Full Coverage Engagement: specimen risk-assessment extract

This specimen continues the findings letter: the same fictional firm, Mittenda Limited, the same finding, one stage on. It is an extract of a single risk's assessment record, in the form the engagement produces it. Everything is synthetic, derived from scenarios seen in practice; nothing was observed in operation; only the OpusDatum Risk register it draws on is real.

Risk reference	R-ORIGINATOR-INFO-VERIFICATION-FAILED; published in full in the register extract.
Designation	‘Strict’, one of the 23: no risk appetite can absorb it.
Risk owner	Head of Financial Crime, Mittenda.
Record stage	Risk assessment complete; treatment plan proposed.
Record control	Assessed 26 March 2026 · revision 1 · approved: the Board, 14 May 2026 · next review: annual, or on material change.

Scope, context and criteria

Scope	The governing tier from stage one: Financial Crime Framework v1.2; AML/CTF Policy v4.2; Risk Appetite Statement v2.0; Customer Due Diligence Standard v2.0; Transaction Monitoring Standard v2.3; Sanctions Screening Standard v5.3; Transfers of Funds and Crypto-Assets Standard v3.2; Record Retention Policy v1.4. Plus the operational tier this risk points to: Payments Operations Procedure v3.1; Crypto-Asset Transfer Operations Procedure v1.7; Payment Platforms Design Note v2.1.
Context	The business-wide financial crime risk assessment (v3.0, 2025 cycle), published in excerpt with the document suite: customers are consumers and small businesses, resident in Ireland and other Member States, onboarded and served app-only, non-face-to-face throughout; joint accounts among them; both rails run, with the crypto-asset rail in its first full year; the assessment rates products and delivery channels medium-high, with electronic verification at onboarding as the assessed mitigation.
Criteria	Mittenda's Risk Appetite Statement §5.1: no appetite for breach of the obligations that admit no risk-based application, met for every customer and every transaction without exception. The Statement never enumerates that class; the register's designations supply the enumeration, and ‘strict’ names exactly that class. Acceptance is unavailable on the firm's own criterion.

Risk identification

Source	Stage one, finding A: Not evidenced against Articles 4(1), 4(4) and 4(6) / 14(1), 14(6) and 14(8). The register's verification risk, quoted in the findings letter.
The risk	The accuracy of the accompanying originator information is never validly established. The Policy verifies the customer; the Transfers Standard enumerates the fields and, at §3.5, rests their verification on the Article 4(5) / 14(7) deeming; no governing document joins the dispatched fields to the verified record.

Risk analysis

Sources. Payments Operations Procedure §11.4: *“Populate the originator name, address and account fields from the customer account record in Garnet. Do not key them by hand.”* The Crypto-Asset Transfer Operations Procedure §7.2 mirrors it on the other rail; §11.6 defaults joint accounts to the primary holder. Two platform facts, from the Payment Platforms Design Note: the account display label is customer-maintained in-app, one feature row among six in the account data model (§3.2); and the firm's own reconciliation schedule (§6.2) lists seven reconciliations, none joining the customer due diligence record to the dispatched fields. On evidence age: the Customer Due Diligence Standard §7 sets the periodic review cycle by customer risk rating and resets it on a change of identity information, and the AML/CTF Policy §6.3 requires verification to be refreshed on such a change; the Transfers Standard §3.5 grounds the deeming in §4, verification methods, and reaches neither.

Consequence. A transfer can carry an account label, a nickname, one holder of two, or a trading name, and every downstream control operates faithfully on the unverified string.

Existing controls.

Control area	Design	Implementation	Effective against this risk
Customer verification at onboarding	Sound	Assumed sound (design only)	**No. Its object ends at onboarding; it never reaches the message.**
Pre-dispatch sanctions screening	Sound	Assumed running (design only)	**No. It consumes the unverified string; it screens faithfully against the wrong name.**
Payment-message schema validation	Sound	Assumed running (design only)	**No. Format is not identity; a plausible label passes.**
Customer due diligence periodic review	Sound	Assumed running (design only)	**Not evidenced. It reaches past onboarding and resets on a change of identity information. It bears on this risk only through the age of the evidence a transfer relies on, and no clause in the governing tier states a maximum; no reconciliation joins the due diligence record to the dispatched fields.**

Control areas only here; this risk's linked controls are published in the register extract, and the register's others stay inside engagements. The analysis is evidence-driven and documentary throughout: every fact above is cited to a governing or platform document; nothing here was observed in operation. Those documents are published in excerpt, and every clause cited above is indexed against them at mittenda.com/check.html. How far a review of documents reaches is set out at mittenda.com/working-papers.html.

Risk evaluation

Level of risk High: unmitigated in effect. No control in view is shown effective against this risk; each passes its own test while the unverified string travels.

Against criteria Outside appetite, on the firm's own statement: Risk Appetite Statement §5.1, read with the register's ‘strict’ designation. Acceptance is not available at any level.

Decision Treat, as priority.

Risk treatment

Treatment A requirement in the Transfers Standard, in two limbs. First, the Article 4(1) / 14(1) fields are drawn from the verified customer record, with the lawful fallbacks (trading name; joint holder) written down and evidenced. Second, the record drawn from is within a stated maximum evidence age at the moment of dispatch, or dispatch is gated on the interval: as drafted, the first limb alone is satisfied by faithfully transmitting a stale verified name. The register carries the second as a linked control, a pre-dispatch check on the interval between the verification evidence and the transfer. The operational procedures inherit both on both rails.

Owner Head of Financial Crime; Payments Operations and the platform owners deliver. Target: the Standard amended by 30 June 2026, procedures and the pre-dispatch check within the quarter.

Evidence path The join demonstrated in implementation, then evidenced in operation over time.

Residual risk The modes that survive both limbs: wrong-record matching, and the interval below whatever maximum age the firm sets. Passed to monitoring and review. Until the second limb is written, stale evidence is an untreated primary exposure and not a residual one.

What a full assessment contains

The full engagement assesses every designated key risk this way, register-derived, on ISO 31000 discipline, the strict set leading, each risk carrying this record. It closes with the complete obligation-to-policy map, remediation priorities, and a position a supervisor can be shown. The diagnostic's fee is credited in full against it. The firm's own sign-off sits on that whole record, the three lines signing together; an extract carries the record control above and not those signatures.

Andrew Travis
Director
OpusDatum Risk