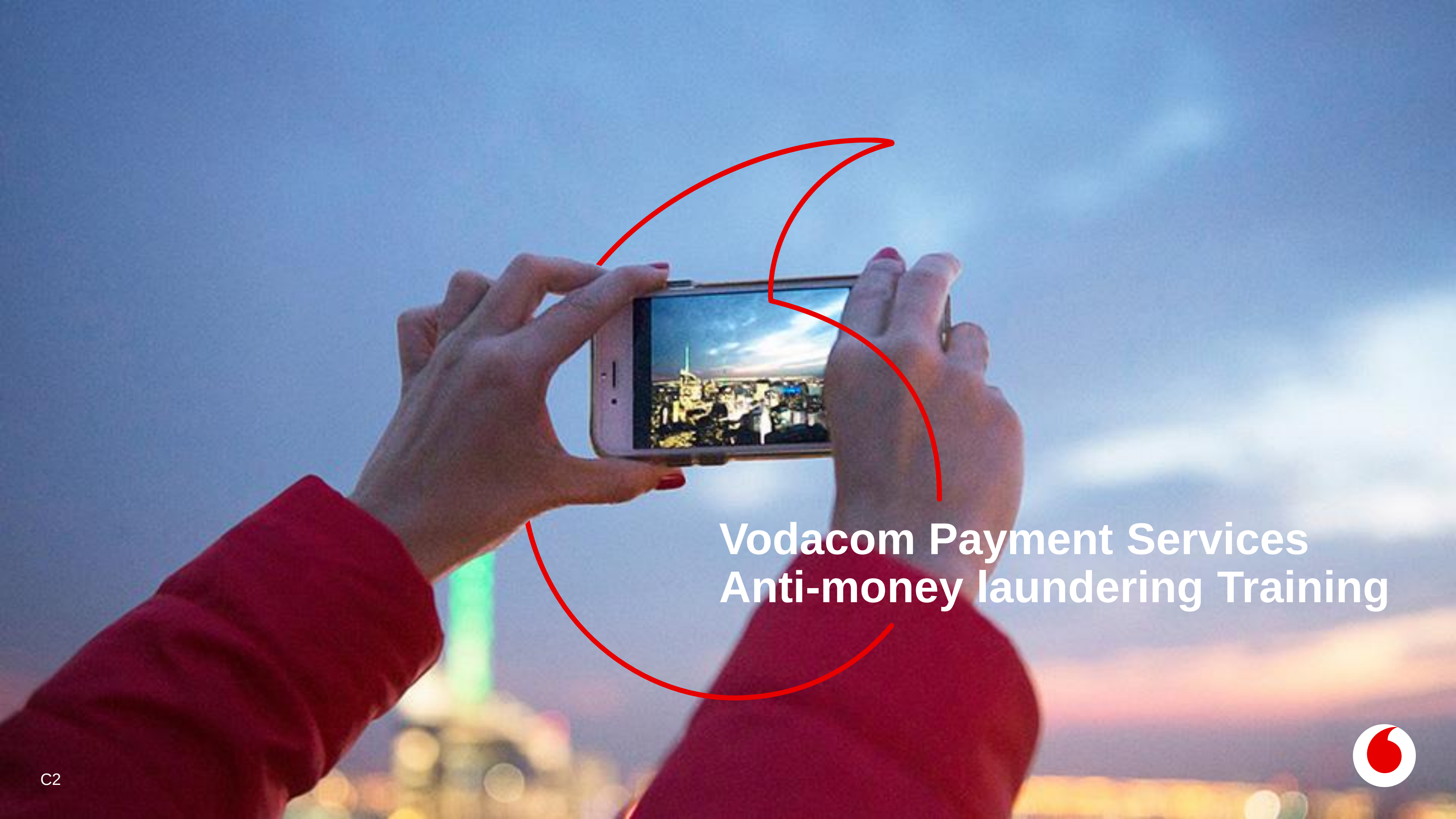

Vodacom Payment Services
Anti-money laundering Training

1

AML in a nutshell

What is money laundering?

Money laundering occurs when **any transaction** takes place **or** any **relationship** is formed that **involves any form of property or benefit** that has come **from any crime**.

The primary objective of the money launderer is to enjoy the benefits of their crimes, without being caught!

Money launderer want to achieve this by:

1. Placing as much distance as possible between themselves and the property
2. Concealing the criminal origin of the property
3. Concealing that they own the property
4. Concealing that they control the property

The three main stages of money laundering

1. Placement

- **What?** Cash from criminal activity is placed into the financial system.
- **How?** Structuring/Smurfing, intermingling, smuggling abroad, asset purchase.
- **Why?** Avoiding detection, easier to handle, quicker to move.

2. Layering

- **What?** Separating the funds from their source by creating complex layers of transactions.
- **How?** Changing form, moving jurisdiction, creating long and incomplete papertrail
- **Why?** To hide the source and ownership of the funds and confuse the authorities and service providers, and make investigations long and complex.

3. Integration

- **What?** Laundered funds re-enter the financial system, appearing to have come from a legitimate source.
- **How?** Inheritance, winnings, investments, insurance policies, sham litigation and deals.
- **Why?** To benefit from the “earnings” and fund future crime.

Terrorist financing

- Terrorist financing is different to money laundering, in that the funds can come from legitimate sources but are used for criminal purposes.

However, they have a number of features and techniques in common:

- The intended purpose and destination is disguised
- The origin is also often disguised in order to maintain funding channels
- Both require interaction with financial services
- Anonymity is sought
- New technologies and services are used


EUROPE, SPECIAL FOR THE WEB

Lessons Learned from the Paris and Brussels Terrorist Attacks

MARCH 29, 2016

Sanctions

- Sanctions are restrictions used by political international communities to achieve a specific foreign policy or national security objective.
- They can be placed on countries, individuals, entities, or activities.
- Sanctions can focus on economic, trade, financial, or travel activity.
- In most jurisdictions it is a regulatory requirement for financial institutions to comply with sanctions controls.
- These businesses need to take appropriate action to comply with international and domestic sanctions and to ensure that they do not perform financial services for those subject to sanctions.

2

Legal and regulatory environment

National frameworks for regulation

Primary legislation

- Financial Intelligence Centre Act – FICA (Anti-money laundering)

Secondary legislation

- Prevention of Organised Crime Act - POCA (Combating racketeering)
- Protection of Constitutional Democracy against Terrorist and Related Activities Act - PROCDATARA (Combating terrorism).

Offences under AML regulation

Primary Offences

There are three broad groups of primary offences related to money laundering that firms need to avoid committing. These are:

- knowingly assisting (in a number of specified ways) in concealing, or entering into arrangements for the acquisition, use, and/or possession of, criminal property;
- failing to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting, that another person is engaged in money laundering; and
- tipping off, or prejudicing an investigation.

Maximum penalty of 15 years imprisonment or maximum penalty of R10, 000,000 or both.

Secondary Offences

It is also a separate offence under the ML regulations not to establish **adequate and appropriate policies and procedures in place to prevent and detect money laundering** (regardless of whether or not money laundering actually takes place).

SA Banks fined more than R200m over the past 5 years

2014 Total: R145 million
Including:
- **ABSA** - fined R10million
- **Standard Bank**- fined R60million
- **Nedbank**- R25million
- **Investec** – fined R20million
- **FNB**-fined R30 million

2016 Total: R43 million
Including:
- **Investec** – fined R20 million
- **Habib** – fined R1 million
- **ABSA**- fined R10million
- **Standard Chartered**- fined R10 million
- **Bank of Athens**-fined R3million

2019 Total: R37.5 million
Including:
- **Standard Bank** – fined R30 million
- **GroBank** – fined R5 million
- **Bank of China**- fined R2million
- **Ubank**-fined R0,5 million

Banks were fined for **secondary offences** which included
- Failure to identify and verify clients
- Failure to adequately train staff
- Failure to adequately screen clients
- Failure to report suspicious transaction & cash threshold breaches

3

Is VPS at risk?

Product vulnerabilities – card acquiring

Products offer the capability to conceal illegal activity

Juristic persons offer an opportunity to conceal the true owner of funds

Perception of an Mobile Network Operators ability to manage the AML risk

Link to the banking system

Third party agents

How do we mitigate the risk?

Know your customer (KYC)

Agent due diligence

Training & comms

Transaction monitoring

Watchlist screening

Reporting suspicious activity

Monitoring AML programme controls

Your responsibilities in AML risk management

Know your customer

(KYC)

- Digital client ID & Verification which verifies information off a golden source.
- Establishing nature of business
- On-site visits and website inspection
- Be vigilant on ID & Verification that can not be verified off a golden source.

Transaction monitoring

- Alerts from transaction monitoring may require
  - Re-establishing nature of business
  - Seeking explanation from clients on transactional activity

Reporting suspicious activity

- Any suspicious activity identified when signing up a client or in the course of the business relationship must be report to the Risk and Compliance team
- Report suspicious activity to lifecompliance@vodacom.co.za

C2