STATEMENT OF WORK

FRAUD AUDIT

SERVICE LINE: Fraud Audit

[DRAFT TEMPLATE — FOR REVIEW BY QUALIFIED LEGAL COUNSEL PRIOR TO USE. COMPLETE ALL BRACKETED FIELDS BEFORE SENDING.]

This Statement of Work ("SOW") is entered into under, and incorporated into, the Master Consulting Services Agreement ("Agreement") dated **[AGREEMENT DATE]** between **Orcly** [INSERT ENTITY NAME] ("Consultant") and **[CLIENT ENTITY NAME]** ("Client"). In the event of any conflict between this SOW and the Agreement, the Agreement governs unless this SOW expressly states otherwise.

1. ENGAGEMENT DETAILS

Client	*[Full legal entity name]*
Client Industry / Sector	*[iGaming / Crypto Exchange / Fintech / PSP / E-commerce]*
Service Line	Fraud Audit
SOW Reference	*[SOW-001]*
SOW Effective Date	*[DD Month YYYY]*
Engagement Lead (Orcly)	*[Founder name]*
Client Point of Contact	*[Name, Title, Email]*
Governing Agreement	*Master Consulting Services Agreement dated [DATE]*

2. SCOPE OF SERVICES

Consultant shall conduct a comprehensive, top-to-bottom review of Client's fraud defences — covering policies, procedures, controls, and technology — stress-tested against the full current threat landscape. The output is a prioritised remediation roadmap with clear ownership and timelines.

- Policy and procedure review — fraud policy, AML policy, acceptable use, escalation procedures
- Product and control gap analysis — detection tools, rule coverage, blind spots
- Threat coverage assessment across the full spectrum:
- — Identity fraud (synthetic identity, account takeover, first-party fraud)
- — Payment fraud (card-not-present, authorised push payment, chargeback fraud)
- — Emerging threats: pig-butchering scams, deepfake identity, mule networks
- Adversarial stress testing — simulated attack scenarios against current controls
- Benchmarking against regulated-industry best practice (iGaming, crypto, fintech)
- Vendor and tooling coverage review — gaps, overlaps, and redundancies
- [Add any additional scope items specific to this engagement]

Out of Scope:

The Fraud Audit is a review and advisory engagement. Consultant does not implement control changes, access live production systems beyond agreed read-only data provision, or conduct active penetration testing. Penetration testing

(if required) should be commissioned separately.

3. DELIVERABLES

- Fraud Audit Report — full findings across policies, controls, products, and threats
- Threat Coverage Matrix — current coverage vs. full threat landscape, scored by risk
- Control Gap Analysis — identified gaps with severity ratings (Critical / High / Medium / Low)
- Adversarial Stress Test Summary — scenarios tested, outcomes, and vulnerabilities identified
- Benchmarking Summary — Client position vs. regulated-industry peer standards
- Prioritised Remediation Roadmap — ranked action plan with suggested owners, effort, and timelines
- Executive Summary — board/leadership-ready summary of key findings and priorities

4. TIMELINE & MILESTONES

Engagement Start Date	*[DD Month YYYY]*
Phase 1 — Documentation & Access	Week [1]: policy documents, data access, stakeholder briefing
Phase 2 — Audit & Testing	Weeks [2–4]: control review, threat assessment, stress testing
Phase 3 — Analysis & Report	Week [5]: findings analysis, roadmap, draft report
Phase 4 — Delivery & Debrief	Week [6]: final report, executive presentation, Q&A;
Estimated Total Duration	*[6 weeks]*

5. FEES & PAYMENT

Fee Structure	*[Fixed project fee: $[__]]*
Estimated Total	*$[__] [all-inclusive, excluding pre-approved expenses]*
Payment Schedule	*[50% on signing / 50% on delivery of final report]*
Payment Terms	*Net [15/30] days from invoice date*
Expenses	*[Pre-approved travel and accommodation billed at cost]*

All fees are exclusive of applicable taxes. Expenses (travel, accommodation, third-party tools) will be pre-approved in writing and billed at cost with supporting receipts.

6. CLIENT OBLIGATIONS

Client shall provide Consultant with timely access to the following for the duration of this engagement:

- Relevant data, reporting, and system access as reasonably required
- Named point of contact with authority to respond within [2] business days
- Attendance at scheduled review calls and milestone sign-off meetings
- Accurate and complete information — Consultant is entitled to rely on Client-provided data without independent verification

7. SPECIAL TERMS & NOTES

Findings and recommendations are based on information, access, and data provided by Client during the audit period. Consultant cannot guarantee identification of all vulnerabilities. Client is solely responsible for prioritising and implementing remediation actions.

IMPORTANT — NO GUARANTEE OF OUTCOME: THIS ENGAGEMENT IS ADVISORY IN NATURE. CONSULTANT DOES NOT GUARANTEE ANY SPECIFIC REDUCTION IN FRAUD LOSSES, CHARGEBACK RATIOS, OR ANY OTHER BUSINESS OUTCOME. ALL IMPLEMENTATION DECISIONS REMAIN SOLELY WITH CLIENT. SEE SECTION 10 OF THE MASTER CONSULTING SERVICES AGREEMENT FOR FULL LIABILITY TERMS.

---

8. AGREED & ACCEPTED

By signing below, each Party agrees to be bound by this SOW and the terms of the Master Consulting Services Agreement.

ORCLY [INSERT ENTITY NAME]

By: _____

Name: _____

Title: _____

Date: _____

[CLIENT ENTITY NAME]

By: _____

Name: _____

Title: _____

Date: _____