



AML/CFT 101

CFATF Secretariat Research Desk
October 27th, 2020

Ponzi or Pyramid Schemes: ML/TF Risks



What are Ponzi/Pyramid Schemes?

* Source: [FATF Report on ML/TF in the Securities Sector](#)

- A Ponzi/Pyramid scheme is a type of investment fraud named after Charles Ponzi, who operated such a scheme in the U.S. in the 1920s.
- Under the scheme, investors are offered unsustainably high rates of interest and are initially paid their interest from a fund consisting of new deposits. When the deposits dry up, the scheme collapses*.
- These types of schemes are designed to defraud persons for financial gains.
- It is a predicate crime category for ML.



Pyramid schemes in the Caribbean

- Pyramid schemes emerged within several CFATF member jurisdictions during the COVID-19 pandemic.
- These schemes were of varying patterns, structures and investment amounts and occurred through several means including via the internet (social media).
- The use of pyramid schemes poses significant ML/TF risks to some of our Member countries including Suriname, Dominica and Trinidad and Tobago.

Did you know?



Several of Caribbean FIUs reported a significant rise of pyramid schemes during the COVID-19 period due to persons' loss of income and job insecurity. This is because the pyramid schemes lure persons with a quick and significant financial return within a short period of time.

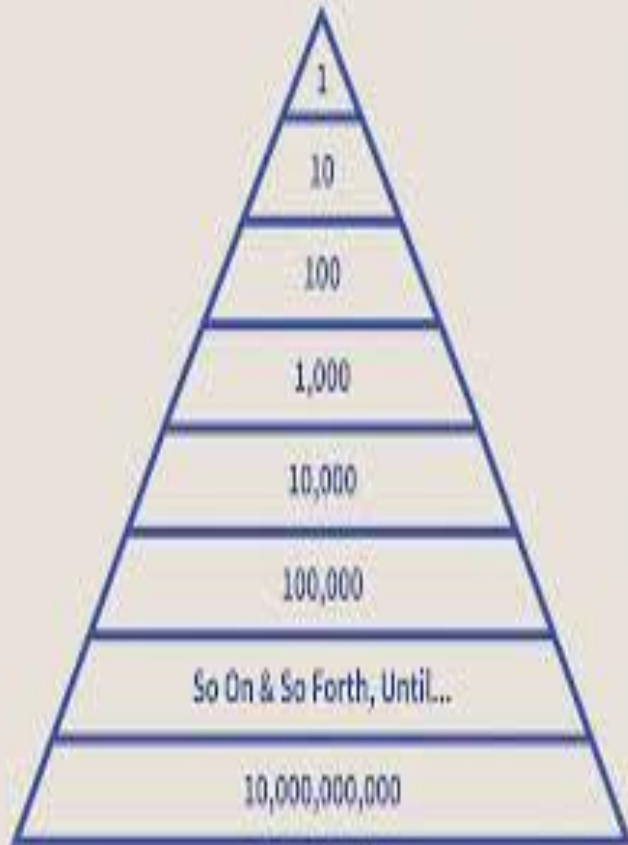
The schemes are operated via different mechanisms inclusive of social media, virtual meeting platforms and even direct face to face meetings.

A pyramid scheme requires persons to make an initial contribution with the promise of receiving higher returns.

In several instances, members of the schemes are also required to recruit new members with the incentive of receiving a higher pay-out.



HOW TO RECOGNIZE PYRAMID SCHEMES



Large start up costs.

Emphasis on recruitment rather than sales. Income is based upon number of people recruited.

No interest in consumer demand or market research.

Requirement to buy significant inventory.

Forced to buy other unnecessary items just to stay in good standing with the company.

ML TRENDS NOTIFICATION AND ADVISORIES

TRINIDAD AND TOBAGO FINANCIAL INTELLIGENCE UNIT ADVISORY



GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO
FINANCIAL INTELLIGENCE UNIT
MINISTRY OF FINANCE

BEWARE OF ROMANCE SCAM

S: **Social Media Platforms** utilised; victims are usually at a vulnerable stage in their lives. **COVID-19 pandemic:** perpetrators take advantage of increase use of social media to identify potential victims.

C: **Communication** is usually done through email, Facebook, Instagram, text or phone calls. There is **NO physical meeting**.

M: **Minimal** information about the purpose of the transaction. Once the 'payment' is made, the perpetrator or co-conspirator makes **ATM or in-branch cash withdrawals**.

A: **Abnormal** transactions conducted by Victim following requests by the perpetrator or an 'alleged Courier Service' to make deposits into named individual accounts for the purpose of '**clearing a package**'.

1. Social Media Platforms Used

2. 'Relationship' develops; promises of gifts

3. Request for money to 'clear packages'

4. ATM/In-branch cash withdrawals

The perpetrator can continue to 'engineer' the relationship or target a new victim

Requests for money can be made multiple times

WARNING Romance SCAM

August 10, 2020

WARNING Romance SCAM

Source: WWW.FIU.GOV.TT



ML TRENDS NOTIFICATION AND ADVISORIES The Eastern Caribbean Securities Regulatory Commission: Pyramid Scheme

WARNING NOTICE: COVID-19 RELATED SCAMS

Author: ECSRC Date: Fri, Jul 24th,2020

The Eastern Caribbean Securities Regulatory Commission (ECSRC) advises the public in the member countries of the Eastern Caribbean Currency Union (ECCU) to be aware of fraudulent investment offerings that are being circulated via the internet and other channels.

These scams are currently being promoted using the COVID-19 pandemic as a cover to target unsuspecting or vulnerable individuals in times of economic stagnation and downturns. They include: Pyramid Schemes, Unauthorised Forex Trading, false COVID-19 related investments and Work From Home and Personal Finance Scams.

Pyramid Schemes

A Pyramid Scheme is a fraudulent investment offering that profits almost solely through the recruitment of other participants into the programme. The ECSRC warns the public to be on the alert for the following red flags of a Pyramid Scheme:

1. Emphasis on recruiting new participants to join the scheme;
2. Promise of a high return over a short time;
3. No genuine product or service is offered; and
4. Complex commission

Source: <https://www.ecsrc.com/gallery/NewsItems/detail/150>



UNAUTHORISED FOREIGN EXCHANGE MARKET (FOREX) TRADING

Unauthorised Forex Trading Scams offer the chance to trade in foreign exchange, contracts for difference, binary options, crypto-assets and other commodities. These scams offer very high returns and guaranteed profits either through managed accounts where the firm makes trades on the investor's behalf or by trading using the firm's trading platform.

The ECSRC also warns of other types of financial scams which all seek to capitalise on the unprecedented anxiety caused by the COVID 19 pandemic, such as:

Work-From-Home Scams: fraudsters seek to take advantage of individuals seeking alternative sources of financing due to COVID 19.

Personal Finance Scams: using the fear of current economic conditions, fraudsters target individuals by posing as a financial institution requesting sensitive personal or financial

All of these schemes are usually operated in violation of the law by evading legal requirements such as obtaining the necessary licences or authorisations to raise funds from the public for collective investment purposes.

How to Protect Yourself

1. Be suspicious of persons who contact you to invest quickly or promise high returns on your
2. Consider seeking financial advice or guidance before you
3. Ensure that any individual or firm with which you conduct business is licensed or authorised by the ECSRC or other relevant government

The ECSRC will continue to take the necessary measures to prevent securities fraud in the Eastern Caribbean Securities Market, therefore, if you are aware of or have been the victim of a fraudulent scheme in the ECCU, we encourage you to contact the ECSRC via email at ecsrc@eccb-centralbank.org or the law enforcement authorities in your country.

[Click here to view ECCB Connects Season 13 Episode 11 – Avoiding Financial Scams.](#)

Source: <https://www.ecsrc.com/gallery/NewsItems/detail/150>



ONDCP COVID-19 FRAUD ALERT



LOOK OUT FOR:



Messages from Unknown Sources

As a general caution, the public should continue to be cautious as always about messages/emails from unknown senders.



Phishing Scams

Cybercriminals contact you by phone, email or social media and lure you to click on links or download attachments which either prompt you to divulge personal and financial information or allow criminals to steal sensitive information from your device.



Imposter Scams

Entities solicit donations or offer relief via phone, email, or social media by impersonating government officials and agencies or international organizations



Product Scams

Various bad actors use online platforms to fraudulently market medical supplies, personal protective equipment, or unapproved products that make false health claims pertaining to COVID-19.



HOW TO IDENTIFY THESE SCAMS:

Invariably, these fraud schemes will contain one or more of the following elements.



Attempts to obtain your personal and financial information such as credit card numbers and security codes



Instructions to download attachments or click on links



Communication from fake entities disguised as legitimate or reputable organizations



Fake social media profiles or websites that are almost identical to the real ones



Offers of assistance or "free" merchandise



PROTECT YOURSELF

- Do not provide personal or banking information to unknown or untrusted entities.
- Do not open attachments or links from unfamiliar sources.
- Beware of individuals impersonating government officials or agencies.
- Beware of offers from banks and other financial institutions for debt waivers, ATM and online banking services.
- Check for variations in usual contact information or payment instructions.
- Contact organizations directly to verify information.
- Do not use contact information obtained from questionable websites or emails. Use a number that you already have or the one listed in the phone book.
- Ask yourself, is this the normal way for this person or company to contact me
- **Nothing free requires you to send money first; this is almost always a sure sign of a scam.**



NEED HELP?

The ONDCP encourages the general public to remain financially vigilant and to report any suspected fraudulent activity related to COVID-19. Designated officers can be contacted via telephone at 764-8934 or 764-8930, or via email at supervisory.authority@ondcp.gov.ag



Pyramid schemes and effective ML/TF Supervision

Criminals continue to find new creative means by which they exploit the financial system and bypass the existing requirements more so during the COVID-19 pandemic.

The FATF has continuously emphasised the risk-based approach in the implementation of their Standards. The effective application of the following FATF Recommendations is critical during this time to defend countries' financial systems against the ML/TF risks of Pyramid Schemes:

Rec. 10 - Customer Due Diligence (CDD)

Rec. 26 - Regulation and supervision of financial institutions

Rec. 27 - Powers of supervisors

Rec. 28 - Regulation and supervision of DNFBPs

FATF Recommendations: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

FATF GUIDANCE



The FATF has published numerous risk-based guidance which provide comprehensive best practices on how its member jurisdictions and the private sector should implement the FATF requirements. The following is a list (hyperlinked for easy access) of some of the guidance that are useful to countries' FIs, DNFBPs and VASPs in the fight against ML/TF including pyramid schemes as a predicate offence:

[Risk-based approach for the banking sector \(2014\)](#)

[Risk-based approach for money or value transfer services \(2016\)](#)

[Risk-based approach for life insurance sector \(2018\)](#)

[Risk-based approach for the Security Sector \(2018\)](#)

[Risk-based Approach virtual assets and virtual asset services providers \(2019\)](#)

[Guidance on Digital Identification \(2020\)](#)

[Guidance on the effective supervision by AML/CFT Supervisors and Law Enforcement Authorities](#)