NEXT HORIZONS
FINANCIAL CRIME & COMPLIANCE CONSULTANCY

SAMPLE — FICTIONAL DATA

INDEPENDENT AML/CFT FILE REVIEW · ILLUSTRATIVE SAMPLE DELIVERABLE

High-Risk Player File Review — Sample Findings Extract

Sample findings extract · Fictional data · Illustrates methodology and deliverable format

DOCUMENT CONTROL

Document status	Illustrative sample
Data classification	Fictional data only
Version	1.0
Issue date	August 2026
Prepared by	Rainier van Dam, CAMS — Founder & Principal Consultant
Intended audience	MLRO / Head of Compliance

This document shows how Next Horizons reports an independent high-risk player file review. It is not based on a real client case. All players, accounts, transactions and findings are fictional and do not relate to any real operator, player or regulatory matter.

01 HOW TO READ THIS DOCUMENT

How to read this document

This sample shows how Next Horizons reviews and reports on a high-risk player file. It uses one fictional file to show the findings at player level and how recurring issues are reported across a wider set of files. Each finding sets out what was available in the file, what the review identified and what action is recommended.

INDEPENDENT ASSESSMENT — SCOPE AND RESPONSIBILITY

This is an independent QA review and not legal advice. It does not decide whether an internal report or suspicious transaction report should be filed. Those decisions remain with the operator and its MLRO.

This is a shortened extract. A full ten-file review would also include the complete evidence schedule and supporting analysis.

REVIEW APPROACH

The review is based on the information available when the operator made its decision. Documents obtained later are noted separately, as they do not change what was considered or recorded at the time.

ASSESSMENT DIMENSIONS

AML/CFT review dimensions

- Customer-risk assessment
- CDD completeness and currency
- Source-of-funds and source-of-wealth evidencing
- Ownership and use of payment instruments
- Third-party funding
- Linked and associated accounts
- Ongoing monitoring
- Unusual-activity review
- Internal escalation quality
- Record-keeping and audit trail

Contextual indicators — considered where relevant

- Affordability information
- Responsible-gaming interactions
- Occupation and declared income
- Transaction velocity
- Withdrawals and recycled winnings
- Other information affecting the plausibility of the player's financial profile

The review takes account of the FIAU Implementing Procedures, including Part I and the guidance for remote gaming in Part II. The operator's licence conditions and internal procedures are also considered.

SEVERITY LEGEND

CRITICAL	An immediate and material control failure that requires urgent action or escalation to senior management.
HIGH	A significant weakness that may affect the reliability of the risk assessment or the outcome of the control.
MEDIUM	A gap in the control or supporting evidence that should be corrected, but does not on its own indicate an immediate material failure.
OBSERVATION	An area that could be improved but is not currently considered a material control weakness.

02 FICTIONAL CASE PROFILE

Case profile — Player A

FICTIONAL CASE

PLAYER PROFILE — AS RECORDED ON FILE

OCCUPATION
Office manager

DECLARED ANNUAL EMPLOYMENT INCOME
€38,000

REVIEW CLASSIFICATION
High-risk player

REVIEW PERIOD
Five months (Months 1–5)

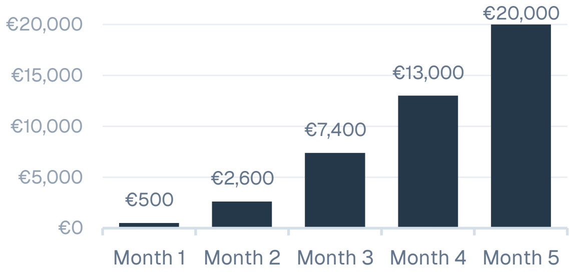
SOURCE-OF-FUNDS EVIDENCE ON FILE
Payslips; unsupported claim of cryptocurrency gains

PAYMENT CONCERN
Two deposits made using cards not held in the player's name

LINKAGE INDICATOR
Shared device fingerprint with a second player account ("Account B")

TRANSACTION PATTERN

External deposits by month, excluding recycled winnings



SUMMARY — REVIEW PERIOD

Total external deposits	**€43,500**
Total withdrawals	**€9,200**
Net deposited amount	**€34,300**
Payment instruments used	**6**
Third-party payment instruments identified	**2**

Mix — 4 cards · 1 e-wallet · 1 bank transfer; both third-party instruments are payment cards.

EVIDENCE INVENTORY

Evidence reviewed

E01 Identity and verification record
E02 Payslips covering three months
E03 Deposit and withdrawal ledger
E04 Payment-instrument data
E05 Device and session data
E06 Contact and CRM notes

Evidence absent

- Cryptocurrency exchange statements
- Wallet transaction history
- Acquisition and disposal records
- Bank entries consistent with claimed gains
- Ownership verification for the two third-party cards
- Documented linkage assessment for Account B

Assumptions requiring validation

- Declared income remains current
- Recycled winnings are correctly classified in operator data
- The device match reflects shared control rather than coincidental shared use

Deposits are reviewed alongside withdrawals, recycled winnings and the financial profile supported by the documents on file. Gross deposits alone do not prove that the activity is unaffordable or illicit.

03 DETAILED FINDINGS

Detailed findings — Player A

FINDING 01 Source-of-funds and source-of-wealth evidencing

HIGH

Assessment area — Source of funds · Source of wealth · CDD evidencing

Evidence — E02 Payslips · E03 Ledger

CONDITION IDENTIFIED

The player declared annual employment income of €38,000, while external deposits increased to €20,000 in Month 5. The file refers to cryptocurrency gains, but no exchange statements, wallet history, purchase or sale records, or matching bank entries were available.

WHY THIS MATTERS — REVIEWER'S ASSESSMENT

The issue is not whether the player receives a salary, but whether the file explains the additional money used for the deposits. The payslips support the declared employment income, but not the level or rapid increase of the external deposits. Without cryptocurrency transaction records or matching bank entries, the explanation provided for the additional funds cannot be verified.

RECOMMENDED ACTION

Request records showing where the cryptocurrency came from, that it belonged to the player and how it was converted into funds. Until this has been clarified, consider appropriate deposit restrictions and review the player's risk classification.

FINDING 02 Third-party payment instruments

HIGH

Assessment area — Payment-instrument ownership · Third-party funding

Evidence — E03 Ledger · E04 Instruments

CONDITION IDENTIFIED

Two deposits were made with cards in someone else's name. The file does not show who owned the cards, what the relationship was, why the cards were accepted or whether the matter was escalated.

WHY THIS MATTERS — REVIEWER'S ASSESSMENT

Cards in another person's name may indicate that a third party is funding or using the account. Because the ownership and relationship were not checked, the file does not show that the risk was properly considered and accepted at the time.

RECOMMENDED ACTION

Stop further use of the cards until ownership has been confirmed. Review the related transactions and any connected accounts, record the relationship and reason for the payments, and decide whether escalation is required under the operator's procedures.

FINDING 03 Linked-account assessment

MEDIUM

Assessment area — Linked and associated accounts · Ongoing monitoring

Evidence — E03 Ledger · E05 Device data

CONDITION IDENTIFIED

The player and Account B share the same device fingerprint. The file contains no assessment of this link, and the activity and financial exposure on both accounts have not been considered together.

WHY THIS MATTERS — REVIEWER'S ASSESSMENT

A shared device does not by itself prove that the accounts are controlled by the same person, but the link should be investigated. By reviewing the accounts separately, combined deposits, funding sources and other risk indicators may be missed. Without a documented assessment, the operator cannot show that the link and the total exposure were properly considered.

RECOMMENDED ACTION

Review and document the link between the accounts. Establish whether they are controlled or funded by the same person, consider the combined risk indicators and financial exposure, and decide whether further monitoring or escalation is needed.

04 QA SCORECARD AND CONTROL THEMES

QA scorecard and cross-file control themes

PLAYER A — QA SCORECARD

0 = Absent or ineffective · 1 = Partially evidenced · 2 = Adequately evidenced

Customer-risk assessment	1	Risk rating assigned; drivers not refreshed after deposit escalation
Identity and CDD currency	2	Identity verified; CDD records current at review date
Source-of-funds evidence	0	Cryptocurrency claim unsupported by transactional evidence
Source-of-wealth assessment	0	No documented source-of-wealth assessment on file
Payment instruments and third-party funding	0	Third-party cards accepted; no ownership checks or rationale recorded
Linked-account assessment	1	Device link flagged by systems; assessment not performed
Ongoing monitoring	1	Alerts generated; dispositions not consistently documented
Escalation and record-keeping	1	Partial audit trail; no escalation recorded for key events

Score 6 of 16 — not passed · pass mark: 13 of 16 points (80%)

NOT PASSED

A file does not pass while a Critical or High finding remains unresolved, even where the numerical score is above the threshold. The 80% threshold is a Next Horizons benchmark used for this sample and is not a regulatory requirement.

Cross-file control themes — fictional ten-file review population

The ten fictional files were selected because they showed higher-risk indicators, including increased deposits, possible third-party funding, linked-account alerts and unsupported source-of-funds explanations. This is a risk-based sample and is not intended to be statistically representative. The results below cover all ten files. Player A is included in the source-of-funds, third-party funding and linked-account findings.

Source-of-funds evidencing standard
Similar gaps in the supporting evidence were found in several files.
RECURRING ACROSS FILES

Source-of-wealth assessment
Missing from several files; the reason should be confirmed with the operator.
REQUIRES CONTROL VALIDATION

Third-party funding controls
Instruments accepted without documented checks in more than one file.
RECURRING ACROSS FILES

Record-keeping
Limited to individual files; no wider pattern identified.
ISOLATED

When the same issue appears in several files, it may point to a wider control weakness. That conclusion should only be drawn after reviewing the underlying process and how the control works in practice.

05 FULL REVIEW AND NEXT STEPS

What is included in a full review

This extract shows one fictional file and a short summary of the themes found across the wider sample. A full ten-file review includes:

- Individual file-level findings with written rationale
- Evidence gaps and required follow-up
- Cross-file control themes
- QA scorecard
- Management findings memo
- Prioritised remediation actions
- Management read-out
- Management action tracker and optional remediation roadmap

01 FIXED FEE · FIVE BUSINESS DAYS

10-File High-Risk Player Review

The review is completed on site at your Malta office within five business days of receiving the complete file set.
Travel and accommodation are agreed in advance at a capped cost and invoiced separately.
Short-notice on-site support is available in Malta. As a Dutch/EU national, no Maltese work permit is required. Current availability is shown on nexthorizonsglobal.com/malta.

Discuss a high-risk file review

€3,500

fixed fee · on-site in Malta

Includes a management read-out.
Scope: one operator and one legal entity; ten pre-selected files.

CONTACT

Rainier van Dam

Founder & Principal Consultant

rainier@nexthorizonsglobal.com
linkedin.com/in/rainier-van-dam
nexthorizonsglobal.com/malta

The review can be contracted through Next Horizons in the UAE or R.D. van Dam Services in the Netherlands, depending on what is agreed.

Response within one business day.

To discuss a review of your high-risk player files, contact Next Horizons through nexthorizonsglobal.com/malta.