Anti-money laundering, combatting the financing of terrorism and counter proliferation financing (AML/CFT/CPF) Guidance Notes

Artificial Intelligence (AI) and Deep Fake Risks for Real Estate Agents & Letting Agents (REAs), Art Market Participants (AMPs) and High Value Good Dealers (HVGDs)

Contents

Disclaimer

The information contained in these guidelines is not intended to be legal advice and is for guidance and information purposes only.

Issued: May 2026
Version: 1.1

Office of Fair Trading • HM Government of Gibraltar • Suite 932b, Europort • Gibraltar GX11 1AA
t (+350) 20071700 f (+350) 20071950 e oft@gibraltar.gov.gi w oft.gov.gi

1. About this document

1.1 Why is the OFT issuing these guidance notes?

The OFT is issuing these Guidance Notes to assist businesses in the real estate, art market, and high-value goods sectors in addressing emerging risks associated with Artificial Intelligence (AI), including deepfake technologies, within their AML/CFT/CPF frameworks.

This guidance is informed by the Financial Action Task Force (FATF) Horizon Scan on AI and Deepfakes, which highlights evolving threats, vulnerabilities and typologies linked to the misuse of AI in financial crime.

Regulated entities are expected to consider these risks as part of their risk-based approach, particularly in relation to customer onboarding, identity verification and transaction monitoring.

1.2 Regulatory Context

Under the FATF Recommendations, jurisdictions are required to ensure that regulated entities:

- Identify and assess risks associated with new and emerging technologies
- Apply Customer Due Diligence (CDD) measures using reliable and independent documentation and data
- Implement appropriate measures to mitigate identified risks

These international standards are reflected in Gibraltar's **Proceeds of Crime Act 2015 (POCA)**, which requires regulated entities to:

- Apply a risk-based approach to AML/CFT/CPF
- Identify and assess risks affecting their business
- Establish and maintain effective policies, procedures and controls
- Conduct appropriate customer due diligence

In this context, risks arising from AI, deepfakes, and synthetic identities should be treated as emerging risk factors within a business' overall AML/CFT/CPF framework.

---

2. Key Risk Findings Relevant to Your Sector

2.1 Nature of AI Enabled Risk

AI is a rapidly developing technology that presents both:

- Opportunities to strengthen AML/CFT/CPF controls, and
- Significant risks when exploited by criminals to circumvent safeguards.

The FATF highlights that AI can be used to bypass existing controls with increasing sophistication.

Key risk typologies include:

- Deepfakes: synthetic video/audio used for impersonation
- Synthetic identities: fabricated or hybrid identity profiles
- AI-generated documentation: false records used to support illicit activity

These developments directly impact CDD, identity verification, and transaction assessment processes.

2.2 Vulnerabilities Relevant to Real Estate Activity

Identity Verification Risk

- Deepfake technology may be used to circumvent biometric and digital identity verification systems.
- Synthetic identities may enable customers to operate under false or manipulated identities

Customer Due Diligence Weaknesses

- AI can generate convincing but false or manipulated:
  - Employment records
  - Contracts
  - Financial documentation
  - These may be used to fabricate source of funds or wealth, supporting money laundering activities during property transactions.
  - Impersonation Risk
- Criminals may impersonate:
  - Buyers or sellers
  - Beneficial owners
  - Legal or professional representatives

This may occur via AI-generated video calls, voice cloning, or messaging, increasing fraud and ML risk.

Remote and Cross-Border Exposure

- Increased reliance on remote onboarding introduces vulnerabilities including:
  - Reduced reliability of digital verification
  - Jurisdictional inconsistencies
  - Limited transparency

These factors increase exposure to identity fraud and misuse of complex structures.

2.3 Art Market Participants

Identity Verification Risk

- Use of synthetic identities or deepfake-enabled impersonation to participate in high-value art transactions
- Difficulty verifying ultimate beneficial owners where intermediaries, agents, or offshore entities are involved

Provenance and Documentation Risk

- Fabricated AI-generated provenance records and ownership histories used to falsely legitimise artworks
- Manipulated certificates of authenticity, valuation reports, or sales documentation

Transaction Structuring Risk

- High-value transactions conducted privately with limited transparency and oversight
- Use of intermediaries or layered ownership structures to obscure beneficial ownership

Valuation Manipulation

- AI tools may be used to fabricate or

influence artwork valuations

• Over- or under-valuation may facilitate the movement and concealment of illicit funds

Cross-Border Exposure

• Frequent cross-border transactions with varying AML/CFT standards

• Reliance on remote negotiation and communication increases impersonation and fraud risk

2.4 High Value Goods Dealers

Identity and Customer Risk

• Synthetic identities used to purchase high-value goods

• Reduced scrutiny in fast-paced or non-face-to-face retail environments

Documentation Risk

• Falsified or AI-generated invoices, receipts, or proof of ownership used to justify source of funds

• False documentation supporting resale, trade, or asset conversion

Transaction Monitoring Limitations

• AI-generated transaction patterns structured to avoid reporting thresholds

• Splitting purchases across multiple dealers or jurisdictions to reduce detectability

Resale and Value Transfer Risk

• High-value goods (e.g. luxury items, vehicles, jewellery) used as portable stores of value

• AI-assisted laundering through rapid resale, asset flipping, or cross-border movement

Reduced Transparency

• Cash-intensive transactions or use of intermediaries

• Limited audit trails compared to financial institutions, reducing traceability

3. Expectations for Regulated Entities

Regulated entities are required, under the **Proceeds of Crime Act 2015**, to apply a risk-based approach and ensure that their AML/CFT/CPF frameworks adequately address risks relevant to their business.

This includes consideration of emerging risks associated with AI and deepfake technologies.

3.1 Business-Wide Risk Assessments

Regulated entities should:

- Identify and assess AI-related risks within their business including exposure arising from:
    - Remote onboarding
    - Digital verification tools
    - Cross-border clients and transactions

- Document how these risks are understood and mitigated

3.2 Customer Risk Assessment

Customer risk profiling should incorporate:

- Whether the relationship is conducted **non-face-to-face**
- Any inconsistencies in:
    - Identity information
    - Supporting documentation
    - Behaviour or communication patterns
- Indicators suggesting impersonation or synthetic identity use

3.3 Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

Regulated entities should ensure that CDD measures are sufficiently robust to mitigate AI-enabled risks.

Where higher risks are identified, regulated entities should apply enhanced due diligence, including:

- Independent verification of identity and documentation
- Additional checks on source of funds and wealth
- Verification across multiple channels

This reflects FATF expectations that CDD systems must remain effective against evolving threats.

3.4 Systems and Controls

Regulated entities should implement multi-layered verification frameworks, including:

- Combining digital tools with manual review
- Applying:
    - Multi-factor authentication
    - Liveness detection
    - Behavioural and anomaly monitoring

Human oversight remains critical, particularly where advanced manipulation techniques are used.

3.5 Training and Awareness

Regulated entities should ensure that staff:

- Are trained on AI-related financial crime risks
- Can recognise indicators of:
    - Deepfake use
    - Digital impersonation
    - Document manipulation

Understand escalation procedures

3.6 Ongoing Monitoring and Review

Regulated entities should:

- Monitor developments in AI-related risks and typologies
- Update policies, procedures and controls as appropriate
- Maintain clear records demonstrating how risks are assessed and managed.

3.7 Measures to Mitigate Deepfake and AI-Enabled Risk

In addition to the measures outlined above, regulated entities may consider the following non-exhaustive measures to mitigate risks posed by AI technologies, including deepfakes:

- Strengthen identity verification processes, including enhanced or multi-step verification methods where appropriate (e.g. liveness checks);
- Enhance CDD controls to identify inconsistencies in customer information, documentation, or communications, particularly in remote onboarding;
- Ensure staff are adequately trained to recognise indicators of AI-enabled risks and understand how to respond;
- Ensure appropriate safeguards are in place to protect systems and customer data;
- Consider whether existing monitoring systems remain effective in identifying unusual or automated activity.

3.8 Practical Indicators and Good Practice

Regulated entities should remain alert to:

- Video or audio interactions that appear:
    - Artificial or inconsistent
    - Lacking natural behavioural cues
- Documentation that:
    - Appears overly consistent or generated
    - Cannot be independently verified
- Behavioural indicators including:
    - Urgency or pressure to complete transactions
    - Inconsistencies between customer profile and activity
- Technical anomalies, such as:
    - Mismatch between location data and stated residence
    - Reuse of devices across multiple identities

These indicators align with FATF observations on behavioural and transactional anomalies linked to AI-enabled fraud.

Regulated Entities are encouraged to:

- Apply multi-layered verification processes
- Avoid reliance on a single digital identification method
- Conduct independent verification using trusted sources
- Maintain robust escalation and reporting procedures

Regulated entities should also promote cooperation with:

- Financial institutions
- Legal professionals

Competent authorities

3.9 Use of Artificial Intelligence by Regulated Entities

Regulated entities may decide to adopt Artificial Intelligence (AI) tools to support

business operations, including customer due diligence, transaction monitoring, and document analysis.

While AI may enhance efficiency, it may also introduce additional risks which should be appropriately managed.

Regulated entities should consider the following:

Limitations of AI Outputs

- AI tools may produce inaccurate, incomplete or misleading outputs
- Outputs should not be relied upon without appropriate human review
- AI-generated information should not replace independent verification

Data Protection and Confidentiality

- Caution should be exercised when inputting:
    - Personal data
    - Customer information
    - Commercially sensitive data
- Use of third-party AI tools may result in data being stored or reused the entity's control
- Appropriate safeguards should be in place to protect data

Over-Reliance on AI

- AI should support, not replace, human judgement
- Excessive reliance may reduce professional scepticism
- Higher-risk decisions should remain subject to human oversight

Model and Bias Risk

- AI systems may produce biased or inconsistent outputs
- Businesses should consider whether AI use may impact customer risk assessments

Governance and Controls
Regulated entities should:

- Define how AI is used within the business
- Implement policies governing acceptable use
- Ensure staff understand AI risks and limitations
- Maintain appropriate oversight of AI-assisted processes
- Periodically review effectiveness of AI tools

The adoption of AI should be accompanied by a clear understanding of its limitations and associated risks. Regulated entities should ensure that any use of AI remains aligned with their overall risk management framework and does not compromise the effectiveness of AML/CFT/CPF controls.

4. Useful Contacts

4.1 Office of Fair Trading

The Office of Fair Trading (OFT) has been appointed as a supervisory authority under the Proceeds of Crime Act 2015. Additionally, it is responsible for business licensing and for consumer protection in Gibraltar.

Suite 932b Europort, Gibraltar

Tel: (+350) 20071700

aml.oft@gibraltar.gov.gi

www.oft.gov.gi

4.2 Gibraltar Financial Intelligence Unit

The Gibraltar Financial Intelligence Unit (GFIU) receives, analyses and disseminates financial intelligence gathered from Suspicious Activity Reports.

Suite 832, Europort, Gibraltar

Tel: (+350) 20070211

Fax: (+350) 20070233

gfiu@gcid.gov.gi

www.gfiu.gov.gi