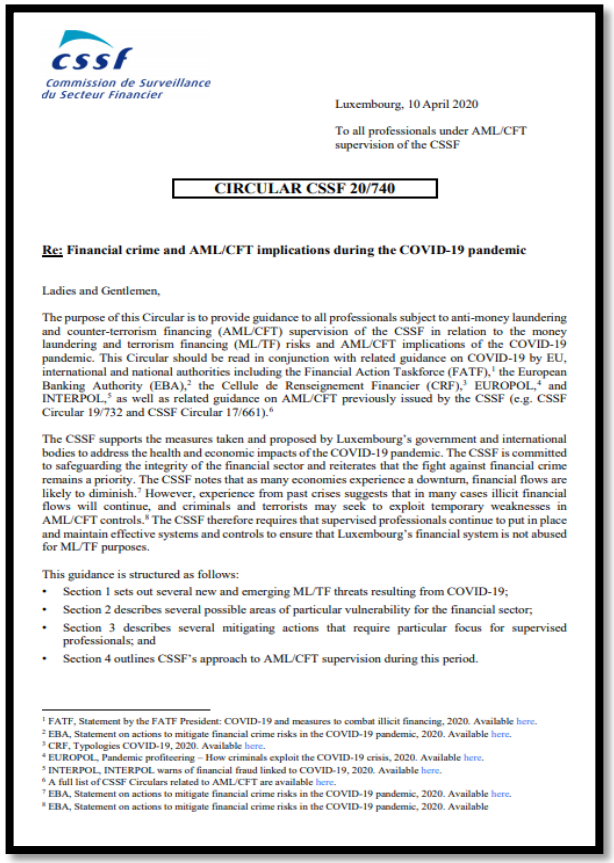
Commission de Surveillance du Secteur Financier

AML/CFT supervision in the Collective Investment Sector during the Covid-19 situation

April 2020

Must read

The **CSSF Circular 20/740** tackles Financial crime and AML/CFT implications during the COVID-19 pandemic. It is, to date, the key document published by the CSSF to provide detailed information to all entities supervised by the CSSF.



cssf
Commission de Surveillance du Secteur Financier

Luxembourg, 10 April 2020

To all professionals under AML/CFT supervision of the CSSF

CIRCULAR CSSF 20/740

Re: Financial crime and AML/CFT implications during the COVID-19 pandemic

Ladies and Gentlemen,

The purpose of this Circular is to provide guidance to all professionals subject to anti-money laundering and counter-terrorism financing (AML/CFT) supervision of the CSSF in relation to the money laundering and terrorism financing (ML/TF) risks and AML/CFT implications of the COVID-19 pandemic. This Circular should be read in conjunction with related guidance on COVID-19 by EU, international and national authorities including the Financial Action Taskforce (FATF),[1] the European Banking Authority (EBA),[2] the Cellule de Renseignement Financier (CRF),[3] EUROPOL,[4] and INTERPOL,[5] as well as related guidance on AML/CFT previously issued by the CSSF (e.g. CSSF Circular 19/732 and CSSF Circular 17/661).[6]

The CSSF supports the measures taken and proposed by Luxembourg's government and international bodies to address the health and economic impacts of the COVID-19 pandemic. The CSSF is committed to safeguarding the integrity of the financial sector and reiterates that the fight against financial crime remains a priority. The CSSF notes that as many economies experience a downturn, financial flows are likely to diminish.[7] However, experience from past crises suggests that in many cases illicit financial flows will continue, and criminals and terrorists may seek to exploit temporary weaknesses in AML/CFT controls.[8] The CSSF therefore requires that supervised professionals continue to put in place and maintain effective systems and controls to ensure that Luxembourg's financial system is not abused for ML/TF purposes.

This guidance is structured as follows:

- Section 1 sets out several new and emerging ML/TF threats resulting from COVID-19;
- Section 2 describes several possible areas of particular vulnerability for the financial sector;
- Section 3 describes several mitigating actions that require particular focus for supervised professionals; and
- Section 4 outlines CSSF's approach to AML/CFT supervision during this period.

[1] FATF, Statement by the FATF President: COVID-19 and measures to combat illicit financing, 2020. Available here.
[2] EBA, Statement on actions to mitigate financial crime risks in the COVID-19 pandemic, 2020. Available here.
[3] CRF, Typologies COVID-19, 2020. Available here.
[4] EUROPOL, Pandemic profiteering – How criminals exploit the COVID-19 crisis, 2020. Available here.
[5] INTERPOL, INTERPOL warns of financial fraud linked to COVID-19, 2020. Available here.
[6] A full list of CSSF Circulars related to AML/CFT are available here.
[7] EBA, Statement on actions to mitigate financial crime risks in the COVID-19 pandemic, 2020. Available here.
[8] EBA, Statement on actions to mitigate financial crime risks in the COVID-19 pandemic, 2020. Available

The circular is structured as follows:

- Section 1 sets out several new and emerging ML/TF threats resulting from COVID-19;
- Section 2 describes several possible areas of particular vulnerability for the financial sector;
- Section 3 describes several mitigating actions that require particular focus for supervised professionals; and;
- Section 4 outlines CSSF's approach to AML/CFT supervision during this period.

Click on the preview to access the complete document

(you will need to be connected to the Internet)

Purpose of the document

This document takes the form of a PowerPoint presentation saved as a PDF file so that it can be quickly disseminated to the employees of supervised entities involved in the Collective Investment Sector ("CIS"). **It is designed to provide sector specific details to the CSSF circular 20/740.**

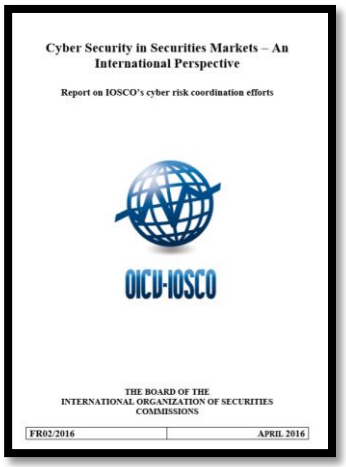
The idea to design this document appeared in the Expert Working Group AML OPC composed of representatives of several fund industry associations as well as service providers and the FIU.

The members recognized that in those difficult times, a ready-to-use document be used as part of the remote training process implemented by the entities so that all their lines of defense remain abreast of the implications of the Covid-19 situation in the fight against money laundering and terrorism financing.

You will see that there is nothing really "new" created by this Covid-19 outbreak, however, a conjunction of factors increased existing threats and vulnerabilities in the CIS.

#Stay Safe
#Bleiwt Gesond

Lists of recommended reading material.


Cyber Security in Securities Markets – An International Perspective

Report on IOSCO's cyber risk coordination efforts

IOSCO

THE BOARD OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR02/2016 APRIL 2016

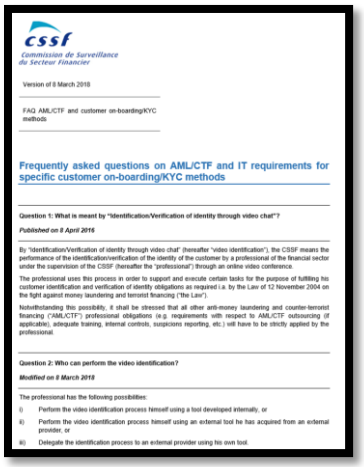

Cyber Task Force

Final Report

IOSCO

The Board OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR09/2019 JUNE 2019


CSSF Commission de Surveillance du Secteur Financier

Version of 8 March 2018

FAQ AML/CTF and customer on-boarding/KYC methods

Frequently asked questions on AML/CTF and IT requirements for specific customer on-boarding/KYC methods

Question 1: What is meant by "Identification/Verification of identity through video chat"?

Published on 8 April 2016

By "identification/verification of identity through video chat" (hereafter "video identification"), the CSSF means the performance of the identification/verification of the identity of the customer by a professional of the financial sector under the supervision of the CSSF (hereafter the "professional") through an online video conference.

The professional uses this process in order to support and execute certain tasks for the purpose of fulfilling his customer identification and verification of identity obligations as required i.a. by the Law of 12 November 2004 on the fight against money laundering and terrorist financing ("the Law").

Notwithstanding this possibility, it shall be stressed that all other anti-money laundering and counter-terrorist financing ("AML/CTF") professional obligations (e.g. requirements with respect to AML/CTF outsourcing (if applicable), adequate training, internal controls, suspicions reporting, etc.) will have to be strictly applied by the professional.

Question 2: Who can perform the video identification?

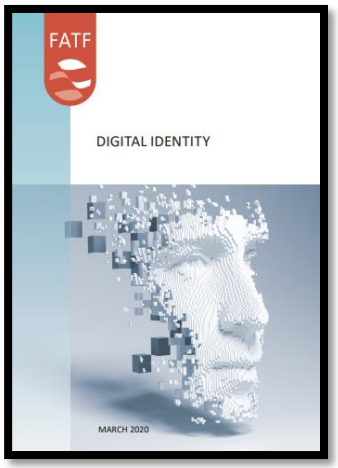
Modified on 8 March 2018

The professional has the following possibilities:

i) Perform the video identification process himself using a tool developed internally, or

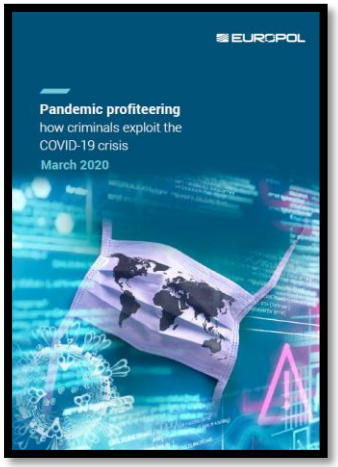
ii) Perform the video identification process himself using an external tool he has acquired from an external provider, or

iii) Delegate the identification process to an external provider using his own tool.


FATF

DIGITAL IDENTITY

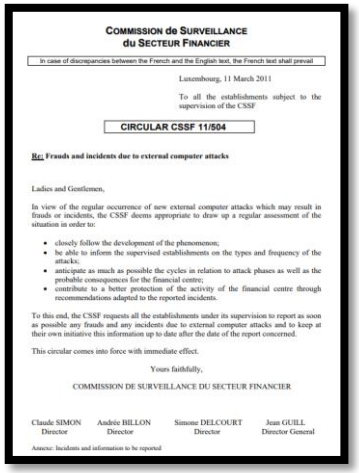
MARCH 2020


EUROPOL

Pandemic profiteering

how criminals exploit the COVID-19 crisis

March 2020


COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 11 March 2011

To all the establishments subject to the supervision of the CSSF

CIRCULAR CSSF 11/504

Re: Frauds and incidents due to external computer attacks

Ladies and Gentlemen,

In view of the regular occurrence of new external computer attacks which may result in frauds or incidents, the CSSF deems appropriate to draw up a regular assessment of the situation in order to:

- closely follow the development of the phenomenon;
- be able to inform the supervised establishments on the types and frequency of the attacks;
- anticipate as much as possible the cycles in relation to attack phases as well as the probable consequences for the financial centre;
- contribute to a better protection of the activity of the financial centre through recommendations adapted to the reported incidents.

To this end, the CSSF requests all the establishments under its supervision to report as soon as possible any frauds and any incidents due to external computer attacks and to keep at their own initiative this information up to date after the date of the report concerned.

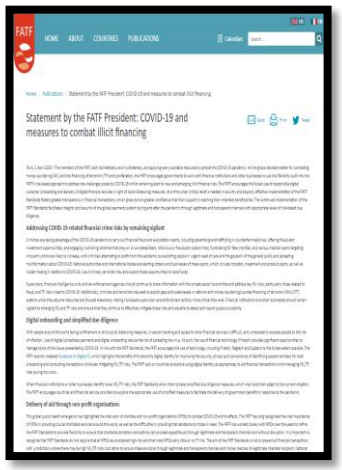
This circular comes into force with immediate effect.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON Director | Andrée BILLON Director | Simone DELCOURT Director | Jean GUILL Director General

Annexe: Incidents and information to be reported


FATF

HOME ABOUT COUNTRIES PUBLICATIONS

Statement by the FATF President: COVID-19 and measures to combat illicit financing

Click on the preview to access the complete documents

(you will need to be connected to the Internet)

Preliminary Remarks
Introduction

HIGHER RESILIENCE

It appears that client onboarding' AML/CFT controls in the Collective Investment Sector ("CIS") have been less affected than in other sectors mostly because non-face to face entering into business relationship is common practice.

OPERATIONAL SET-UP

Nevertheless, like the other sectors, some work performed by internal and external controls function have been affected to different extent depending on the operational set-up of the entities.

IMPACT ASSESSMENT RR & RC

Therefore, even though there is no definite and accurate assessment of the magnitude of the impact of Covid-19 on the AML/CFT controls in the CIS, it is clear that there is an impact which entails a case by case analysis by the *Responsable du Respect* and *Responsable du Contrôle* of these entities.

Overview

1. **Understanding Covid-19 ML/TF threats & vulnerabilities**
2. Implementing tailor-made mitigation measures
3. Typologies & Red flags
4. Quiz

Understanding Covid-19 ML/TF threats
At a glance

- New uncontrolled communication channels (Zoom, WhatsApp) increase insider trading threats

- Spear phishing emails (aka CEO fraud): increase risk of revealing confidential information or performing undue transactions.
- Use of Malware (e.g. ransomware) to damage or gain unauthorized access to systems

- Market volatility and high transactions volume create white noise making market abuse easier.
- Illiquidity and fund suspension are catalysts for market abuse.

- Some employees may use the less stringent control environment to steal data from their employers.

Have a look at section 1 of CSSF 20/740 for further information

Understanding Covid-19 ML/TF vulnerabilities
At a glance

> Vulnerability is the relative exposure of a sector or sub-sector for ML/TF purposes. FATF defines vulnerabilities as "things that may be exploited by the threat or that may support or facilitate its activities".[42] This may also include the features of a particular sector, a financial product or type of service that make them exposed to ML/TF.

Source: CSSF Sub-Sector Risk Assessment (CIS) – 01/2020

<u>The following list is not exhaustive:</u>

- Physical distancing may entail difficulties to communicate within the entity and get advice from RR or RC.
- Quarantine measures make it difficult for investors to comply with some existing AML/CFT procedures requirements (e.g. certification of documents)
- Change of investors' behaviors may confuse transactions monitoring software and generate increase amount of alerts to review and document.

Have a look at section 2 of CSSF 20/740 for further information

Understanding Covid-19 ML/TF vulnerabilities
An example of to-do-list for RR & RC

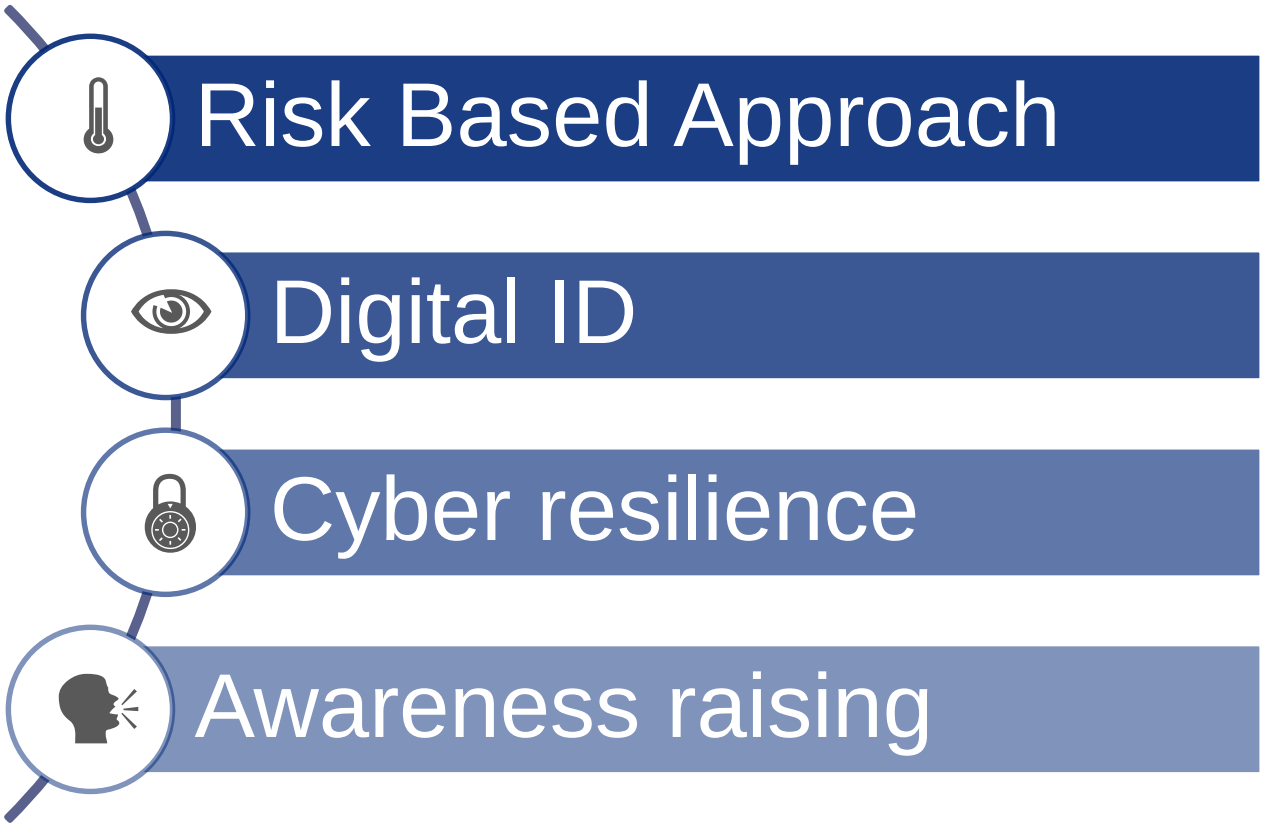
- If you do not have an RR and RC in your entity, now is the time to appoint them.
- Ensure that you have submitted the yearly CSSF AML/CFT survey.
- Ensure that your questionnaire has not been reset due to potential mistakes (notification by email and available in eDesk).
- Regularly communicate with your colleagues to remind them you are available for AML/CFT related questions, for instance a weekly conference call when colleagues can discuss AML/CFT matters requiring clarification.
- Read the SSRA CIS and re-evaluate (as necessary) the AML/CFT risk scoring of the Entity.
- Read the amended AML Law which was transposed AMLD5 in March 2020.

Overview

1. Understanding Covid-19 ML/TF threats
2. **Implementing tailor-made mitigation measures**
3. Typologies & Red flags
4. Quiz

Implementing tailor-made mitigation measures

At a glance



Have a look at section 3 of CSSF 20/740 for further information

Implementing tailor-made mitigation measures

Risk Based Approach

- RBA is the cornerstone of an efficient AML/CFT framework.
- In times of crisis, regular mitigation measures may no longer apply, therefore the procedures of the Entity need to be reviewed to curb the risks in an adequate and appropriate manner (e.g. implementation of four eyes control).
- A distinction should be made by Entities between the legal requirements and the in-house additional controls that could be adapted to the circumstance.

Illustration (legal requirement):

During the Covid-19 outbreak, a new investor appears to be a PEP following the name screening control, the Entity must apply Enhanced Due Diligence as required by the AML law of 12 November 2004 as amended.

Illustration (in-house additional control):

Usually Entity TipTop SARL requires subscription orders to be sent by Fax. During the Covid-19 outbreak, it could allow subscriptions sent by email with a call back to the subscriber.

Implementing tailor-made mitigation measures

Digital ID

Additional source: FATF Guidance on Digital identity – March 2020

- New ways of identifying (who are you?) and authenticating (are you the one I identified?) are available and could replace wet ink certification. They could be used to overcome travel restrictions and quarantines.
- Due Diligence on service providers must still be performed even during the Covid-19 outbreak, Digital ID providers are no exception (see points 138-141 of FATF Guidance on Digital ID).
- GDPR must be taken into consideration when changing operational process related to Personal Identification Information.

Implementing tailor-made mitigation measures

Cyber resilience

> Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack.

Source: European Central Bank

Cyber threats have been reported as increasing sharply during the Covid-19 outbreak.

CIS entities must ensure that the IT (local) and Cyber (Internet) components are sufficient to ensure security, integrity and confidentiality of data as required by article 5.2 of CSSF Regulation 10/04.

There are multiple vectors of cyber threats and any successful attack (e.g. computer infected by a Ransomware) must be reported to the CSSF in accordance with CSSF circular 11/504.

Penetration testing, social engineering audit could be performed to test the resilience of the cyber defenses of the Entities.

Access rights to critical software and documents repositories must be performed by the Entity. In addition, a review of the modification logs for controls software should be performed (e.g. rules implemented in transactions monitoring system).

Implementing tailor-made mitigation measures

Awareness raising

Working remotely for a significant amount of time may prevent employees from being aware of the latest typologies of ML/TF that the Entity has been confronted with.

Working hours may be shuffled around to take care of children, rendering communication more difficult between colleagues.

It is paramount that the RR and/or the RC of the Entities keep in contact with their colleagues and provide regular update on the Covid-19 related threats and on the operational modifications that they entailed on the Entity's AML/CFT framework.

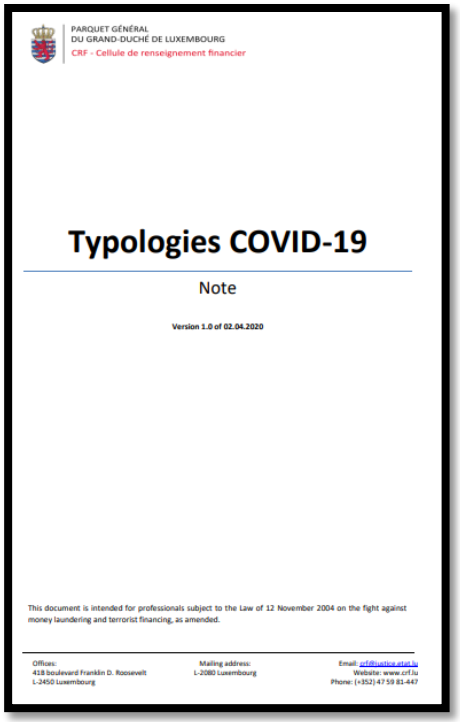
AML/CFT professional obligations are not put on hold during the crisis, it is the role of RR and RC to ensure that they are complied with.

Overview

1. Understanding Covid-19 ML/TF threats
2. Implementing tailor-made mitigation measures
3. **Typologies & Red flags**
4. Quiz

Typologies & red flags

Typologies COVID-19 (FIU-LUX)


PARQUET GÉNÉRAL
DU GRAND-DUCHÉ DE LUXEMBOURG
CRF - Cellule de renseignement financier

Typologies COVID-19

Note

Version 1.0 of 02.04.2020

This document is intended for professionals subject to the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended.

Offices:
41B boulevard Franklin D. Roosevelt
L-2450 Luxembourg

Mailing address:
L-2080 Luxembourg

Email: crf@justice.etat.lu
Website: www.crf.lu
Phone: (+352) 47 59 81-447

Focus on : Social Engineering

Under the pretext of corporate disruption, fraudsters argue that payments are no longer to be made to the company's central banking accounts, but directly to the banking accounts of the relevant production sites. They may also argue, for example, that they are experiencing cash flow problems or problems with their accounting department. This scheme allows payments made within the framework of an existing business relationship to be diverted to fraudulent accounts.

Typologies & red flags

Typologies COVID-19

Focus on : Corruption

Theoretical illustration:

An investor in a fund is a Politically Exposed Person due to her function as Health Minister in country X.

Up until the Covid-19 crisis she had made ten subscriptions over five years mounting to 1 000 000 EUR in holdings in the fund.

In April 2020, she suddenly sends a subscription order for a single value of 2 000 000 EUR and informs the Registrar Transfer Agent ("RTA") that the source of funds is the sale of her yacht.

The Depositary Bank provides the SWIFT message of the transaction to the RTA which notices that the bank account from which the money was sent is not the one that has been entered in the payment system.
An Internet search reveals that the IBAN used on the SWIFT is mentioned on the webpage of a foundation owned by a pharmaceutical company.

Further Open Source INTelligence research reveals that this particular pharma company has just secured a multi billion dollars contract to provide Country X with masks and respirators.

Typologies & red flags

Red flags

- The investor insists on the urgency of the redemption to be carried out. This attitude may be the result of the pressure exerted on the investor by the criminal, who explains that failing immediate payment, the goods (e.g. masks) - which are in great demand - will be sent to another customer.

- New subscriptions explained by income not linked to regular professional activity, for instance, sale of masks, sale of pharmaceutical products.

- Third party redemption to supposedly pay for the medical bills of a person infected by the Covid-19.

- Email request of change of banking details before sending a redemption order.

Overview

1. Understanding Covid-19 ML/TF threats
2. Implementing tailor-made mitigation measures
3. Typologies & Red flags
4. **Quiz**

Quizz

Rules

This quiz is composed of 5 questions related on this document's content.

The answers to the 5 questions are provided at the end of the document.

The quiz results are not sent to the CSSF.

Quizz

Question 1/5

The Collective Investment Sector’s professionals have been severely impacted by Covid-19 for onboarding new clients as they usually meet with them face to face.

- ☐ True
- ☐ False

Quizz

Question 2/5

According to current information, what is the ML/TF threat that has been mostly observed in the CIS due to the Covid-19 outbreak ?

a) Insider Trading

b) Cybercrime

c) Data theft

Quizz

Question 3/5

The FATF recently published a Guidance on Digital Identity which could prove useful for investors' onboarding and KYC remediation during the Covid-19 outbreak.

- ☐ True
- ☐ False

Quizz

Question 4/5

What should RR and RC do during the Covid-19 with regards to the AML/CFT framework of their Entity? (multiple answers may apply)

a) Review the procedures to assess if they are adapted to the current situation.

b) Organize regular calls with their colleagues to answer their questions and bring them up to date on COVID-19 impact on the AML/CFT framework.

c) Read the CIS SSRA (if not already done) and the FATF Guidance on Digital ID.

Quizz

Question 5/5

What could Entities do to assess their Cyber and IT resilience?

a) Organize Networks Penetration testing (a.k.a. Pentests).

b) Review logs and access rights to folders and software.

c) All of the above.

Thank you for your attention !

#Stay Safe
#Bleiwt Gesond

https://www.cssf.lu/en/financial-crime/

For further information or for any question, please feel free to contact us.

Quiz answers

1. False | 2. b | 3.True | 4. a + b+ c | 5. c