



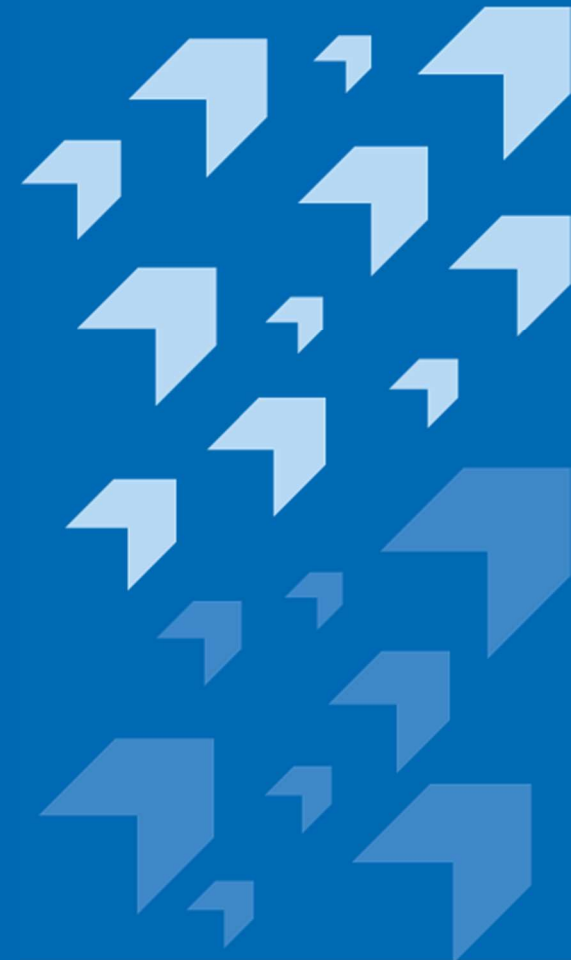
Key Observations of Insurers' AML/CFT Control on Virtual Customer Onboarding

Dickson Chui, Senior Manager

Joseph Lee, Manager

Market Conduct Division

4 December 2020



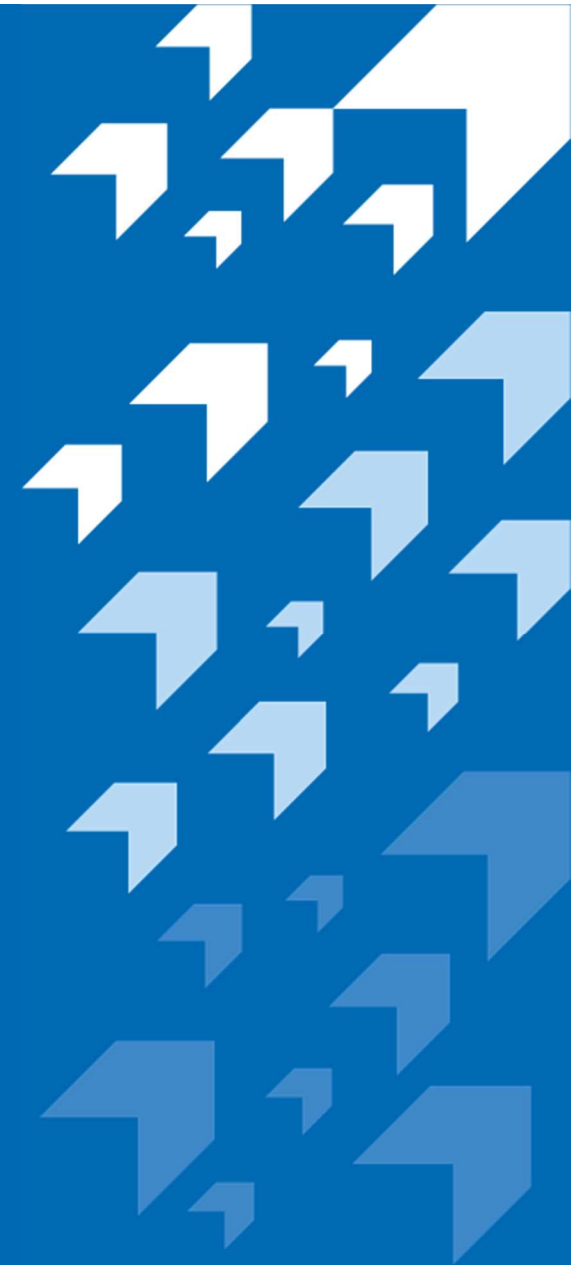


DISCLAIMER

Where the online sharing session aims to enhance the audience's understanding of the topic and refers to certain requirements of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance ("AMLO") and the Guideline on Anti-Money Laundering and Counter-Terrorist Financing ("GL3") published by the Insurance Authority ("IA"), it provides information of a general nature and is not intended to cover all the statutory requirements that are applicable to you and your company. In any circumstances, the information and materials from the sharing session should not be regarded as a substitute of any law, regulations and guidelines. Your company should seek its own professional legal advice in ensuring its compliance with the AMLO, GL3 and fulfillment of relevant regulatory obligations.

The IA reserves the copyright of the presentation for this online sharing session and it may be used for personal viewing purposes or for use within your company. The materials may not be reproduced for or distributed to third parties, or used for commercial purposes without prior written consent from the IA.

Onboarding in a virtual world



Onboarding in a virtual world

Virtual Insurers

- 2 virtual insurers carrying on long term business have been authorized under the Fast Track.



Sandbox

- Sandbox facilitates a pilot run of innovative Insurtech applications.
- Most applications are related to virtual onboarding.

Covid-19

- Difficult to carry out face-to-face meeting.



- Non-Face-to-Face business relationships / transactions are traditionally considered by the Financial Action Task Force (“FATF”) to be higher risk situations.



Favour
anonymity

Key AML/CFT Regulatory Requirements



Key AML/CFT Regulatory Requirements

Anti-Money Laundering and Counter-Terrorist Financing Ordinance (“the AMLO”)

➔ **Section 9 of Schedule 2** to the AMLO stipulates that if a customer has not been physically present for identification purposes, an insurer must carry out **at least one** of the following measures:-



(a) **further verifying the customer’s identity** on the basis of documents, data or information referred to in section 2 of Schedule 2 but not previously used for the purposes of verification of the customer’s identity under that section;



(b) taking **supplementary measures** to verify information relating to the customer that has been obtained by the insurer;



(c) ensuring that the payment or, if there is more than one payment, the **first payment** made in relation to the customer’s account is carried out through an account opened in the **customer’s name** with an **authorized institution**...(or a similar institution in an equivalent jurisdiction)

➔ Why the **additional measure(s)** is/are required in the AMLO?



Impersonation Risk

Key AML/CFT Regulatory Requirements

Guideline on Anti-Money Laundering and Counter-Terrorist Financing (“GL3”)

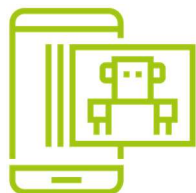
Paragraph 4.12.2

- ▶ the **extent of additional measures** set out in the AMLO will depend on the nature and characteristics of the product or service requested and the **assessed ML/TF risks** presented by the customer.



Paragraph 4.12.3

- ▶ when taking **supplementary measures, e.g. using appropriate technology** to mitigate the risks, an insurer should be able to demonstrate to the Insurance Authority the measures taken can **adequately guard against impersonation risk**.



Key AML/CFT Regulatory Requirements

Guideline on Anti-Money Laundering and Counter-Terrorist Financing (“GL3”)



Paragraph 2.10

- an insurer should identify and assess the ML/TF risks that may arise in relation to:
- (a) the development of new products and new business practices, including **new delivery/distribution mechanisms**; and
- (b) the use of **new or developing technologies** for both new and pre-existing products.

Paragraph 2.11

- an insurer should **undertake the risk assessment prior to the launch** of new products, new business practices, or the use of new or developing technologies, and should **take appropriate measures to manage and mitigate the risks identified**.



Key AML/CFT Regulatory Requirements

IA circular issued on 5 Aug 2020

- Sandbox application for the distribution of long term insurance policies via video conferencing tools.
- Details of the AML/CFT controls required, including:



ML/TF Risk Assessment



The corresponding additional measures

Key AML/CFT Regulatory Requirements

What's more

➤ What impact would have on your AML/CFT system arising from virtual onboarding?

➤ (a) Adherence to same set of AML/CFT policies and procedures regardless of the distribution channels.

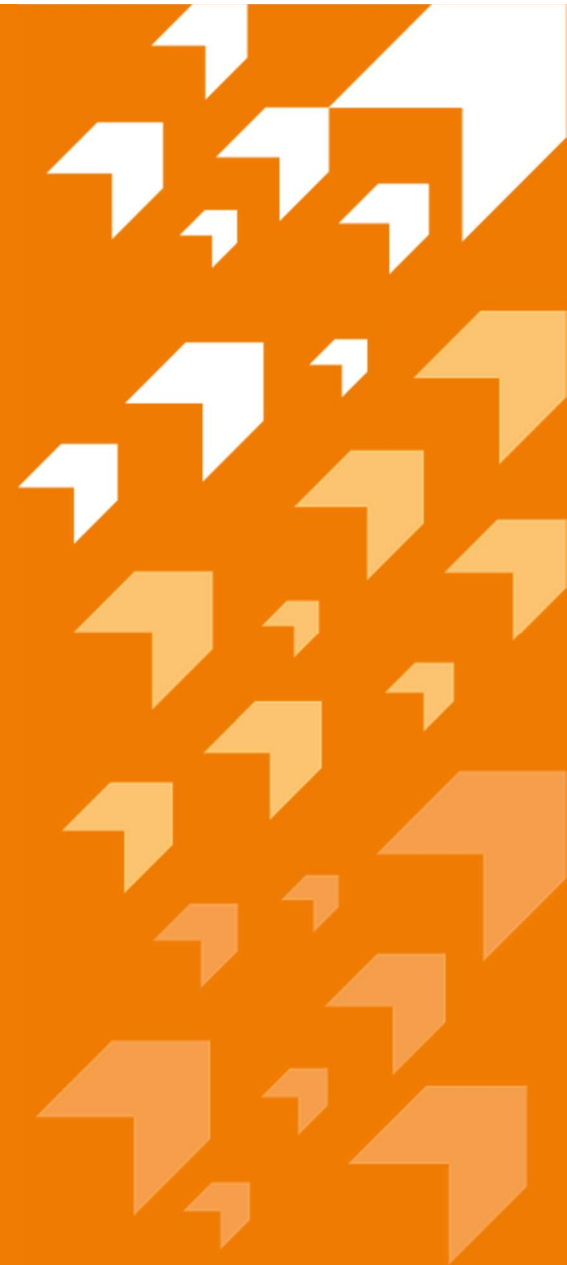


E.g. The KYC information collected during NF2F onboarding should be adequate for AML purpose.

➤ (b) Issues on data integration with policy administration system and/or AML risk profiling system



**Key AML/CFT Considerations
– Expectation, Good Practices
and Alerts**



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

Key AML/CFT considerations

- Risk-based approach
- No one-size-fits-all

What should you be alert to? What is the good practice in the market?

Good Practice Company



1. AML/CFT risk assessment



2. Additional measures for NFTF channel



3. Identity Information



4. Premium collection



5. Transaction monitoring



6. Technology adopted



3. Straight-through process

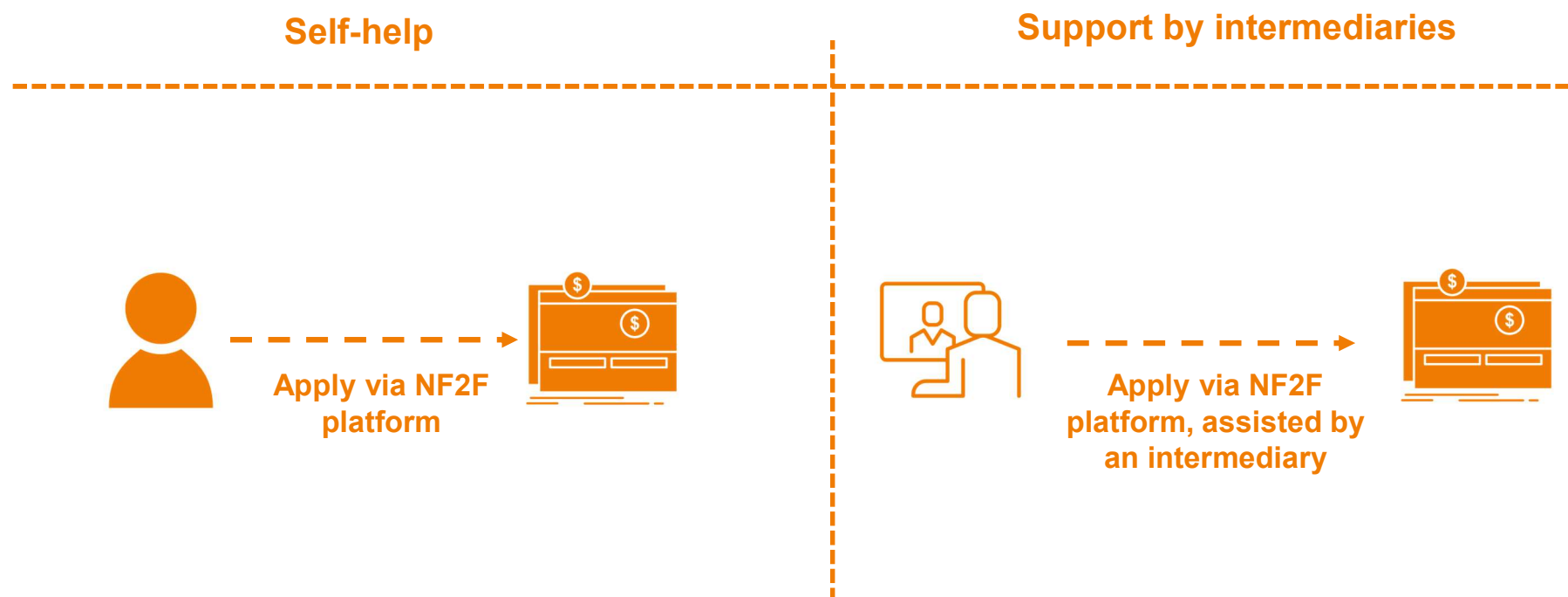


8. CDD performed by an insurance intermediary

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

1. AML/CFT risk assessment

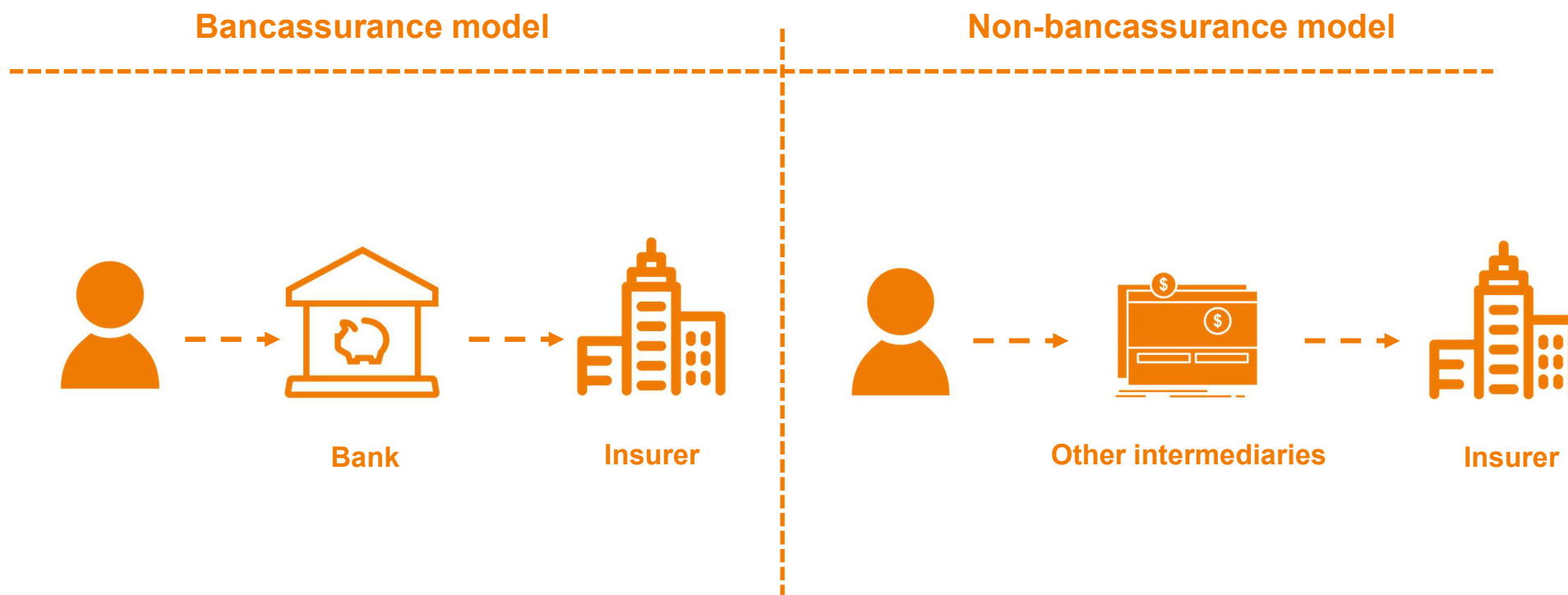
- The online journey can entail different level of risks depending on the **operational models used**.
- Self-help vs support by intermediaries (through video conferencing)



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

1. AML/CFT risk assessment

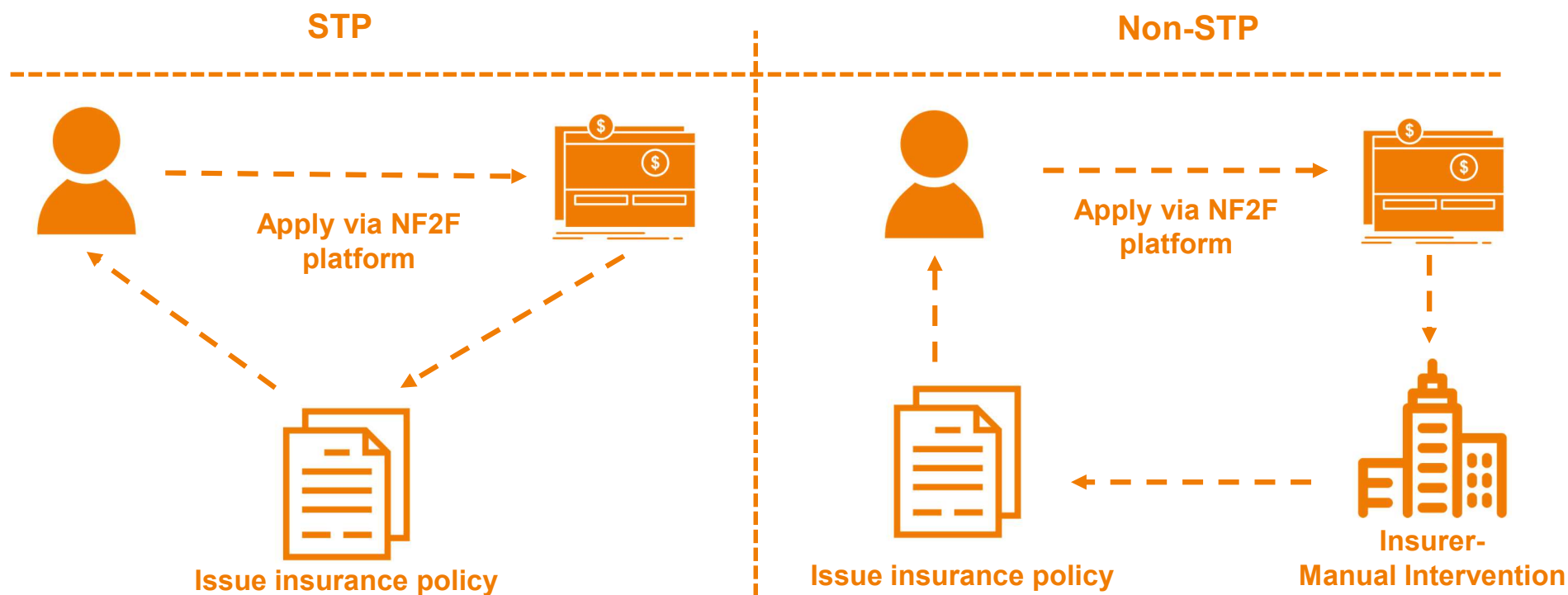
➤ Bancassurance model vs non-bancassurance model



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

1. AML/CFT risk assessment

- Straight-through processing (“STP”) vs non-STP



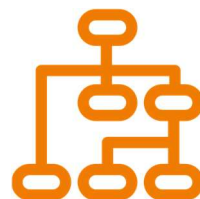
Key AML/CFT Considerations – Expectation, Good Practices and Alerts

1. AML/CFT risk assessment

➤ Customer risk:



Offshore clients



Corporate vehicles/legal structures

➤ Product risk:



unit-linked or with profit single premium contracts



single premium life insurance policies that store cash value



Allowance of **unlimited** top-ups and partial withdrawals



Refundable premium





saving / endowment policies with **no / minimal early surrender penalty**

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

1. AML/CFT risk assessment



Good Practice Company




-  → Good Practice Company conducts a **thorough risk assessment** with respect to each risk factor prior to its launch.
-  → Good Practice Company has **restrictive measures** to mitigate higher ML/TF risks posed by NFTF channel, i.e. the Company restricts its **customer segment** to Hong Kong residents only, has placed a **premium cap** on the products sold online, etc.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

1. AML/CFT risk assessment



Good Practice Company

-  When the premium exceeds certain amount, Good Practice Company requests the customer to visit the Company's office in person **for face-to-face identity verification.**
-  For Customer Risk Assessment purpose, Good Practice Company aggregates premiums amount on a **per policyholder basis**, so that the Company is able to monitor for the premium cap and calculate a risk score on the customer.
-  Good Practice Company considers NFTF customers are having higher ML/TF risk and assigns **higher scores / grades** in risk rating of these customers.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

2. Additional measures for NFTF channel

➤ Some common examples in the market:



To upload **second identity document / passport** for the purpose of verification of the customer's identity;



To take **real-time selfie photo** to match it against the photo in identity card document;



To ensure **initial premium payment** is received from an account in the customer's name with a bank in Hong Kong.

➤ **Extent of additional measures** depends on the nature and characteristics of the product or service requested and the assessed ML/TF risks presented by the customer.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

2. Additional measures for NFTF channel



Good Practice
Company



➤ Good Practice Company has a **combination of additional measures**, which is also commensurate with the ML/TF risks posed by NFTF channel.



Paragraph 4.3.4 of GL3

➤ For the second identity document / passport, it should also contain a **photograph** of the customer.



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

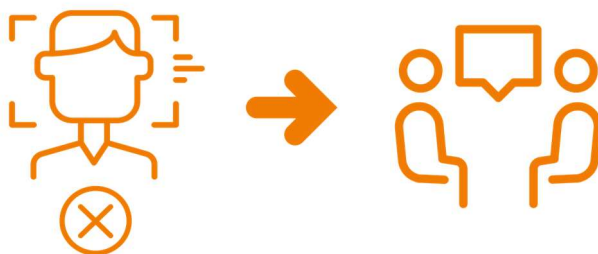
2. Additional measures for NFTF channel



Good Practice Company



➤ If facial recognition using real-time selfie fails or the uploaded identity document is unclear, Good Practice Company requires the customer to visit the Company's office in person for **face-to-face identity verification**.



E.g. Instead of real-time selfie photo, an insurer proposes to allow a customer to upload a photo image for identity matching purpose.

Impersonation risk by photo editing?



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

3. Identity information



- All identification information as required in the GL3 for a natural person customer should be **captured** during the onboarding process.
 - Full Name
 - Date of Birth
 - Nationality
 - Unique identification number and document type
 - Residential address information

- If these information has any connection to **high risk countries/jurisdictions**, enhanced due diligence measures applied should be commensurate with the nature and level of ML/TF risks.
- For an existing customer, appropriate measures are expected to be in place to **authenticate the identity** of such customer.



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

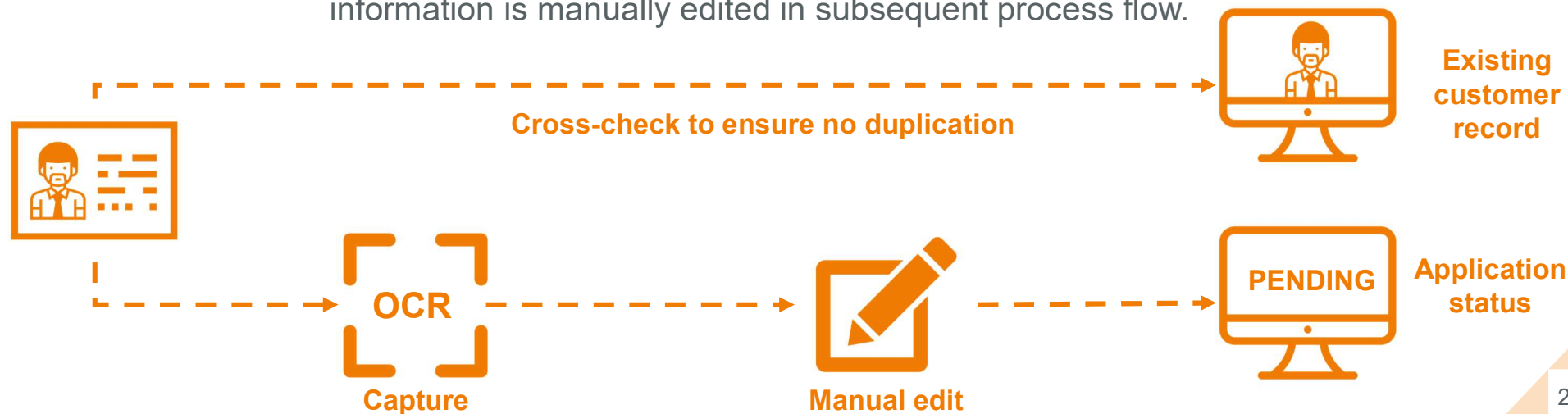
3. Identity information



➤ Good Practice Company checks an individual's identity information against the Company's existing customer records and combines the same customer records into the Company's database, in order to ensure **no duplicate customer profiles** are created.



➤ Identity information is captured by Optical Character Recognition ("OCR"), Good Practice Company puts the application into **pending status** if the information is manually edited in subsequent process flow.



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

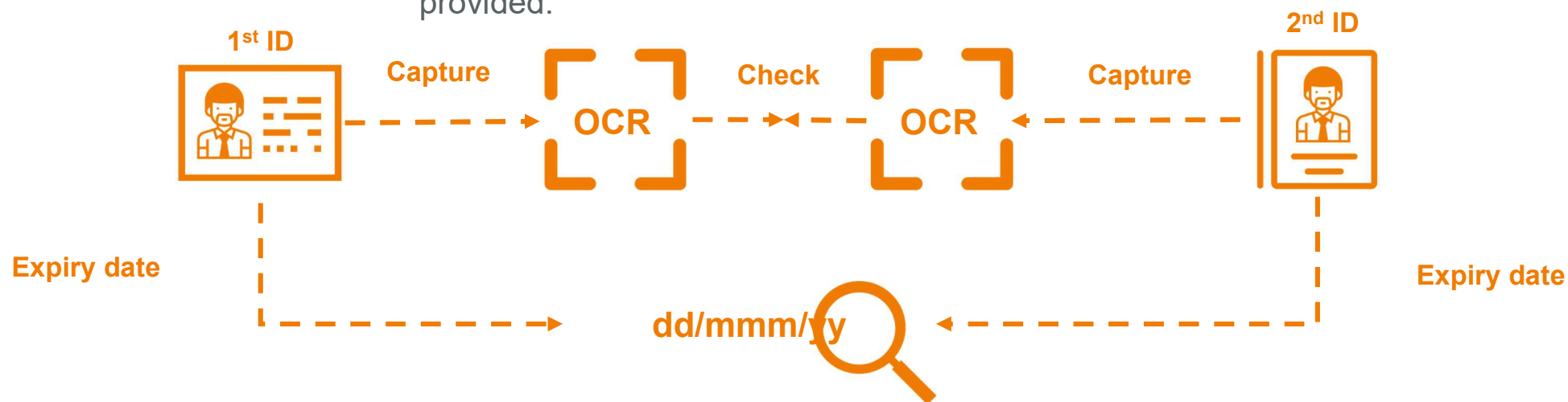
3. Identity information



➤ Good Practice Company applies OCR to capture identity information from a Hong Kong identity card and a second identity document provided by the same customer. Then, it **checks identity information** from the documents obtained against each other.





➤ An automated control is in place to ensure an unexpired passport is provided.





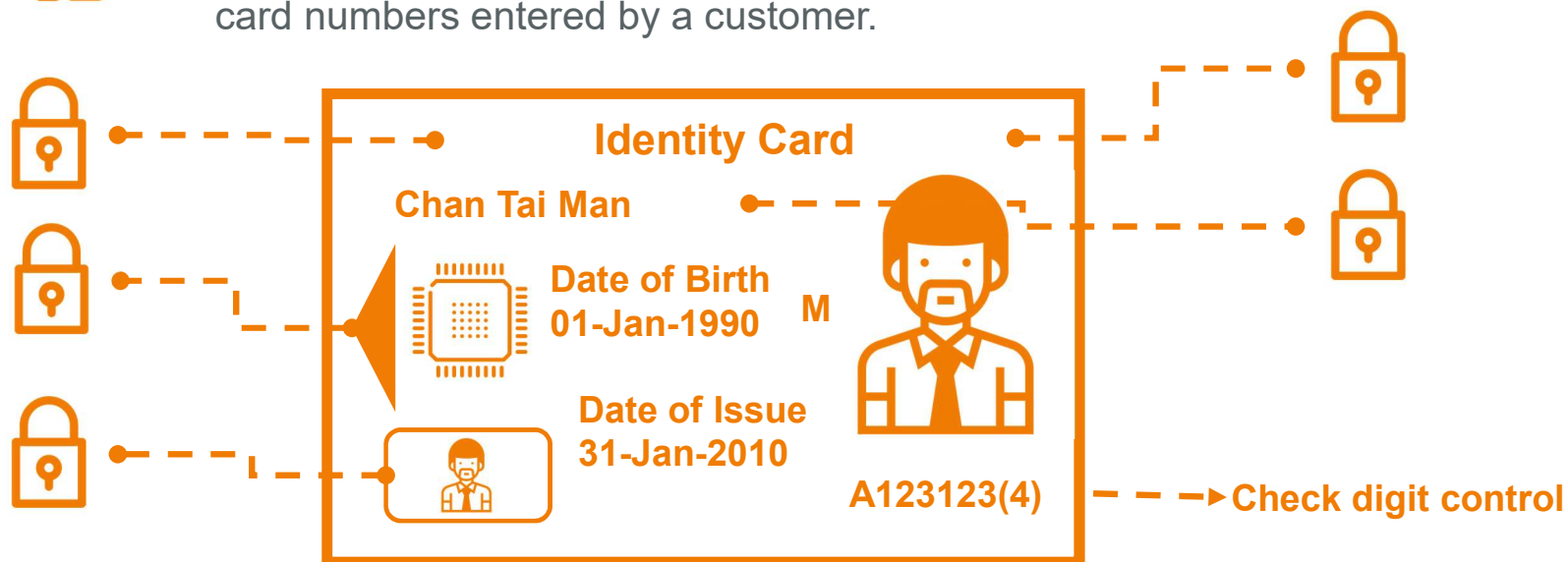
Key AML/CFT Considerations – Expectation, Good Practices and Alerts

3. Identity information



  Good Practice Company applies identity authentication technology to ensure reliability of the identity documents. It means the technology supports **detection of security features** of identity documents.

  Good Practice Company uses **check digit control** for Hong Kong identity card numbers entered by a customer.



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

3. Identity information



- When selecting nationality from a dropdown list, Good Practice Company **removes all high risk and sanctions countries** and does not allow the customer to select from them.



Cannot select high risk countries from dropdown list

Pop up message to show acceptable identity documents



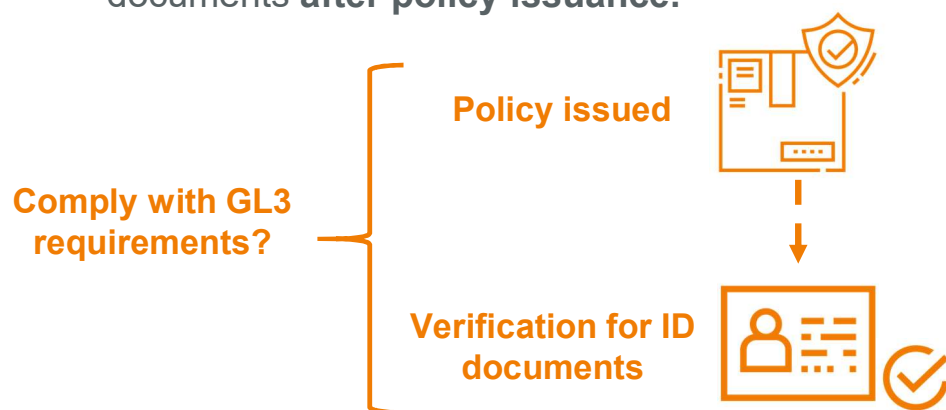
- When requesting for second identity document, Good Practice Company will **pop up a message** to a customer showing the acceptable types of identity documents.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

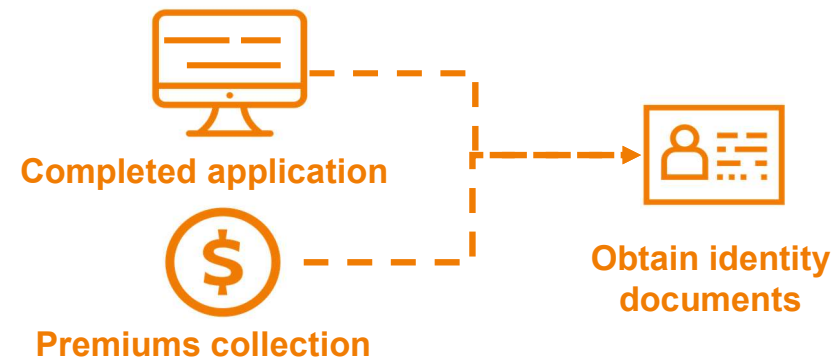
3. Identity information



- Some insurers consider, during the virtual customer onboarding process, the submission of identity documents **interrupts the normal conduct of business**, and request for verification of identity documents **after policy issuance**.



- Some insurers allow a customer's identity document to be obtained **after premium collection or after the entire application process**.



- How about a scenario that the customer intentionally fails to upload the identity document and requests for a premium refund by cancelling the application – higher ML/TF risk?

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

4. Premium collection



- Reasonable control measures should be in place on premium refunds and over-payments.

Max



- If there is a premium **payment cap control (an internal requirement)** on the channel, an insurer is required to have control measures to ensure such requirement will not be circumvented.



3rd party payor

- For the purpose of compliance with paragraph 4.12.1 part C of the GL3, when an insurer imposes an additional measure to ensure first premium payment is received from a bank in the customer's name, then there is **no room** for it to receive initial premiums payments from a third party payor.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

4. Premium collection

- 👍 ➔ Good Practice Company restricts initial premium payments to **limited payment methods**, that can place “name matching” controls effectively to match a payor’s name against the customer’s name.





- 👍 ➔ For credit card payments, Good Practice Company requires a customer to **upload an image of credit card**;
- 👍 ➔ Good Practice Company also only allows the customer to select a bank from a **dropdown list of designated banks**.
- 👍 ➔ In addition, for Faster Payment System (“FPS”) payments, Good Practice Company obtains **payment file(s) from a bank(s)** to check the payor’s name against the customer’s name.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

4. Premium collection



 For bank transfers / deposit slips / unnamed cheques which do not show a payor's name, Good Practice Company requires the customer to provide **bank statement(s) showing the account number and account holder's name.**

 For premium payment above a defined threshold, Good Practice Company requires the customer to provide **additional information of source of funds / source of wealth** and may need to have a face-to-face interview with the customer.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

4. Premium collection



Good Practice
Company



For group life policies, Good Practice Company sends **an insurance licensed staff** to verify that the credit card holder is the corporate customer and obtains an image of the credit card for record-keeping purpose.



Insurance licensed staff



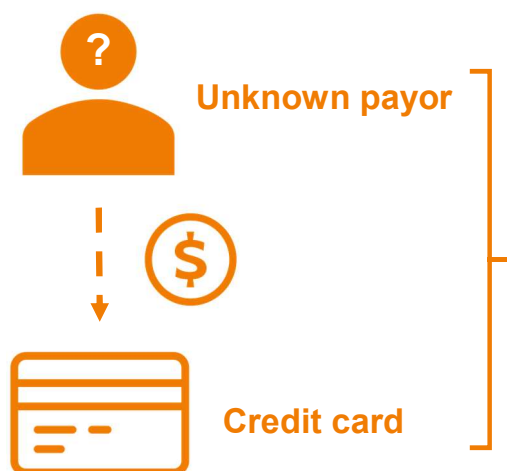
Corporate Customer

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

4. Premium collection



- In some cases, since the payor's name for credit card payments may not be obtained from a bank(s) or customer(s), premium refunds by original channel could favour **anonymous use** of insurance products for ML/TF purpose.



Does an insurer know from whom and to whom the funds are transferred??




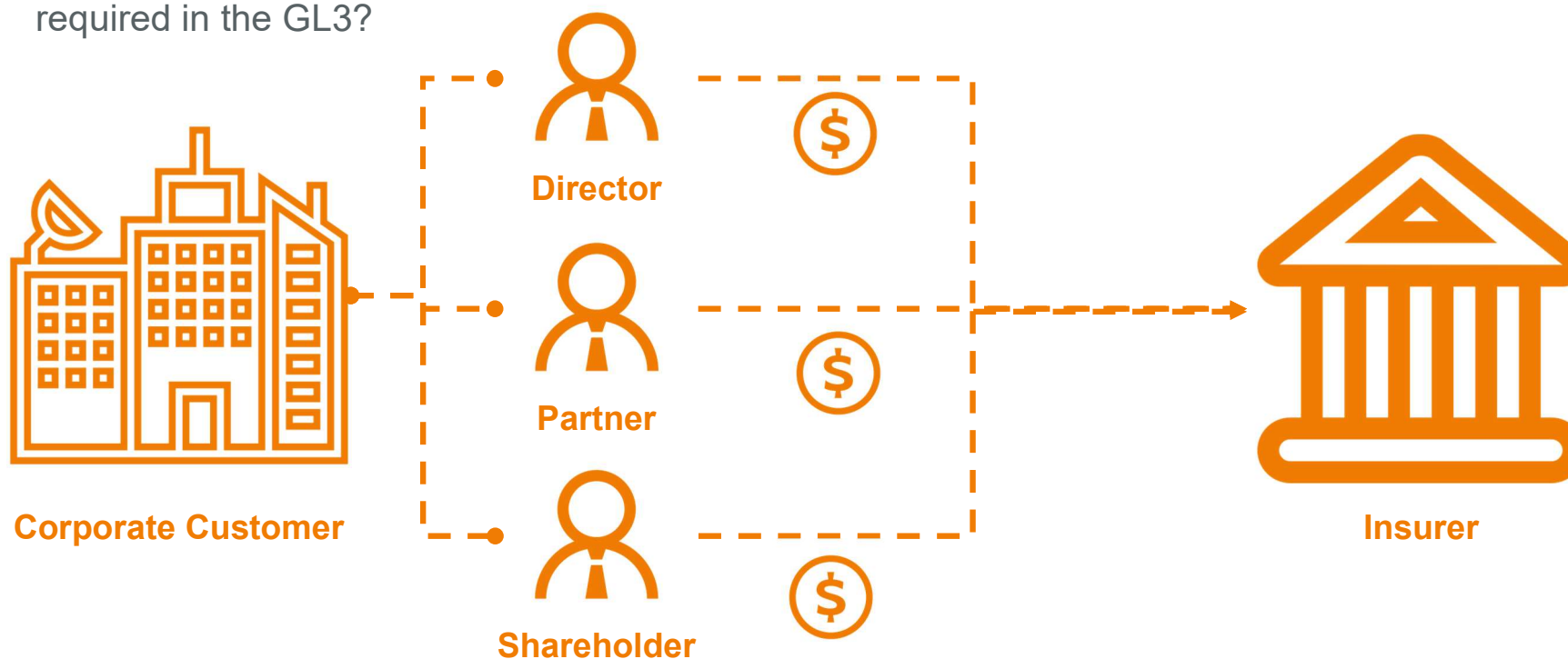
- For third party payments, some insurers solely rely on **self declaration** statement by a customer to understand his relationship with a payor – should it be on a risk-based approach for validation?



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

4. Premium collection

-  For a group life policy, an initial premium is collected from a **director(s) or partner(s) or shareholder(s)** of a corporate customer – does it comply with the additional measures as required in the GL3?



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

5. Transaction monitoring



Good Practice Company



Good Practice Company has implemented transaction monitoring systems **specific to the new business practice** in connection to the customers from virtual onboarding process.



For the **new transaction monitoring reports** with respect to virtual onboarding customers, Good Practice Company monitors regularly transaction patterns for them.

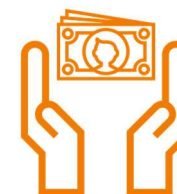
Examples of transaction monitoring reports:



Cross-border payments for offshore customers



Early surrender / cooling-off cases



Premiums refunds volume



Withdrawals frequency and volume



Number of JFIU reported cases

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

6. Technology adopted



Verify the identity of customer

- For a natural person customer, technology may be applied to assist an insurer on the customer's identification and verification. The technology can support:-
 - identity **authentication** - genuineness of the identity document; and
 - identity **matching** – linking a customer to identity document provided by the customer.



Corporate Customer

Verify the identify of PPTA

- For a legal person customer, technology may be applied to facilitate onboarding of the corporate customer, for example, through the verification of the identity of the **person(s) purporting to act on behalf of the customer and the beneficial owner(s)**.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

6. Technology adopted



Good Practice
Company



Subsequent to implementation, Good Practice Company performs **quality checks** to monitor the effectiveness of technology (e.g. OCR and facial recognition) which assists the Company on customer's identification and verification.



Particularly to facial recognition technology, Good Practice Company has set a defined score to gauge the technology; and the Company **calibrates the score** regularly to monitor effectiveness of such technology.



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

7. Straight-through process



- Real time name screening - at the establishment of business relationship with a customer, an insurer should normally finish **identity verification**, determine whether a customer (or beneficial owner of a customer) is a **Politically Exposed Person**; and complete **sanctions screening** on a customer (or beneficial owner of a customer).



- Other customer due diligence measures, or **enhanced due diligence** in case of high risk countries/jurisdictions, high risk occupations and other high risk situations as stipulated in the GL3, should normally be completed at the establishment of business relationship with a customer.



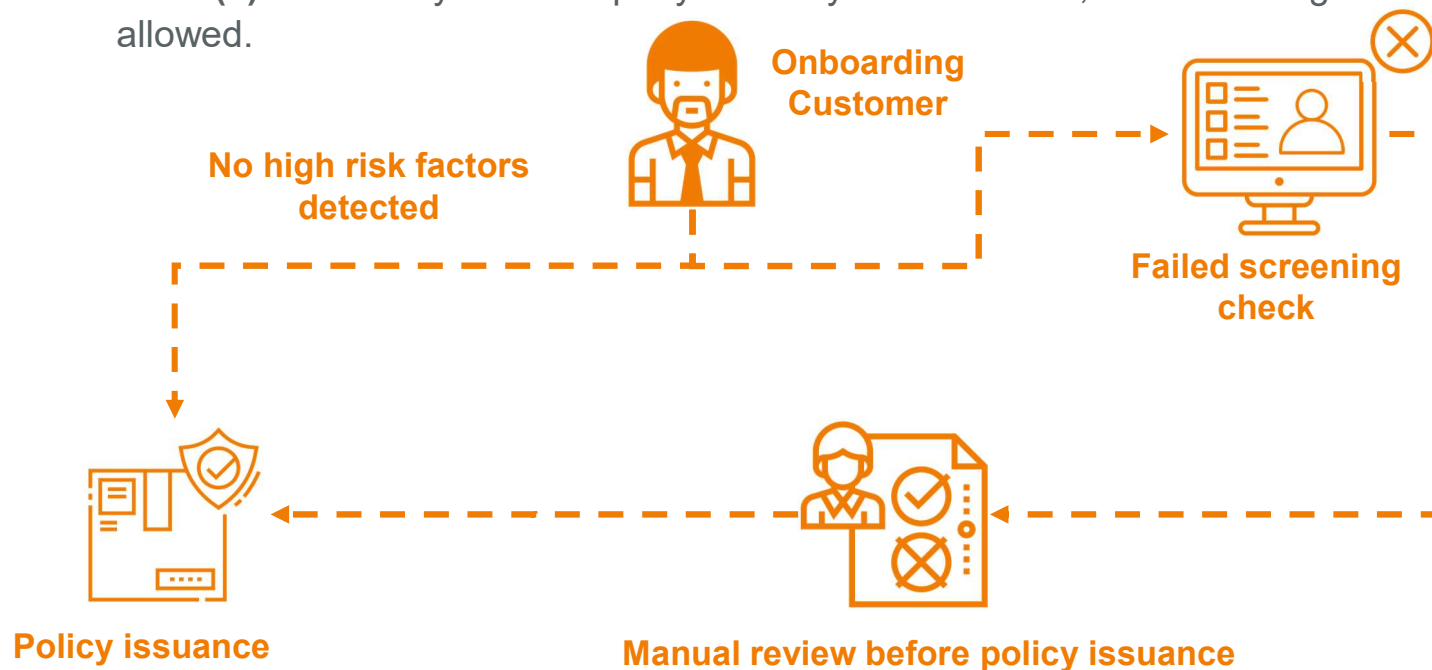
- For Mainland China Visitors, an insurer should embed the **Important Facts Statement** (in Simplified Chinese) into the onboarding process and ensure the customers are able to read and understand the Statement.

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

7. Straight-through process



For applications by straight-through process, Good Practice Company stops the virtual onboarding process when a customer **fails the screening check**, and diverts the customer to manual review when a **high risk factor(s)** is detected or a **trigger event(s)** defined by the Company is hit by the customer, i.e. no “straight-through” is allowed.



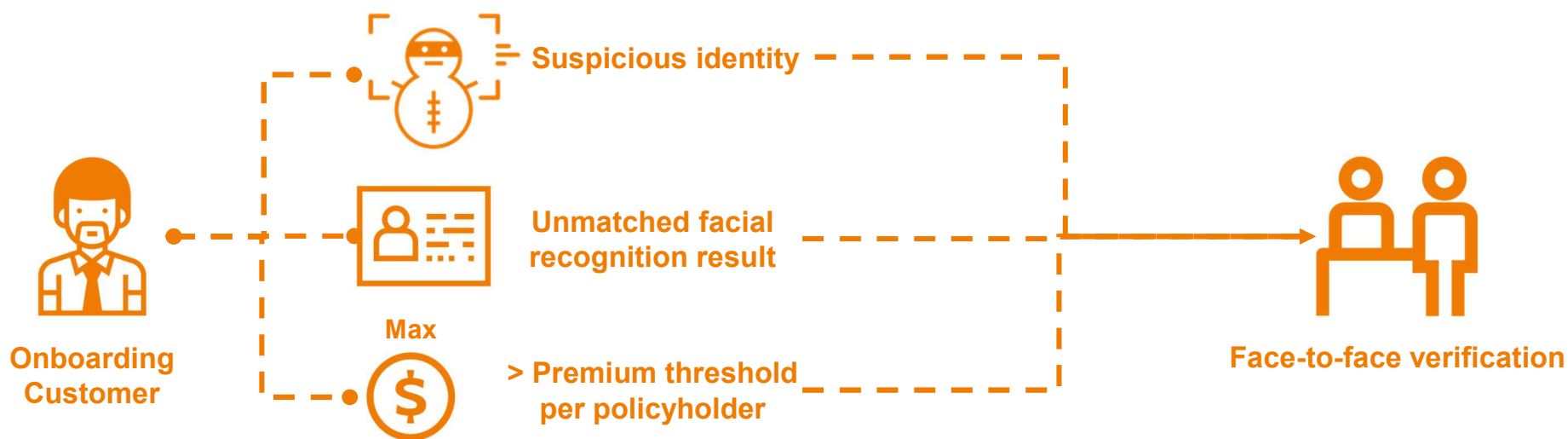
Key AML/CFT Considerations – Expectation, Good Practices and Alerts

7. Straight-through process



Good Practice Company suspends virtual customer onboarding process and requires **face-to-face verification** in case:-

- Suspicious identity or transaction is found;
- Unmatched facial recognition result is found; or
- Aggregated premium on a per policyholder basis exceeds certain amount.



Key AML/CFT Considerations – Expectation, Good Practices and Alerts

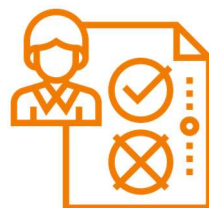
8. Customer due diligence performed by an insurance intermediary



Good Practice Company



For banassurance business, Good Practice Company requires a technical representative of its bank agency to **verify bank account name** of a customer for an initial premium payment before submitting such policy application to the Company.



For video conferencing with a licensed insurance agent, Good Practice Company provides adequate training to the agent with **written training materials**, and the agent is able to guide a customer to complete the onboarding process properly.






Key AML/CFT Considerations – Expectation, Good Practices and Alerts

9. Other Good Practices



Good Practice Company

-  For first personal data amendment and first financial change request (including cooling-off, surrender or withdrawals), Good Practice Company requires a customer to come to the Company's office **in person** for identity verification.
-  For a policy **surrender and withdrawal**, Good Practice Company would only pay it to a customer in the name of policyholder by cheque(s).
-  For **full surrender** application (before maturity), Good Practice Company requires face-to-face identity verification by the Company's staff.



Face-to-face verification



Cheque



Policyholder

Key AML/CFT Considerations – Expectation, Good Practices and Alerts

9. Other Good Practices



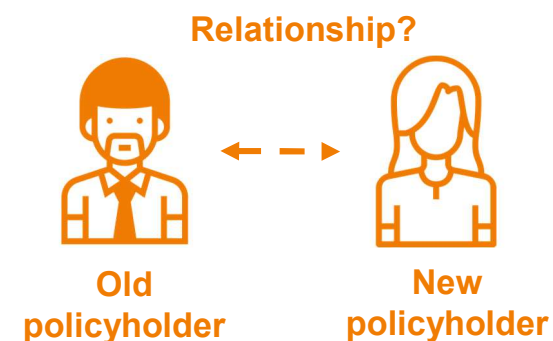
Good Practice
Company



Upon application completed, Good Practice Company calculates risk score of a customer – risk factors include the customer’s occupation, nationality, premium size, payment method, etc. **Enhanced due diligence** will be required for a customer with a score above a defined threshold.



For a change of policy ownership, Good Practice Company applies the same set of due diligence measures as policy inception to the new customer. The Company will ascertain, on a risk-based approach, the **reason of change** of policy ownership and the relationship between the new and original policyholder.



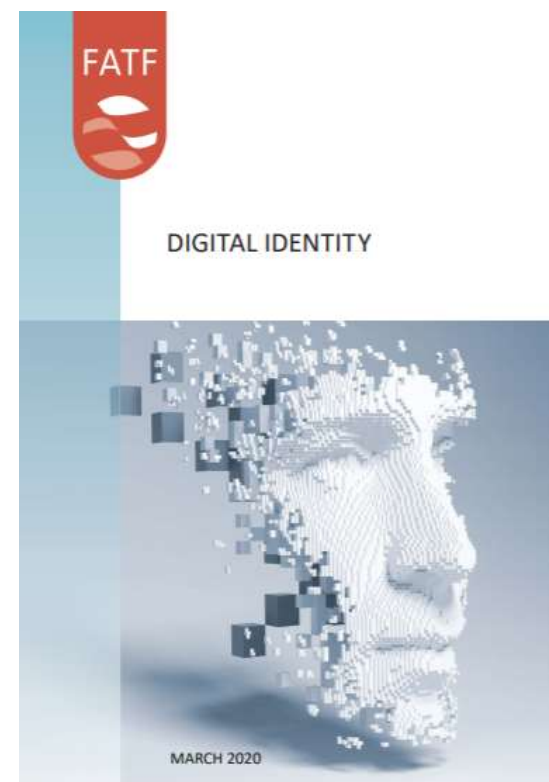
Digital Identity



Digital Identity

Current FATF instance

- In light of recent development in financial technology (“Fintech”), the FATF has **relaxed its regulatory stance** and accepts that reliable and **independent digital identification systems with appropriate risk mitigate measures may help lower the ML/TF risks** of NTF customer identification and transactions.



Digital Identity

Benefits of digital identity

Minimize weakness in human control measures

Improve customer experiences

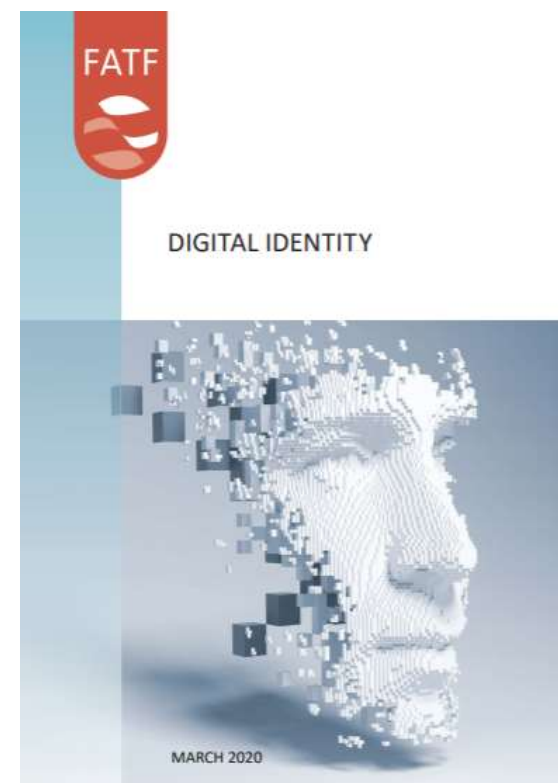


Benefits



Generate cost savings

Others
e.g. financial inclusion



AMLO amendment public consultation

- To add the use of **independent and reliable digital identification systems** for customer identification and verification purposes as a permissible way to satisfy the requirements under section 9 of Schedule 2.



Digital Identity

iAM Smart (formerly known as “eID”)

Key features/ functionalities



Unique electronic identity



Transacting online with the Government and commercial entities



Bound to personal mobile device

3 Functions



Authentication



Form filling



Digital signing

iAM Smart- Pilot Sandbox Programme

- Initiated by Cyberport in collaboration with the Government.
- To facilitate interested organizations of the financial sector to conduct mock-up tests on various functions of the iAM Smart through its Application Programming Interfaces (“API”) provided by the OGCIO.
- Programme will be open until the end of this year tentatively.

Enrolment


Should you be interested to participate in the Programme, please nominate a contact person of your organisation and provide the following information by email to the Insurance Authority mailbox iam_smart@ia.org.hk for registration.

- Name of authorized insurer
- Name of contact person
- Company phone number of contact person
- Company email address of contact person
- Types of applications for which APIs are currently in use (if applicable)






Thank You

 (852) 3899 9983

 www.ia.org.hk

 (852) 3899 9993

 KoiSaiPoKam

 enquiry@ia.org.hk

