CLIENT FUNDS AND PAYMENT TERMS

DEPOSITS, WITHDRAWALS, CRYPTO-ASSET PAYMENTS AND PAYMENT-RISK CONTROLS

VENOR MARKETS

WEBSITE AND CRM CONTRACTUAL CONDITIONS

LEGAL ENTITY	Venor Ltd
REGISTRATION	Saint Lucia 2026-00242
DOCUMENT	Client Funds and Payment Terms
DOCUMENT ID	VM-PAY-CFP-001
VERSION	2.0
CLASSIFICATION	PUBLIC WEBSITE + CRM

IMPORTANT: Read this document with the prevailing Client or Partner Agreement and the current schedules displayed through Venor's approved channels.

IMPORTANT: KYC is compulsory before any deposit is credited or withdrawal is processed. Crypto transactions may be irreversible.

DOCUMENT STATUS AND CONTRACTUAL APPLICATION

These Client Funds and Payment Terms form part of the Venor Markets Client Agreement and govern deposits, credits, conversions, withdrawals, refunds, reversals, chargebacks and payment-related risks through the website and CRM Portal. Venor currently supports only the approved cryptocurrency assets and blockchain networks shown in the authenticated CRM. Any future payment method is subject to the transaction-specific terms displayed before confirmation. These Terms must be read with the Terms of Service, AML/CFT Policy, Privacy Policy, Risk Disclosure, Product Specifications and applicable CRM instructions.

CONTENTS

1. APPLICATION AND ACCEPTANCE

1.1 These Crypto-Asset Deposit and Withdrawal Terms and Conditions (the "Payment Terms") govern every crypto-asset deposit, credit, conversion, transfer, refund and withdrawal made through the Venor Markets website or CRM Portal.

1.2 These Payment Terms form part of the Client Agreement and must be read with the Terms of Service, AML/CFT Policy, Privacy Policy, Risk Disclosure, Product Specifications and CRM instructions. If there is an inconsistency, mandatory law prevails, followed by any product- or jurisdiction-specific term and then these Payment Terms.

1.3 By creating a payment instruction, displaying a deposit address, sending assets, requesting a withdrawal or continuing to use the payment service, the Client confirms acceptance of these Payment Terms.

1.4 The Company may use wallet, blockchain, custody, payment, liquidity, screening, analytics and technology providers. No provider becomes a party to the Client Agreement or owes a contractual duty to the Client.

2. MANDATORY KYC AND ACCOUNT ELIGIBILITY

2.1 Know-your-customer verification is compulsory before the Company permits or credits a deposit and before it accepts, approves or broadcasts a withdrawal.

2.2 The Client must complete identity, liveness, address, nationality, tax-residency, sanctions, politically exposed person, adverse-media and risk screening to the Company's satisfaction. A corporate Client must also verify its incorporation, business activity, ownership, beneficial owners, controllers and authorised signatories.

2.3 The Company may require source-of-funds, source-of-wealth, wallet-ownership, transaction-purpose, counterparty and Travel Rule information at any time, including after funds have reached a Company-controlled address.

2.4 KYC approval for account opening is not permanent approval for every payment. The Company may repeat or enhance verification, impose transaction limits, or suspend payment access whenever information expires, changes, appears inconsistent or creates additional risk.

2.5 The Company may decline to credit received assets, place them in a suspense account, or block withdrawal until all requested verification is completed. The Client has no right to interest, trading profit or compensation for that review period.

2.6 False, incomplete, expired or misleading information is a material breach and may result in rejection, freezing, return of funds, close-only status, account termination and reporting to competent authorities.

3. CRYPTO-ONLY PAYMENT MODEL

3.1 The Company accepts and pays only the crypto-assets and blockchain networks expressly enabled in the CRM Portal. Fiat methods are unavailable unless separately introduced in writing.

3.2 Deposit availability does not guarantee withdrawal availability. The Company may add, remove, suspend, limit or substitute an asset or network for legal, compliance, liquidity, security, technical, provider or market reasons.

3.3 The Company may require withdrawal in a different supported asset or network where the original route is unavailable, subject to a commercially reasonable conversion and the Client's verification of the replacement destination.

4. CLIENT PAYMENT INSTRUCTIONS

4.1 The Client must use only the authenticated CRM Portal and must independently verify the asset, network, complete address, token contract, amount, memo or destination tag, minimum, confirmations and fees before submitting a transaction.

4.2 An instruction submitted using the Client's authenticated credentials and security factors will be treated as authorised unless the Company had actual notice of compromise before acting on it.

4.3 The Company is not required to verify whether an address pasted or entered by the Client is economically intended by the Client. Address validation confirms format only and does not confirm ownership, identity, safety or recoverability.

4.4 Blockchain transactions are normally irreversible. The Company has no obligation to cancel, recall or recover an asset after broadcast.

5. DEPOSIT ADDRESSES

5.1 The Client must obtain the current deposit address directly from the authenticated CRM Portal immediately before each transfer.

5.2 Addresses supplied by email, messaging applications, social media, screenshots, employees, affiliates or introducing brokers must not be used.

5.3 An address may be unique, shared, temporary, rotated, suspended or retired. Previous successful use does not prove that an address remains active.

5.4 The Client must not share an assigned address or permit another person to use it. The Company may treat deposits from another person as prohibited third-party funding.

6. SUPPORTED ASSETS, NETWORKS AND INCORRECT TRANSFERS

6.1 Tokens with identical or similar names on different networks are distinct assets and are not interchangeable.

6.2 The Company is not responsible for assets sent through an unsupported network, to an incorrect or expired address, under an incorrect token contract, without a required memo or tag, below the stated minimum, or through an unsupported bridge, privacy protocol or smart-contract method.

6.3 Recovery is not guaranteed even where technically possible. Before attempting recovery, the Company may require ownership evidence, indemnities and advance payment of all network, provider, legal, investigation and administration costs.

6.4 The Company may decline recovery where the value does not justify the cost, recovery could affect another customer, or legal, sanctions, security or provider restrictions apply.

7. OWNERSHIP AND THIRD-PARTY FUNDING

7.1 Deposits must originate from a wallet or exchange account legally and beneficially owned and controlled by the Client. Withdrawals must normally be made to a wallet or exchange account legally and beneficially owned and controlled by the same Client.

7.2 Third-party deposits and withdrawals are prohibited unless the Company gives prior written approval following enhanced due diligence.

7.3 The Company may require a cryptographic signature, verification transfer, exchange statement, account record, transaction hash, video verification or other evidence of wallet ownership.

7.4 Unverified third-party funds may be frozen, rejected or returned to the verified source, less applicable costs, where legally and technically possible.

8. PROHIBITED SOURCES AND USE

8.1 The Client must not use the account for money transmission, pass-through payments, asset storage, layering, concealment or any activity unrelated to genuine permitted trading.

8.2 Funds connected with fraud, theft, scams, cybercrime, ransomware, sanctions evasion, terrorist financing, darknet markets, illegal gambling, mixers, tumblers, stolen wallets, tax evasion or other unlawful activity are prohibited.

8.3 The Company may refuse privacy coins, anonymising protocols, high-risk bridges, peer-to-peer counterparties or unregulated services outside its risk appetite.

8.4 Splitting, structuring or coordinating transactions to avoid limits, monitoring, Travel Rule requirements or enhanced review is prohibited.

9. BLOCKCHAIN SCREENING AND COMPLIANCE HOLDS

9.1 Every deposit and withdrawal may be screened against blockchain analytics, sanctions, fraud, adverse-media and internal risk systems.

9.2 The Company may delay, suspend, reject, freeze, return, block or report a transaction where an alert, mismatch, legal request, security concern or unusual pattern exists.

9.3 The Company may preserve and share information with banks, exchanges, wallet providers, analytics providers, regulators, law-enforcement bodies and competent authorities where permitted or required.

9.4 The Company is not required to disclose confidential monitoring thresholds, detection methods, provider data, suspicious-activity reports or legal requests.

10. WHEN A DEPOSIT IS RECEIVED AND CREDITED

10.1 A transaction hash, wallet deduction, blockchain broadcast or initial network confirmation does not mean that the Company has received, accepted or credited a deposit.

10.2 A deposit is eligible for credit only after detection on the correct supported network, completion of required confirmations, transaction-integrity validation, compliance clearance, correct account matching and final ledger posting.

10.3 The Company may increase confirmation requirements or delay credit during congestion, volatility, reorganisations, forks, attacks, provider outages or enhanced review.

10.4 Until final ledger posting, the Client has no right to trade, withdraw or claim interest, profit, opportunity loss or compensation in respect of the pending deposit.

10.5 If assets are confirmed as received by a Company-controlled wallet but are not credited because of a Company ledger error, the Company's obligation is limited, subject to verification and applicable law, to correcting the ledger or returning the verified amount less unavoidable network and third-party charges. The Company is not liable for market movement, missed trades, lost profit or other indirect or consequential loss.

11. VALUATION, CONVERSION AND STABLECOINS

11.1 The trading ledger may be denominated in USD even where the deposited or withdrawn asset is a crypto-asset.

11.2 Conversion applies at the commercially reasonable executable rate available when the Company processes the transaction, including any spread, liquidity cost and provider charge, and not necessarily when the Client broadcasts or requests it.

11.3 A stablecoin is not legal tender, a bank deposit or necessarily equivalent to USD. The Company does not guarantee its peg, liquidity, reserves, redemption or continued support.

11.4 The Company may suspend or convert a stablecoin affected by de-pegging, issuer action, blacklist, freeze, reserve concern, market disruption or network failure.

12. LIMITS, RESERVES AND FEES

12.1 The Company may impose minimums, maximums, frequency limits, velocity limits, reserves and approval thresholds by Client, asset, network, wallet, jurisdiction, verification level or risk rating.

12.2 The Client is responsible for all gas, network, processing, conversion, liquidity, provider, investigation, recovery and administration charges. Fees may be deducted from the amount sent, received, credited or withdrawn.

12.3 Fees and limits may change before execution. If the balance is insufficient, the Company may reduce, defer or reject the transaction.

12.4 Attempts to avoid a fee, reserve or limit constitute a material breach.

13. WITHDRAWAL ELIGIBILITY

13.1 A withdrawal may be requested only through the authenticated CRM Portal after compulsory KYC and all requested enhanced checks are complete.

13.2 The Client must have sufficient cleared and withdrawable balance after open positions, Margin, unsettled deposits, fees, reversals, liabilities, reserves and set-off rights are taken into account.

13.3 A displayed balance does not guarantee immediate availability. Deposits, profits, rebates, commissions and partner remuneration may have different settlement and withdrawal conditions.

13.4 The Company may require genuine trading activity and may return unused or minimally traded deposits only to the verified source wallet.

14. BENEFICIARY VERIFICATION AND ADDRESS ALLOWLISTING

14.1 Withdrawals will normally be made only to a verified Client-owned wallet. The Company may require return to the original funding source.

14.2 A new or changed address may require password confirmation, two-factor authentication, email or mobile approval, wallet-ownership evidence, manual approval and a cooling-off period.

14.3 A cooling-off period or withdrawal hold may follow a password, email, telephone, device, security-factor or beneficiary change, unusual login or suspected compromise.

14.4 The Company will never request a private key, seed phrase or recovery phrase.

15. WITHDRAWAL REVIEW AND COMPANY DISCRETION

15.1 A withdrawal request is an instruction for review and not an unconditional debt immediately due or a guarantee of execution.

15.2 Review may include KYC refresh, balance and Margin checks, wallet ownership, device and IP analysis, sanctions and blockchain screening, source-of-funds review, behavioural analysis, Travel Rule compliance, liquidity checks and multi-person approval.

15.3 The Company may contact the Client through verified channels and may decline to act until satisfactory confirmation is received.

15.4 Venor may delay, restrict, cancel or reject a request only where it reasonably identifies a legal, regulatory, compliance, sanctions, security, fraud, trading-abuse, payment-integrity, liquidity, provider, blockchain, technical, operational, audit or force-majeure concern. The measure may apply to the affected transaction, account, linked accounts, wallet, beneficiary or amount and must be no broader or longer than Venor reasonably considers necessary, subject to applicable law and rights that cannot be waived.

16. WITHDRAWAL EXECUTION AND FINALITY

16.1 A withdrawal becomes final only after confirmed blockchain settlement. Pending, approved, signed or broadcast status is not final settlement.

16.2 Before broadcast, the Company may cancel, amend or reject the request. After broadcast, the transaction will generally be irreversible.

16.3 The Company does not guarantee execution time, confirmation time, receipt time, a particular fee or the continued availability of a route.

16.4 The Client must verify the address, network, asset, token contract, memo, destination compatibility and amount. The Company is not responsible for loss caused by incorrect Client instructions, subject to liability that cannot lawfully be excluded.

17. COMPANY DEBITED BUT BENEFICIARY NOT CREDITED

17.1 A debit, signed transaction or blockchain broadcast from a Company-controlled wallet does not guarantee that a receiving wallet, exchange, custodian or service provider will credit the Client.

17.2 If Company or provider records show a successful on-chain transfer to the destination instructed and confirmed by the Client, the Company's payment obligation is discharged to the extent permitted by law, even if the receiving platform delays, rejects, freezes, misapplies or fails to credit the transfer.

17.3 The Company is not responsible for the receiving platform's policies, insolvency, maintenance, compliance review, unsupported token or network, memo requirements, internal ledger failure or account restrictions.

17.4 If the Company's wallet is debited but the transaction fails on-chain or no valid transfer is completed, the Company will investigate. Subject to reconciliation and legal clearance, the Company may reprocess the withdrawal or restore the net amount actually recovered. This is the Client's exclusive contractual remedy, except for liability that cannot lawfully be limited.

17.5 The Company is not liable for price movement, lost trading opportunity, lost profit, exchange-rate change, business interruption, reputational loss or indirect, incidental, special, punitive or consequential loss arising during investigation, reprocessing, recovery or delayed credit.

17.6 The Client must first pursue the receiving wallet or exchange where the blockchain confirms delivery to the Client-supplied destination. The Company may provide reasonable transaction evidence but is not required to litigate, arbitrate or recover funds from the recipient on the Client's behalf.

18. PROVIDER, NETWORK AND FORCE MAJEURE RISK

18.1 The Company is not responsible for delay, failure, error, suspension, insolvency, cyber incident or service interruption affecting a blockchain, validator, bridge, stablecoin issuer, wallet, exchange, custodian, analytics service, internet service or other independent provider, except to the extent liability cannot lawfully be excluded.

18.2 During an abnormal event the Company may suspend deposits or withdrawals, increase confirmations or fees, change routes, require another asset, cancel pending requests, preserve reserves or take other reasonable protective action.

18.3 No processing estimate is a guarantee. Time is not of the essence for a deposit or withdrawal unless mandatory law expressly provides otherwise.

19. SECURITY AND CLIENT CREDENTIALS

19.1 The Client must secure passwords, email, devices, wallets and two-factor authentication and must notify the Company immediately of suspected compromise.

19.2 The Company may suspend access and require renewed identity, device and wallet verification before restoring payment functionality.

19.3 The Company is not required to process a withdrawal while a security investigation remains open.

19.4 The Client is responsible for instructions authenticated through the Client's credentials unless the Company acted fraudulently or with liability that cannot lawfully be excluded.

20. REVERSALS, ERRORS AND NEGATIVE BALANCES

20.1 The Company may correct a duplicate, erroneous, provisional or mistaken credit and may reverse any amount not finally received or lawfully due.

20.2 If an error, reversal, failed settlement, asset freeze or provider adjustment creates a deficit, the Client must immediately repay it. The Company may close positions, withhold withdrawals, set off balances and recover reasonable costs.

20.3 The Client must notify the Company promptly after discovering an incorrect credit and must not trade, withdraw or transfer an amount known or reasonably suspected to be erroneous.

21. SET-OFF, WITHHOLDING AND RECOVERY

21.1 To the extent permitted by law and the Client Agreement, the Company may combine accounts, withhold amounts and set off any matured obligation owed by the Client against funds, profits, commissions, rebates or other amounts payable by the Company.

21.2 The Company may retain a reasonable reserve for open positions, unsettled transactions, fees, investigations, indemnity claims, suspected fraud, provider reversals or anticipated liabilities.

21.3 The Client is responsible for reasonable recovery, investigation, legal and enforcement costs arising from breach, fraud, incorrect instructions or prohibited funding.

22. INVESTIGATIONS, FREEZES AND REPORTING

22.1 The Company may place an account or asset under review where unlawful activity, sanctions exposure, fraud, third-party funding, stolen assets, prohibited trading, inaccurate information or control evasion is suspected.

22.2 During review, the Company may suspend deposits, withdrawals, trading, transfers and access without liability for trading opportunity or market movement.

22.3 Funds may remain restricted for as long as reasonably required by the Company, a provider, regulator, court, law-enforcement body or applicable law.

23. REJECTED, RETURNED AND UNCLAIMED ASSETS

23.1 A return is subject to legal, compliance, technical and operational feasibility and will normally be made only to the verified source wallet.

23.2 The returned amount may be reduced by network, conversion, provider, investigation, recovery and administration costs and market movement.

23.3 The Company may decline a return where an authority, sanctions restriction, asset freeze, provider rule or legal obligation prevents it.

23.4 Unclaimed or unidentifiable assets may remain in suspense and be dealt with under applicable law and the Company’s unclaimed-property procedures.

24. FORKS, AIRDROPS AND UNSUPPORTED ASSETS

24.1 The Company has no obligation to support a fork, airdrop, staking reward, governance right, token migration, rebasing event or unsupported asset.

24.2 The Client acquires no entitlement merely because an unsupported asset is technically associated with a Company-controlled address.

24.3 The Company determines whether and how to recognise any fork, migration or distribution.

25. RECORDS AND CONCLUSIVE EVIDENCE

25.1 CRM records, Company ledgers, provider records, blockchain data, transaction hashes, server logs, security records, screening results, communications and approval records are evidence of payment activity unless shown to be manifestly incorrect.

25.2 The Company’s determination of timestamps, confirmations, executable conversion rates, fees and transaction status will apply absent manifest error.

25.3 Blockchain data is public and may remain permanently accessible. Records will be retained according to applicable law and Company policy.

26. CLIENT INDEMNITY

26.1 To the extent permitted by law, the Client indemnifies the Company, its affiliates, officers, employees and agents against direct losses, liabilities, penalties, claims and reasonable costs arising from the Client's breach, unlawful funds, third-party claims, incorrect payment instructions, misrepresentation, tax failure, wallet compromise or prohibited conduct.

26.2 The indemnity does not apply to loss finally determined to have resulted directly from the Company's fraud or wilful misconduct and does not exclude rights that cannot lawfully be waived.

27. LIMITATION OF LIABILITY

27.1 To the maximum extent permitted by law, the Company is not liable for indirect, incidental, special, exemplary, punitive or consequential loss, loss of profit, loss of opportunity, market movement, loss of business, loss of reputation or loss of anticipated savings arising from a payment service.

27.2 Where liability cannot be excluded, the Company's aggregate liability for a particular payment event is limited to the net amount of the affected transaction actually received and controlled by the Company, excluding market movement, hypothetical profit and third-party charges, unless mandatory law requires a higher amount.

27.3 Nothing excludes liability for fraud, wilful misconduct or any liability that applicable law does not permit the Company to exclude or limit.

28. CLIENT TAXES AND REGULATORY RESPONSIBILITY

28.1 The Client is responsible for determining and paying all taxes, duties and reporting obligations arising from crypto-asset deposits, conversions, trading and withdrawals.

28.2 The Company does not provide tax, legal or financial advice and may make disclosures or withhold amounts where required by law.

29. DATA, PRIVACY AND INFORMATION SHARING

29.1 The Company may process wallet addresses, transaction data, device information, identity records and compliance results for payment execution, fraud prevention, AML/CFT, sanctions, security, legal compliance and dispute handling.

29.2 Information may be shared with relevant providers, counterparties, analytics services and authorities in accordance with the Privacy Policy and applicable law.

30. COMPLAINTS AND DISPUTES

30.1 The Client must report a missing, incorrect or unauthorised payment promptly through an official support channel and provide the account number, asset, network, amount, address, transaction hash, date and supporting evidence.

30.2 A complaint does not require the Company to release funds, reverse a blockchain transaction or restore access while a lawful compliance or security restriction remains in place.

30.3 Governing law, jurisdiction and dispute-resolution provisions are those stated in the Client Agreement. No different jurisdiction is created by the location of a wallet, blockchain node or service provider.

31. AMENDMENTS AND SUSPENSION

31.1 The Company may amend these Payment Terms to reflect legal, regulatory, provider, asset, technology, security, operational or risk changes.

31.2 Material changes will be published on the website or CRM Portal where reasonably practicable. Continued use after the effective date constitutes acceptance except where express consent is required by law.

31.3 The Company may suspend or discontinue a payment service at any time, subject to mandatory law and the orderly treatment of verified Client balances.

32. PAYMENT DELAY, WITHDRAWAL RESTRICTION AND REVIEW EVENTS

32.1 Venor may place a payment, withdrawal, balance or account under review where trading activity appears irregular, manipulative, abusive, coordinated, artificial, economically inconsistent, unauthorised or connected with a breach of the Client Agreement, Product Specifications, Order Execution Policy, Prohibited Trading Practices Policy, promotion terms, partner terms or applicable law.

32.2 Relevant trading concerns include suspected latency or price-feed exploitation; manifest-error or stale-price trading; arbitrage or hedging arranged to exploit a technical, pricing, bonus, rebate or execution defect; coordinated or collusive accounts; account, identity or device sharing; unauthorised copy, signal, API, expert-adviser or automated activity; wash, circular or offsetting activity lacking a genuine commercial purpose; excessive order-message, cancellation or platform abuse; artificial volume; bonus, swap-free, rebate, CPA, IB or loyalty abuse; and transactions whose pattern, ownership, funding or economic purpose is materially inconsistent with the verified client profile. A profitable strategy, high trade frequency or use of automation alone is not sufficient evidence of abuse.

32.3 During a trading-integrity review, Venor may suspend the affected withdrawal, segregate disputed or provisional credits, restrict new deposits or orders, apply close-only status, preserve relevant open positions where operationally possible, request trading records or explanations, reconcile prices and executions, and withhold only the amount reasonably connected with the review or reasonably required as a reserve. Undisputed verified funds should not be restricted merely because another amount is under review, unless law, security, sanctions, insolvency risk or account interdependence reasonably requires a wider hold.

32.4 Venor may delay or suspend payment while carrying out a scheduled, event-driven or ad hoc internal audit; financial, wallet, ledger, reconciliation, treasury, security, risk, compliance, technology or trading audit; external independent audit; service-provider reconciliation; or a review requested or conducted by a court, regulator, tax authority, financial-intelligence unit, law-enforcement body, sanctions authority, government department or other competent authority. Venor is not required to disclose information where disclosure is prohibited, would prejudice an investigation or would reveal confidential controls.

32.5 Processing may be delayed by weekends, public or banking holidays, reduced staffing periods, maintenance windows, end-of-day, end-of-week, month-end or year-end reconciliation, wallet replenishment, treasury scheduling, blockchain congestion, confirmation delays, chain reorganisation, validator or node failure, provider cut-off times, liquidity constraints, conversion availability, cybersecurity controls, beneficiary checks or unusually high payment volumes. Published processing times are service targets and not guaranteed settlement deadlines.

32.6 Venor may pause a payment where it detects or reasonably suspects unauthorised access, compromised credentials, SIM-swap or email compromise, wallet-address substitution, malware, social engineering, disputed ownership, a changed beneficiary, unusual device or location activity, false or inconsistent information, duplicate or erroneous credits, a negative balance, an unsettled deposit, an open margin obligation, a chargeback or reversal risk, a third-party claim, a lien, set-off right or another matured or reasonably anticipated liability.

32.7 Venor may suspend, defer, reroute or cancel processing because of an act of God or force-majeure event, including natural disaster, fire, flood, storm, earthquake, epidemic, pandemic, war, terrorism, civil disorder, labour disruption, power or communications failure, cyberattack, critical infrastructure failure, blockchain or protocol failure, exchange or custodian failure, government action, sanctions, legal prohibition, court order, market closure or another event beyond Venor's reasonable control. Venor must take commercially reasonable steps to limit disruption and resume or resolve affected processing when reasonably practicable.

32.8 A restriction may remain in place for the period reasonably required to obtain information, protect the client or Venor, complete reconciliation, determine ownership, validate trading and payment activity, comply with law or an authority, preserve evidence, quantify a disputed amount, recover an erroneous credit, or receive a necessary response from an independent network, provider or authority. No fixed deadline applies where the duration depends on an external process, but Venor will review the restriction at reasonable intervals and will lift, narrow, continue or convert it into another lawful measure according to the available evidence.

32.9 Where legally and operationally permitted, Venor will provide a general status or request for information through an official channel. Venor may give notice before or after imposing an urgent restriction and may omit reasons or timing where disclosure is prohibited, could facilitate evasion, compromise security, prejudice an investigation or expose confidential monitoring methods.

32.10 Following review, Venor may approve or reprocess the payment; request another verified destination or supported asset; restore an amount actually recovered; return verified funds to source; correct or reverse an erroneous, invalid or provisional credit; deduct disclosed charges and amounts lawfully due; cancel profits, rebates, rewards or commissions demonstrably attributable to prohibited conduct where contractually permitted; terminate or restrict the relationship; or report or preserve assets as required by law. Venor may not confiscate verified funds as a penalty without a lawful and contractual basis.

32.11 A client may submit a complaint or payment-review request through Venor's official support channel. A complaint does not automatically release a lawful restriction, but Venor will maintain an internal record of the trigger, affected amount, decision, approvals, review activity and outcome, subject to legal privilege, confidentiality and disclosure restrictions.

32.12 Nothing in this section permits arbitrary delay, avoids a debt that is finally due, excludes Venor's fraud or wilful misconduct, or limits any right or liability that applicable law does not permit the parties to exclude or limit.

33. CLIENT DECLARATION

33.1 Each time the Client submits a deposit or withdrawal, the Client confirms that the Client is fully verified; is the lawful and beneficial owner of the funds and wallets; acts for the Client’s own benefit; uses no unlawful funds; has checked all transaction details; accepts irreversibility, fees and provider risks; and will provide further information on request.

33.2 The Client also acknowledges that payment screening, investigation, delay, rejection, freeze, return, set-off and reporting may occur without creating liability for market movement or lost opportunity, subject always to mandatory law.

APPROVAL, COMMENCEMENT AND REVIEW

This document has been approved and issued by Venor Ltd and becomes applicable when published or otherwise communicated through an official Venor channel. It remains applicable until amended, replaced or withdrawn.

Venor may review or update this document where reasonably required by legal, regulatory, operational, commercial, technology, security, risk, product or market developments. Material changes apply prospectively following any notice or renewed acceptance required by the applicable agreement or law. Administrative, explanatory or non-material updates may take effect upon publication or valid communication.

Where publication channels are temporarily not synchronised, the latest version validly communicated to the affected person applies. Venor will correct any discrepancy within a reasonable period. Earlier versions continue to govern matters arising while they were applicable.

CLIENT ACCEPTANCE

By selecting the acceptance box, submitting a deposit or requesting a withdrawal through an official Venor channel, the Client confirms that the Client has received or had access to, read, understood and accepted these Terms. Venor may retain the document identifier and version, acceptance timestamp, account or user identifier, jurisdiction, language and available device or network evidence as the electronic acceptance record.