AVIS Land
Wolfsberg Principles and Financial Crime Compliance Statement

Version 1.0 | 25 November 2026

GENESIS sets the following financial-crime standards for its operation of AVIS Land, its QUANTUM gateway and the services it undertakes. This company-issued Statement establishes programme commitments and responsibilities informed by relevant Wolfsberg Group publications, proportionate to the actual entity, activity, territory and risk.

1 Issuing operators and contact

The issuing operators are GENESIS Collateral House Company Limited, Irish company number 823931, registered at 51 Bracken Road, Dublin D18 CV48, Ireland, and GENESIS Collateral House Company, North Carolina entity number 3214399, registered at 4111-E Rose Lake Drive, Charlotte, North Carolina 28217, USA. GENESIS operates within the Monkeyrock group. Each operator is responsible for the activities it undertakes and the legal requirements applicable to it.

Enquiries and due-diligence requests use legalcube@avis.land. Principal operating and correspondence office: GENESIS, 17–25 Via Ingegno, 84087 Sarno (SA), Italy. Telephone and WhatsApp: +34 674 002 006. Website: https://avis.land. Confidential information must be exchanged through an appropriately secured channel agreed for the request.

2 Meaning and scope of this Statement

GENESIS shall apply the relevant Wolfsberg principles as programme standards alongside applicable law. The programme covers money laundering, terrorist and proliferation financing, sanctions evasion, bribery and corruption, fraud and relevant predicate crime. It shall pursue three outcomes: fulfil financial-crime legal obligations; reduce the opportunity for services to facilitate crime through proportionate controls; and provide useful information to competent authorities in relevant priority areas. Wolfsberg guidance does not replace legislation or a regulator's requirements. Higher lawful requirements apply; conflicts with local law must be escalated and resolved through documented controls.

This is a GENESIS statement, not a Wolfsberg-issued certificate, membership claim, external assurance opinion or completed due-diligence questionnaire. Statements about an implemented control, examination, test or regulatory status must be supported by current evidence. A policy requirement and evidence that the requirement is operating must be distinguished in every assurance response.

Independent vendors, franchisees, issuers, banks and other providers retain their assets, permissions and obligations. Gateway access does not create bank status or transfer a participant's licence to GENESIS. GENESIS shall assess its actual role and remain responsible for its own services, including controls it outsources.

3 Governance and accountable functions

Each operator's governing body shall approve the programme, risk appetite and material changes, ensure adequate expertise and resources, and receive reporting on material exposures, control performance, overdue actions and incidents. Management shall designate the responsible

financial-crime officer and any locally required money-laundering reporting officer, with sufficient authority, access to information and direct escalation to the governing body.

Operational management shall own customer relationships and first-line controls. A compliance function with appropriate independence shall set standards, advise, challenge and oversee compliance. Internal audit or a suitably qualified independent reviewer shall assess the programme as the third line. Arrangements may be proportionate to scale, but conflicts must be managed and no person may independently assure their own control work.

Staff and relevant contractors shall receive training suited to their roles before undertaking relevant duties and thereafter according to risk and change. Management shall track completion, competence and corrective action. Staff shall be able to report concerns confidentially without retaliation; commercial targets must not suppress escalation or reporting duties.

4 Risk assessment and proportionality

GENESIS shall assess inherent and residual risks across customers, beneficial owners, products, counterparties, jurisdictions, delivery channels, transaction patterns and technology. Assessments shall cover marketplace trading, financing, tokenisation, project and construction flows, franchise networks, manufacturing and research arrangements where relevant to the operator's activities. They shall consider credible national priorities and threat information, with reasons recorded for material judgements.

The programme shall prioritise material risks and permit simplified measures only where lawful and justified. Higher risk calls for appropriate additional measures, not an unsupported finding of criminality. Changes in ownership, licence, payment corridor, business model, customer behaviour, technology or adverse information shall trigger reassessment. New or materially changed services require assessment and the necessary controls before the relevant activity begins. Redundant controls may be redesigned through documented governance without removing legal obligations.

5 Customer knowledge beneficial ownership and enhanced diligence

For a relationship or activity requiring customer due diligence, the responsible function shall identify and verify the customer, authority of representatives, relevant natural-person beneficial owners and controllers, using reliable evidence at the stage required by applicable law and the service. Any permitted delayed verification requires its legal conditions, documented justification and appropriate transaction controls. It shall understand the ownership structure, business purpose, expected activity, intended products and relevant funding. Nominee, trust and layered structures require an explanation sufficient to identify who ultimately owns, controls or benefits; a registry entry alone does not resolve inconsistent evidence.

Higher-risk relationships require enhanced diligence tailored to the concern, including corroboration of source of funds and, where relevant, source of wealth, commercial rationale, counterparties and geographic exposure. Required senior approval must precede the relevant commitment. Reviews shall occur on a documented risk basis and on material events; unresolved material identity or ownership concerns must be escalated before proceeding.

Politically exposed persons, relevant family members and close associates shall be identified and assessed under applicable requirements. Political exposure is a risk factor, not an allegation of wrongdoing. Required approval, funding checks and enhanced monitoring must be applied. Any later declassification requires a documented assessment and the applicable approval; leaving office does not automatically end the risk.

Adverse information shall be assessed for identity match, source reliability, relevance, seriousness, age and procedural status. An allegation must not be recorded as a conviction. Screening results and decisions shall preserve the rationale and the basis for correcting a false match.

6 Correspondent banking and non bank payment relationships

The requirements for correspondent banking apply when the actual relationship has that character. A technology connection or ordinary corporate payment account shall not be described as a correspondent-banking service without assessing its substance. Financial-institution and payment-provider relationships shall identify the legal entity, regulator and required permissions, ownership, services, customers, payment flows, control responsibilities and any material enforcement history.

Where correspondent services are provided or received, the responsible entity shall perform the required due diligence, obtain appropriate approval and document each party's responsibilities. Nested or downstream arrangements must be disclosed and assessed for the institutions, customer types, jurisdictions and transparency involved. Payable-through access requires the applicable assurance about the respondent's customer diligence and timely access to relevant customer information. GENESIS shall not establish relationships with shell banks or knowingly facilitate indirect access for them. Required financial permissions must be verified.

For non-bank payment providers, assessments shall distinguish proprietary payments from customer, bundled, netted and sponsored-account flows. Third-party disbursements must not be concealed as proprietary liquidity transfers. Agreements shall address agents, access to underlying information, safeguarding responsibilities and changes to flows. Each provider's statutory duties remain its own.

7 Payment transparency and digital asset information

For applicable fiat-payment activity, GENESIS shall apply the Wolfsberg Payment Transparency Standards according to its actual role. Payment design shall identify the debtor, creditor and relevant intermediary providers accurately, preserve required identifiers and use the required message fields. Bundling, internal netting or use of domestic infrastructure must not disguise the underlying cross-border or third-party nature of a payment.

Required payment information must not be stripped, falsified or deliberately obscured to bypass screening. Message conversion shall preserve required meaning and traceability. Missing or inconsistent data shall be investigated and handled under applicable rejection, suspension, information-request or other rules. Agreements shall allocate the responsibilities of originating, intermediary and receiving providers and require appropriate cooperation.

The 2023 Wolfsberg Standards do not apply directly to digital assets. Digital-asset transfers shall instead meet the information, counterparty, originator and beneficiary verification and transmission requirements applicable to that transfer and provider, including any applicable Travel Rule. Blockchain visibility or a wallet address does not by itself establish customer identity. Data shall be transmitted securely through suitable mechanisms; personal information need not be placed on a public blockchain merely to demonstrate transparency.

8 Sanctions bribery corruption tax crime and fraud

The responsible entity shall identify the sanctions regimes applicable to its business and transactions, maintain relevant screening inputs and assess ownership, control, indirect benefit and restricted activities. A potential match requires a documented resolution; name screening alone does not address every prohibition. Freezing, rejection, licensing, reporting and release decisions must follow applicable law. Routing, resubmission or alteration of information to evade a prohibition is forbidden.

GENESIS prohibits offering, promising, giving, requesting or receiving an improper advantage, directly or through another person. Controls shall address public officials, procurement, agents, referrals, gifts, hospitality, employment opportunities, donations, franchise awards and acquisitions. Payments require a legitimate purpose and accurate records. Due diligence, approvals and post-acquisition integration shall address identified corruption risks.

GENESIS shall not knowingly facilitate criminal tax evasion, false beneficial-ownership representations, fraudulent invoicing or concealment of criminal proceeds. Legitimate tax planning shall not be presumed criminal merely because it is cross-border. Suspected tax crime requires appropriately qualified review and escalation.

Fraud controls shall address impersonation, account takeover, payment diversion, false documents, merchant collusion and misuse of financing or project claims. Fraud and cyber-incident information shall inform financial-crime investigations where lawful. A customer may be a victim rather than a perpetrator; safeguarding and recovery action shall reflect the evidence.

9 Monitoring for suspicious activity and responsible automation

Monitoring shall combine relevant transactions with customer knowledge, behaviour, relationships, account changes, credible adverse information and referrals. Rules, analytics and human investigation shall address the operator's material threats and payment flows. Unusual activity requires assessment in context; an alert is not a finding of crime. Monitoring coverage, data quality, investigator capacity and unresolved backlogs shall be governed and reported.

Robotic and QUANTUM processes may assist collection, analysis and case preparation within their approved authority. Responsible staff remain accountable for decisions and legally required reports. Material model changes require proportionate validation, documented purpose, data assessment, testing of relevant risks, explainability appropriate to the user and monitoring for deterioration. Transition criteria shall test improved risk coverage and useful investigative outcomes, with safeguards against loss of required controls.

Effectiveness shall not be measured solely by alert or report counts. Management shall evaluate the quality and timeliness of investigations, coverage of priority threats, material omissions, useful authority feedback where available, and whether controls identify and reduce real exposure. Reducing low-value alerts must not suppress a report required by law.

10 Escalation reporting confidentiality and information sharing

Staff shall promptly refer suspicions and significant control failures to the designated financial-crime function. That function shall preserve relevant records, assess the facts and statutory reporting position, and arrange timely reporting to the appropriate authority where required. Responsibilities must remain clear where several operators or providers are involved; referring a matter to another provider does not discharge an independent reporting duty.

Investigations, reporting decisions and disclosures shall be documented. Access shall be limited to authorised persons with a legitimate need. Communications must respect suspicious-report confidentiality, tipping-off restrictions, data protection and legal privilege. Customers may receive information and review rights where lawful, without disclosure that prejudices a protected investigation.

Information may be shared with competent authorities, relevant providers or legitimate public-private arrangements only through an applicable legal basis and authorised channel. The recipient, purpose, permitted use and necessary safeguards must be established. The platform's general asset-processing mandate does not authorise unrestricted disclosure across the technology cluster. Retention shall follow the applicable legal schedule, with preservation for lawful holds and secure disposal when justified retention ends.

11 Assessment independent testing and correction

Management shall review the programme at least annually and after material changes. Independent testing shall follow a documented, risk-based plan and any mandatory frequency. Reviews shall examine legal requirements, control design and actual operation, relevant data, outsourcing, payment

transparency and the quality of escalation and reporting. Reviewers shall have appropriate expertise, access and freedom from interference.

Findings shall identify the affected scope, significance, responsible owner and corrective timetable. Management shall address root causes, apply justified interim measures, escalate material delay and obtain appropriate validation of closure. Reports shall distinguish completed work from planned improvements. A test of one entity, system or sample must not be presented as assurance over every participant or transaction.

12 Questionnaires evidence and public representations

As at this Statement's date, the official published forms are CBDDQ version 1.4 and FCCQ version 1.2, supported by CBDDQ Guidance version 2.0, Glossary version 3.0 and FAQs version 3.0. The responsible function shall check the official publication before issuing a response and identify its version, responding entity, covered locations and assessment date.

A CBDDQ shall be completed at legal-entity level, identifying covered branches and material differences; subsidiaries must not be silently included. A materially different branch requires the treatment specified by the guidance. An FCCQ may describe a clearly defined group programme but does not replace the required assessment of correspondent-banking activity. A non-bank gateway shall answer only for its actual role, using a tailored response where appropriate.

Responses shall be complete, accurate and supported by records. Proposed controls must not be answered as implemented; unknown or inapplicable matters require an honest explanation. Required business and compliance sign-offs must be obtained before a CBDDQ is released; the FCCQ requires the specified senior compliance sign-off. Supplementary questions shall remain separate from the official form.

GENESIS shall review issued questionnaires within 12 months and correct material changes as soon as reasonably practicable. This is GENESIS's review commitment, not a Wolfsberg certification period. External statements must identify their scope and evidential basis. This Statement neither supplies a completed questionnaire nor grants an assurance, licence or endorsement from the Wolfsberg Group.

Reference publications

Guidance on the Risk-Based Approach (2026)

Guidance on the Provision of Banking Services to non-bank Payment Service Providers (2026)

Statement on Effective Monitoring for Suspicious Activity, Part II: Transitioning to Innovation (2025)

Statement on Effective Monitoring for Suspicious Activity (2024)

Principles for Auditing for Effectiveness (2024)

Payment Transparency Standards (2023) and Roles and Responsibilities (2024)

Financial Crime Principles for Correspondent Banking (2022)

CBDDQ/FCCQ FAQs version 3.0 (2023) and current forms