this policy may result in disciplinary action including dismissal from the employment of NICHIE SYSTEMS LTD

Contents

Foreword

Scurdex Wallet is one of the crypto asset products offered by NICHIE SYSTEMS LTD and its subsidiary, Scurdex Capital Management, to retail investors in the Federal Republic of Nigeria and other foreign countries. Scurdex Capital Management is dedicated to assisting the fight against money laundering and terrorist financing by employing a successful risk-based approach. The company will do this in an effort to continue complying with legal and regulatory standards.

Through risk mitigation measures, this policy actively controls the risks connected to money laundering and terrorism funding and works to avoid, identify, and disclose any suspicions of such activity.

1. Purpose

This policy outlines NICHIE's (the company's) guiding principles and the steps it has taken to comply with all relevant legal and regulatory obligations for the fight against money laundering, corruption, and terrorism funding. This document outlines the level of care that must be taken when establishing, managing, monitoring, declassifying, or terminating business relationships at different points in the client relationship's lifespan, particularly when using our non-custodial Scurdex wallet and any of our related services.

These fundamental guidelines must be followed by the company, all of its branches, and all of its representative offices.

i. We do not take custody of funds or crypto assets of customers, investors, or users of Scurdex wallets.

ii. We don't take cryptocurrency that we know or should know are proceed of criminal activities.

iii. We don't establish or keep business connections with shell banks (financial institutions with no physical presence in any country).

iv. We must always employ an internationally regulated on-ramp and off-ramp firm to identify the user of the Scurdex wallet in relation to fiat-crypto and crypto-fiat-related transactions.

v. Throughout the whole lifecycle of the customer relationship, a risk-based strategy is used.

vi. For commercial partnerships and transactions that have higher risks, we conduct further investigations.

The major goals of this policy for employees are to:

i. Give staff members the freedom to take a risk-based approach to reducing the risks of money laundering (ML) and terrorism financing (TF), and give them a reasonable level of assurance that the company won't use the Scurdex wallet to facilitate the transfer of or accept assets that it knows are, or should be able to reasonably be expected to know are, the proceeds of crime.

ii. Make that the business adheres to all applicable money laundering laws and regulations;

iii. Establish a procedure for workers to follow when they see questionable activity, transactions, or conduct so they may alert the Money Laundering Compliance Officer (MLCO) or compliance department or escalate the situation;

iv. Maintain the trust of the organization's important stakeholders, such as the government and law enforcement.

2. Scope

This policy is applicable to all commercial ventures the firm engages in where customer relationships must be carefully investigated for anti-money laundering reasons. Each staff member is responsible for making sure they are aware of their own tasks and responsibilities as they relate to this policy, which is applicable to all workers of the company.

Discipline, up to and including dismissal, may be taken if any provision of this policy is broken.

This policy is meant to guarantee that any such interactions may be conducted in a way that safeguards the financial industry's integrity and the firm's image, rather than to forbid any business unit from engaging in activities that might be seen as higher risk.

3. *Roles and Responsibilities*

(a) The Board

The board will be in charge of making sure the firm's AML/CFT controls are reliable and sufficient for business operations. The board will also be in charge of making sure that any employees who report suspicious activities or make whistleblower complaints are shielded from mistreatment in any way.

(b) The Executive Management

Executive management, headed by the CEO, will be largely accountable for the development and upkeep of an efficient AML program that satisfies the company's goals. The executive management team must make sure that sufficient resources are made available for the AML/CCFT program's implementation, review, and control. This includes designating an AML/CFT Compliance Officer with the necessary skills, permission, and independence to lead the institution's AML/CFT compliance program.

(b) AML/CTF Compliance Officer

The AML/CFT Compliance Officer's responsibilities will also include the following:

i. Creating an AML/CFT compliance handbook

ii. Reporting to the board on matters pertaining to the AML/CFT program of the firm;

iii. Collecting and examining employee complaints of suspicious transactions;

iv. Submitting NFIU suspicious transaction reports;

v. Where required, providing regulatory reports to the NFIU to guarantee compliance;

v.i Ensuring that the firm's compliance program is implemented;

i. arranging for employee training on AML/CFT awareness, detection techniques, and reporting requirements; and

ii. serving as both a point of contact for all employees with regard to money laundering and terrorist financing problems as well as a liaison with the SEC and NFIU

4. *Overview of Money Laundring*

(a) What is Money Laundring

Money laundering is the practice of making unlawfully obtained funds appear to have been acquired legally. The nature and ownership of these unlawful gains are obscured through a wide range of techniques. The result is that the money's source and rightful owner are concealed, and it may be used again to the criminal's and/or their associates' advantage.

The initial, unlawfully obtained gains, which can take the shape of cryptocurrency, money, property, or jewels, are frequently changed into other forms, such deposits or securities, and then moved from one financial institution to another to obfuscate the audit trail.

(b) 3 Stages of Money Laundring

The operating principles are generally the same regardless of who employs the gadget for money laundering. The dynamic, three-stage process of money-laundering necessitates:

i. **Placement**

Transferring the crypto asset or money from its direct ties to crime and placing it in the banking system, an excahnge or wallet In general, this stage does two things: (a) it frees the criminal from having to retain and monitor substantial sums of heavy currency; and (b) it enters the financial system. Money launderers are more likely to be discovered during the placement phase. This is because putting a lot of money into the established banking system can make anti-money laundering investigators suspicious.

There are several options for where to put the profits of crime. For instance, money may be hidden in a suitcase and smuggled into a nation. Alternatively, structuring could be used by the launderer to prevent detection and get around reporting threshold rules. Other typical techniques include:

- Repaying debts or credit cards using money obtained illegally.
- Purchase of gaming tokens or wagering on sporting events constitutes gambling..
- The act of physically crossing a border with contraband money or other financial instruments is known as currency smuggling.
- Exchange of currencies: Buying foreign currency with ill-gotten gains.
- Using a legal cash-focused firm to mix illicit assets is known as "blending monies."

ii. **Layering**

hiding the trail to thwart a chase. Placement is followed by the layering phase. The layering step is the most challenging and frequently involves the transfer of money across borders. This phase's main goal is to detach illegal funds from their source. This is accomplished by money launderers through a succession of intricate transactions that obfuscate the audit trail and break the connection to the initial crime. For instance, in order to avoid being caught, money launderers may start moving money electronically from one nation to another before dividing it up into investments in cutting-edge financial instruments or international markets.

iii. **Integration**

The process of money laundering ends here. At this point, the criminal seems to get money from what appear to be reliable sources. The illicit proceeds, which were first put as cash and stacked via a variety of financial transactions, have now been fully incorporated into the financial system and are available for use in any way.

More and more people are realizing how easy it is to launder money and how this encourages and facilitates illegal activities. Regulations are therefore in place mandating all financial institutions to set up suitable and risk-proportionate systems and controls. In accordance with our legal and regulatory responsibilities, we must take steps to reduce the possibility that our operations may be utilized for illegal activities such money laundering, financing terrorism, corruption, or actions that violate sanctions.

5. *The AML Policy*

(a) The Policy

As part of its corporate strategy, **SCURDEX CAPITAL** complies with all applicable anti-money laundering and counter-terrorism funding laws and regulations in Nigeria as well as global best practices.

All employees, including senior management, are dedicated to abiding by the laws and policies in place to stop financial crime, terrorism, and money laundering. The company will execute and abide by the Securities and Exchange Commission's AML laws as well as industry best practices in order to accomplish this. This AML/CFT document must be read by all staff members; failing to Observing the processes outlined below might result in disciplinary action and, if required, termination of employment, independent of any legal, regulatory, or statutory consequences that might also be imposed on the employee. The business promises to:

i. Make sure that the clients' identities are successfully confirmed;

ii. Ascertain the clients' identities during the acceptance process and the duration of the business partnership;

iii. Make sure that every staff has the necessary training;

iv. Encourage staff to be aware of the need to report any questionable customers or transactions right away;

v. Adopt and disseminate a risk-based strategy to confirming the legitimacy of transactions and the identities of clients;

vi. Assign top management the proper duties for addressing the risks related to money laundering and terrorism funding, and

vii. A dedicated AML/CFT compliance officer should be appointed and supported.

(b) Regulatory Overview

The firm must abide by two parallel regimes: the regulatory and legislative regimes, as a registered and regulated business in Nigeria.

i. Regulatory

The SEC's Capital Markets Operators' anti-money laundering and Combating the Financing of Terrorism Regulations, 2013, as well as Rules 9.12 and 9.13 of the NSE Rule book, which strives to prevent and detect money laundering, as well as the regulatory requirements. To The laws specify mechanisms and controls that senior management must implement in order to reduce the possibility that a company's services or products would be utilized in the commission of financial crime.

To prevent criminals from utilizing financial institutions to launder money, the SEC regulations from 2013 on institutional responsibility call for the implementation of systems and processes. The guidelines that need to be defined and covered further in the handbook include the following

- Measures for customer due diligence (CDD) and ongoing surveillance;
- Reporting internally,
- Record-keeping procedures
- Internal controls
- Risk assessment and management;
- Compliance monitoring
- Suspicious transaction detection and reporting processes
- Programs for training staff

ii. Regulatory

The Money Laundering Prohibition (Amendment) Act's legal requirements The Terrorism (Prevention) Act of 2012, often known as the TPA The 2013 (Amendment) Act is a fund-raising initiative. Nigeria is the beneficiary of all illegal proceeds due to the nationwide anti-laundering laws. The law has a disclosure regime that makes it illegal for a company or one of its employees to conceal information or a suspicion of money laundering or the proceeds of crime. The following are only a few of the offenses in the list:

- Involvement in racketeering and organized crime.
- Terrorism, including financing of terrorism;
- Illegal distribution of psychoactive substances and narcotics;
- Smuggling of migrants and human trafficking;
- Illegal trafficking in weapons;
- Illegal distribution of psychoactive substances and narcotics;
- Corruption and Bribery;
- Fraud;
- Counterfeiting currency;
- Product theft and counterfeiting;
- Environmental crime;
- Nurder, severe physical injury;
- kidnapping, taking hostages, and unlawful restraint;
- Robbery or theft
- Smuggling
- Extortion;
- Forgery;
- Piracy; and
- Insider trading and market manipulation.

Additionally, SCURDEX CAPITAL is required to:

- Ensure to notify the NFIU and the Securities and Exchange Commission of any transactions above the thresholds of N5,000,000 for individuals and N10,000,000 for corporations, or the equivalent in any currency ("SEC").
- Ensure to notify the Securities and Exchange Commission ("SEC") and NFIU of any transfers of money or securities worth more than $10,000 USD or the equivalent in Nigerian Naira.

6. *Principal provision of Money Laundering Prohibition Act 2012*

SCURDEX CAPITAL faces AML and anti-corruption scrutiny from the following regulatory bodies (in addition to other statutory bodies):

- Securities and Exchange Commission (SEC)
- Special Control Unit Against Money
- Laundering (SCUML) - (NFIU)
- Nigerian Stock Exchange (NSE)

The MLPA 2012 establishes four primary crimes, which are largely outlined below:

- Assistance
- Failure to report
- Retaining
- Tipping off

(a) Assistance

A person commits a crime when they get, use, hold, hide, disguise, transfer, or remove property outside of Nigeria or when they enter into a contract knowing or suspecting that it would enable someone else to obtain, retain, use, or control unlawful property.

It is illegal to help someone who you know or think is laundering any money made via illicit activity. A person must have had the necessary knowledge in order to commit an offense of this nature; they cannot merely have committed the act of help.

As a result, the individual must either be aware of, suspect, or be complicit in the crime for which the property is the profits.

someone who is, has been, or has benefited from criminal activity. Anyone found guilty and sentenced for this crime risks a minimum two-year jail term.

(b) Failure to report

Employees of this business and others in the financial industry are now subject to the obligatory reporting crime. It is against the law for anyone to keep their knowledge from the firm's designated money laundering compliance officer or, where necessary, law enforcement agencies if they learn something during the course of their employment that leads them to believe that criminal funds are being laundered or that gives them a good reason to believe that they are.

There is particular Nigerian law pertaining to terrorism in addition to the MLPA 2012. According to the primary legislation, The Terrorism (Prevention) Act 2011 and the Terrorism (Prevention Amendment Act 2013), it is unlawful for anyone employed in the regulated sector to fail to report (as soon as practicable) any knowledge, suspicion, or reasonable grounds for suspicion of any of the following offenses or attempted offenses:

i. Fundraising refers to inviting others to contribute money or property to fund terrorism.

ii. Use and possession: this refers to the use of money or other items for terrorism.

iii. Engagement in financial arrangements that allow for the availability of funds or other assets to terrorist organizations.

(b) Failure to report

Anyone who keeps the proceeds of a crime or any unlawful action on behalf of another person commits an offense and, if found guilty, risks a sentence of at least five years in prison, a fine equivalent to five times the proceeds of the criminal activity, or both.

(d) Tipping off

Staff must normally take care not to alert the suspicions of the putative money launderer, even when suspicions have been reported, since this may be an infraction for the employee. If found guilty, this offense carries a sentence of two to three years in jail or a fine ranging from N500,000 to N1,000,000.00.

The Federal High Court may order the corporation's dissolution and the forfeiture of its assets to the Federal Government of Nigeria when a company is found guilty of a violation of the Money Laundering (Prohibition) Act. The staff must be on guard and make sure that no customer interaction puts the company at danger.

You are reminded of your duties and obligations to notify the compliance department right away if you have any reason to believe that there has been illegal behavior, including but not limited to money laundering.

7. *Risk - Assessment*

We describe the risk assessment for the company below in order to comply with legal regulations for anti-money laundering and terrorist financing.

The company will periodically analyze its money laundering risks using a risk-based approach with the goal of identifying the key risk factors related to our customers, goods, and services utilizing both internal and external data. The business will examine the partnership at least once a year in cases where risks have been classified as high or greater. Additionally, a Risk Management Committee will be created, and meetings will be held to discuss and debate problems and concerns pertaining to the use of the risk-based strategy.

Each business unit will need to evaluate its AML and CTF risks based on its operations, offerings, and target market.

(d) Risk-based Approach:

The company will categorize each of its clients into one of three (3) AML risk categories—high, medium, or low risk—using the proper risk factors, and it will make sure that these evaluations are periodically reviewed. When evaluating a client's risk profile, the business will take a variety of criteria into account. This will include, but not be limited to, the customers' geographic risks, industry or activity risks, and political exposure risks (PEPs). In terms of the firm's risk-based strategy, management neglects to:

i. Establish precise client acceptance requirements that call for more scrutiny as client risk rises.

ii. Establish methods for client identification and screening against relevant databases and/or information sources to assess acceptability.

iii. Create procedures to make sure client profile identifies the goal and causes of clients looking to do business with the firm.

i. Make sure that roles and duties are properly defined and recorded.

ii. Create and carry out pertinent training.

iii. Make a decision on a designated money laundering compliance officer who will be in charge of managing the AML program.

iv. Establish surveillance practices to spot and report any odd or suspicious activities.

v. Keep track of transactions and client verification procedures documentation for the time period required by law.

8. *Client/Customer Due Diligence Measures*

(a) Who is our client?

Establishing a client's identification before starting a business connection with them is one of the most crucial techniques to avoid money laundering. It is crucial that we determine who the underlying client(s) is or are as a result. You must understand your client (KYC). Although normally the link will be evident, you may want to consult the money laundering compliance officer in some complicated agreements.

Know your clients requirements:

i. Assist the company in doing the client's due diligence so that it may be fairly certain that clients are who they claim to be, are not working on behalf of others, are not subject to any government sanctions, and;

ii. give law enforcement information about clients or actions that are being looked into.

Following our initial contact with the customer, the client must be recognized as soon as practically possible, and quick verification shall follow. Most of the time, we will get this data before handling a financial transaction.

If a client's identity cannot be sufficiently confirmed, the money laundering compliance officer must be notified. Suspicion may be raised as a result of the client's resistance to the due diligence procedure.

In addition to determining the client's identification, KYC should determine the type of commerce that will be conducted. The Compliance Department must get full assistance from Client Relationship Managers (CRM) in order to gather all necessary client-related data. At the beginning of the customer relationship, extra information may be collected, including:

- the purpose or justification for starting a relationship.
- predicted activity type and intensity

- ties between the signatories and the underlying beneficial owners
- anticipated source of funding

Employees, especially CRMs, should be aware that the company has to determine who is in charge of the finances associated with or forming the basis for the connection that is being established. You must talk about the possible transaction with the money laundering compliance officer if this cannot be quickly determined.

(b) Sanction Check

The EFCC, the Nigerian Police Force, and the United Nations Security Council sanctions lists for financial sanctions targets should be compared with all prospective clients. Before carrying out the transaction for the client, this should be done. Post-transaction checks shouldn't be carried out except in extraordinary circumstances as determined by the Compliance department. All personnel are reminded that it is against the law to provide any individual on the sanctions list with money or financial services.

(c) Cleint take-on Process (onboarding)

When a client joins the business, whether through a marketing channel or a direct request for financial services from Scurdex Capital Management, the onboarding procedure must be followed. The following stages are intended to be completed concurrently, therefore they serve as an example of a work flow. All procedures must be followed, nevertheless, before starting any new firm.

Process Summary

- Before doing business, the individual introducing the firm must have finished the client onboarding form.
- Obtain the client's entire name, or the name of their firm or business;
- Make that the planned business is inside the firm's approved business operations.
- Obtaining a Board resolution on the official letterhead of the client company, together with any other pertinent corporate papers, can help you confirm, if the customer is a corporation, that the person is/are authorized to act on the client's behalf.
- AML and account opening processes must have been followed to correctly authenticate the client's identity;
- Employees must always treat customers fairly and keep in mind their other regulatory and fiduciary obligations, which are detailed elsewhere in the Compliance Manual.

9. Due Deligence Assessment

The danger of money laundering that a customer could provide to the company will be evaluated during client identification and verification, and it will be decided which of the two procedures will be used on this basis:

9.1 Enhanced due deligence(EDD)

for customers operating in high-risk environments, complicated enterprises, and politically exposed individuals, as well as for circumstances with increased risk. When a customer and product/service combination is thought to create a higher risk of money laundering or financing terrorism, a higher level of due diligence is necessary. There are several circumstances that qualify as high-risk, including:

i. where you don't really meet your customer

ii. the country where the customer resides, including any sensitive or high-risk nations

iii. the client's industry, i.e., a sensitive industry, such as tobacco, defense, or the manufacturing of guns; or

iv. while interacting with someone who is politically active (PEP).

When a client has been identified by the company as having a higher risk profile, it may be necessary to carry out further due diligence on their account. Develop a knowledge of (and documentation proof, where appropriate) the following before beginning an expanded due diligence process:

i. the source of the client's money, riches, or assets

ii. The customer may also have assets in the following companies:

iii. the prospective client's financial situation, both now and historically;

iv. any other organizations or affiliated parties linked to the client;

v. The names of each signatory and beneficial owner

vi. the client's projected account activity levels, goods, services, and transaction geography.

While having a high-risk customer does not guarantee that they will engage in money laundering or other illegal behavior, it does enhance the likelihood that they will.

(a) Sensitive Country

A sensitive nation is one that the Financial Action Task Force (FATF) has designated as having insufficient safeguards against the funding of terrorism and money laundering. As of October 2018, it had been examined in more than 80 nations. and of the 68 nations the FATF classified as having strategic shortcomings, fifty-five (55) have implemented the required changes to resolve their AML/CFT vulnerabilities, which have been eliminated. off of the list. The Financial Action Task Force (FATF) suggests that businesses:

i. Apply increased due diligence procedures in accordance with the dangers of doing business with such nations, and take into account that Iran and the Democratic People's Republic of Korea are high-risk nations. in accordance with the 2007 Money Laundering Act Regulations.

ii. Take the necessary steps in connection to the following jurisdictions (current list as of May 17, 2019) to reduce the risks involved, which may include stepping up due diligence in high-risk circumstances. Periodically, the FATF website will be examined with the goal of updating the list below as necessary.

- Bahamas
- Botswana
- Cambodia
- DPRK
- Iran
- Pakistan
- Serbia

- Sri Lanca
- Trinidad and Tobago
- Tunisia
- Yemen

(b) Politically Exposed Persons(PEPs)

When EDD measures are used, PEPs are high-ranking members of the public, including officials, lawmakers, and these individuals' immediate families and close relatives. Due to their status and potential for corruption, prominent PEPs may provide a greater danger. The CEO and the money laundering compliance officer must both approve any commercial dealings with people of this sort before the company enters into them.

The money laundering compliance officer and the CEO's consent is required in cases when the customer is already a client of the company, has an ongoing contact with us, and is classified as a PEP before the commercial relationship may proceed.

(c) What is a PEP?

The business must take into account the risks involved in offering services to people or organizations connected to politically exposed persons (PEPs). The Financial Action Task Force (FATF) definition of PEP shall be used for the purposes of this document and is as follows:

Demestic PEPs : People who currently hold or have previously held prominent domestic public positions, such as heads of state or governments, governors, local government chairmen, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, significant political party officials, family members and close friends, and members of royal families.

Foreign PEPs : Foreign officials who now hold or formerly held prominent public positions, such as Heads of State or Government, leading politicians, senior judicial, military, or government officials, senior CEOs of state-owned enterprises, or major political party figures.

- Obtaining a Board resolution on the official letterhead of the client company, together with any other pertinent corporate papers, can help you confirm, if the customer is a corporation, that the person is/are authorized to act on the client's behalf.

- AML and account opening processes must have been followed to correctly authenticate the client's identity;

- Employees must always treat customers fairly and keep in mind their other regulatory and fiduciary obligations, which are detailed elsewhere in the Compliance Manual.

International Organization PEPs: Members of senior management or those who have been given analogous roles, such as directors, deputy directors, and board members, are referred to as "persons who are or have been entrusted with a significant duty by an international organization."

A PEP's husband, partner, children and their spouses or partners, and parents are considered family members if they are linked to the PEP either directly or through marriage or other comparable (civil) forms of relationship.

Close associates are those who have a close social or professional connection to a PEP. They are people who have joint beneficial ownership in a company or other legal arrangement, who have a strong working connection with them, or who are the only beneficial owners of a company or other legal arrangement that the primary PEP established.

When working with PEPs, the staff member in charge of onboarding new clients should go through enhanced due diligence procedures to confirm the legitimacy of the client's source of funds and the nature of their business. They should also take into account the need for enhanced ongoing monitoring of account activity for potentially suspicious activity.

Before onboarding a customer, the money laundering compliance officer must receive approval from the MLRO and CEO if due diligence checks reveal that the client is a PEP or has a connection to one.

(9.2) Simplified Due Deligence(SDD)

It could be utilized by some financial sector businesses, businesses registered on a regulated market, government entities, specific pension funds, and low-risk goods.

The lowest degree of due diligence that can be finished for a customer is simplified due diligence. This is suitable in cases where there is minimal chance or risk that the use of your services or that of your clients would facilitate the funding of terrorism or the laundering of money.

When performing streamlined due diligence, you are not required to verify your customer's identification to the same degree as you would when using a standard or advanced due diligence strategy. However, the business connection must be constantly watched for developments that might necessitate the need for more due diligence in the future.

Clients who must reveal information about their ownership structure and business operations or organizations subject to the Money Laundering Regulations are often considered to be lower risk.

For instance, the MLCO may be satisfied if the client has provided documentation of their status, such as capital market operators, in cases where they are a financial services company subject to anti-money laundering regulations but are not money service operators.

Additionally, because the customer must disclose information if they are listed on a regulated market, they can be seen as having a reduced risk and subject to SDD.

A higher level of due diligence should be carried out, and the problem should be brought up with the money laundering compliance officer, if at any time during the relationship with a client, new information comes to light that indicates that the client or product may pose a higher risk than first believed.

(a) Who Qualifies for Simplified Due Deligence

The following customers and goods qualify:

i. Capital Market Operators, assuming they are subject to guidelines for preventing money laundering and funding terrorism that are in line with the guidelines in this manual and are monitored for compliance;

ii. public firms that must comply with regulatory disclosure obligations (listed on a stock exchange or in circumstances comparable to these);

iii. Ministries, parastatals, and businesses of the government;

iv. a pension, superannuation, or similar plan that offers retirement benefits to employees, where contributions are paid by payroll deduction and the plan regulations prohibit the transfer of a member's interest therein; and

v. Beneficial owners of pooled accounts owned by Designated Non-Financial Businesses and Professions (DNFBPs), if they are required to comply with anti-money laundering and anti-terrorist financing laws under the terms of the Money Laundering (Prohibition) Act.

(b) Tips to keep in mind

When working with customers, whether they be people or institutions, it is helpful to keep the following in mind:

Do's

- Always be aware of who you are dealing with; knowing your client (KYC) and being able to provide proof that you do is crucial to proving you and the company adhere to the rules against money laundering.

- Inquire about someone's identity and address, and accept the response you receive. Always respectfully respond to questions from clients by saying, "You are conducting required due diligence tests that will safeguard the customer as well as the firm."

- The law shields you from being sued once you have submitted a suspicion report to the MLCO, therefore disclose suspicions when you have "concerns." It is either you are suspicious of a customer transaction or you are not; there are no levels of suspicion.

Don'ts

- Don't talk about your suspicions with customers or coworkers. You put yourself at risk of being charged with "tipping off," a crime that might result in a serious jail sentence.

- Don't let anyone intimidate you by providing less than necessary documentary proof of identification. You and the company are always protected if there is proof that the right steps were taken and completed in full.

- Do not be reluctant to address circumstances or inquiries with the MLCO if required. When there are questions, he or she is required to offer assistance in cases of financial crime or money laundering.

10. *Introductions by an Intermediary who is an agent of the client*

Blind dependence on intermediaries or other third parties is not advised while working with them. We continue to be in charge of customer identification and verification, and we must take all required efforts to ensure that the intermediaries are following acceptable AML procedures.

Depending on the specifics of the transaction, Scurdex Capital Management's engagement with the intermediary may comprise a written agreement as well as an evaluation of the intermediary's disciplinary history, goods offered, operational expertise, and any other pertinent information available. A yearly examination and evaluation of intermediaries is required to determine if it is reasonable to depend on their confirmation.

Employees must use due diligence and confirm both the intermediary and the underlying client. They must also be satisfied that the intermediary:

a. in rare circumstances where Scurdex Capital Management does not have direct access to the underlying customers, is able to offer the information required on its due diligence procedure;

b. is governed or regulated in compliance with the fundamental AML/CFT principles;

c. is able to promptly provide copies of identity information and other pertinent documents pertaining to CDD requirements upon request;

d. will give account information upon request from the appropriate authorities.

11. *Making Payments*

Staff must confirm that a customer hasn't been added to any sanctions or wanted lists before paying them.

On notice by the money laundering compliance officer of an update to the list of financial sanctions targets, it is generally believed that all clients are assessed promptly.

Additionally, payments must be paid directly to the client—never through a third party. When money is sent in connection with a client's transaction, it must come from or go to a client's recognized, confirmed bank account.

12. *Record Keeping*

According to the money laundering legislation, businesses must keep records of customer identity and transaction data so that they may be used as evidence in any potential future investigations. The firm's policy is to keep copies of these papers for six (6) years after the client-firm relationship has ended. Our client on-boarding documents help establish the client's identification and verify the client.

The complete range of records that must be kept should include:

a. Client information

b. Transactions

c. Internal and external suspicion reports

d. Reports from Money Laundering Compliance Officers

e. Evidence of compliance monitoring and training

13. *Staff Training*

The company's policy is that all new hires get anti-money laundering training before starting their roles or within a fair amount of time after starting. Every relevant employee must obtain sufficient training on preventing money laundering and terrorist funding, as per statutory requirements. Training at Scurdex Capital Management may be conducted via online courses, in-person seminars, or ad hoc emails. The money laundering compliance officer and the compliance department will work together to produce the given training. The following crucial areas will be at the very least included in the training's scope: Regulations and Offenses Regarding AML/CFT

a. how money laundering operates;

b. Suspicious transactions and money laundering "red flags," including trade-based money laundering typologies

c. requirements for reporting;

d. Understand the needs of your clients, and

e. Policy for storing and retaining records

Each employee must annually certify to the company that they have read and comprehended the anti-money laundering handbook.

Additionally, during a fair amount of time following their membership, this declaration will be made accessible for new members to testify to. This time frame shouldn't exceed 30 days.

To document the pertinent training given to each employee, a training register will be kept.

The Compliance department will be in charge of making sure that the SEC and NFIU receive a copy of the yearly AML/CFT training program by December 31 each year so that it may be compared to the next year.

14. *Monitoring*

The client relationship manager is in charge of doing routine business relationship monitoring with their clients. Following are some examples of ongoing relationship monitoring in business:

a. to verify that the transactions are consistent with the firm's understanding of the client, his company, and his risk profile, it is required to closely examine transactions made during the life of the relationship (including, when necessary, the source of money);

b. ensuring the company maintains the most recent versions of any documents, data, or information it holds.

c. Monitoring customer behavior enables the detection of odd behaviour throughout the course of an ongoing engagement. Unusual occurrences may include money laundering or financing terrorism if they cannot be properly explained. Monitoring customer behavior and transactions throughout the course of a partnership contributes to a higher level of comfort that the company isn't being utilized for financial crime.

What is monitoring?

Any monitoring system must include the following at a minimum:

- It highlights certain transactions or activities for closer inspection.
- These complaints are quickly examined by the right person(s); and
- The results of any additional investigation are followed by the necessary action.

The company will monitor in two different ways.

First, a manual approach will be used, and employees' awareness will be relied upon. It will depend on elements like an employee's intuition,

their direct interaction with a client in person or over the phone, and their capacity to identify transactions that don't appear to make sense for that customer based on their practical experience. The money laundering compliance officer will be consulted about any possible problems. The following qualities will be highlighted in further training for employees:

- the transaction's exceptional characteristics, such as its extraordinary size or frequency for that customer or peer group;
- a series of transactions' nature, such as a sequence of cash credits;
- the location of a payment, such as to or from a nation with a high level of risk;
- parties involved: an example would be a request to send or receive money from someone on a sanctions list.

Second, a sample of both new and current clients will be chosen for compliance monitoring, which will be done on a risk-based basis. A combination of these methods or certain sorts of transactions, the client's profile, a comparison of their behavior or profile to that of a similar peer group of clients, or other methods may be used as a basis for the sampling.

Accounts and customer relationships with a higher level of risk, including those with PEPs, would often need more frequent or intense monitoring. In these circumstances, it may be necessary to conduct compliance monitoring more often, but this will be specified in the compliance strategy and plan for the year. The frequency and quantity of monitoring reviews undertaken, as well as the results of those reviews—if necessary, on an exceptional basis—will be reported to senior management on a regular basis.

15. *Reporting Obligations*

When regulatory thresholds are exceeded, it is the firm's responsibility (more specifically, the money laundering compliance officer's job) to disclose the situation to the NFIU and SEC as part of the firm's regulatory reporting requirement. The anti-money laundering reporting requirements and associated fines are shown in the table below. It should be emphasized that, in addition to the NFIU, the SEC expressly demands that the report be submitted with it.

Report Type	Reportable Transaction	Penalty for Non-compliance
Mandatory Disclosure	a single transaction involving an individual making at least N5 million or a corporate entity making at least N10 million within seven days of the transaction.	N250,000 to N1,000,000 per day for every day the violation occurs.
International Transfers of Funds and Securities	$10,000 or more in money or securities, or its equivalent in other currencies, must be transferred to or from a foreign jurisdiction within seven days of the transaction's completion.	N10,000,000 or at least three years incarceration or both for a single person. N25 million has been allocated for organization types
Suspicious Transaction	Any transactions that have one or more of the following traits: • a frequency that is excessive or unjustified • a frequency that is excessive or unjustified • looks to have neither an economic nor a legal grounding.	One million naira every day. For business organizations, the crime persists.)

SUSPICION TRANSACTION "RED FLAG"

Additionally, where there is a red flag, or a good cause to believe a transaction is connected to money laundering or terrorism funding, we are obligated to disclose it to the NFIU.

You must be able to see the telltale indicators of a potentially suspicious transaction while dealing with transactions as a business employee. When dealing with, staff members need to be attentive and enhance their concentration.

i. transactions between nations at high risk of money laundering,

ii. transactions involving fictitious businesses.

iii. Deals with reporters who have been deemed to carry a higher level of danger.

iv. large transaction activity using financial instruments, particularly serially numbered ones, including traveler's checks, bank drafts, and money orders.

v. Transactions with amounts slightly below the required reporting level or queries that seem to test an institution's own internal monitoring thresholds or procedures.

Customer-facing and relations employees would need to be on the lookout for any complex transactions, abnormally big ones, or strange patterns of transactions that serve no obvious or discernible economic or legal purpose.
the following transactions or patterns of transactions:

i. major business in the context of a relationship

ii. transactions that are over specified thresholds,

iii. significant account turnover, a little balance compared to other accounts, or

iv. Transactions that don't follow the account's typical activity pattern

TERRORIST FINANCING "RED FLAGS"

i. Particularly when the address is also a business location that does not seem to fit with the declared vocation (e.g., student, jobless, or self-employed), parties to a transaction may share an address or phone number.

ii. A non-profit or charity organization buying or selling stocks for which there doesn't seem to be any rational economic justification and where there doesn't seem to be any connection between the organization's declared objective and the other parties involved.

iii. huge amount of securities transfers through a company account when there doesn't seem to be any discernible commercial or other financial reason for the transfers, especially when this activity includes places that have been identified as high-risk

iv. The kind and intensity of account activity are not compatible with the clients' claimed occupations.

v. Several individual and commercial accounts, as well as non-profit or charitable accounts used to gather and transfer securities to a select number of overseas beneficiaries.

Escalations

A Money Laundering Compliance Officer should be established as soon as possible when an employee has good reason to believe they have discovered or detected an unusual transaction. A review panel will be established right once to look into the situation, working under the direction of the ML Compliance Officer.

The secrecy of the ongoing inquiry and its possible results, as well as a record of every step done throughout the investigation, shall be upheld.

The Review Panel will need to investigate the history and purpose of such transactions as thoroughly as they can without giving the customer away, then report their findings in writing. A suspicious activity report would be sent to the NFIU when The Panel determines that there are adequate or reasonable reasons to think that the funds are the proceeds of criminal activity or connected to terrorist funding. Regardless of the value, any suspicious transactions, including attempted Transactions, will be reported.

It is not permitted for any employee to discuss the need to submit a report with the authorities.