



Anti-Money Laundering & Sanctions Policy

How ERIANUX, LLC takes payment, what it screens for, what its regulatory position actually is, and what it will not do — maintained as a standing record for banking, processing and platform relationships.

ISSUED BY ERIANUX, LLC

WYOMING, USA

EFFECTIVE 11 SEPTEMBER 2026

DOCUMENT REFERENCE

ERX-POL-003

VERSION

2.0

POLICY OWNER

Managing Member

APPROVED BY

Managing Member

CLASSIFICATION

Public

REVIEW CYCLE

Annual, or on material change

COMPLIANCE CONTACT

legal@erianux.com

NEXT REVIEW

11 September 2027

01 · Statement of policy

1.1 ERIANUX, LLC (the “Company”) will not accept, process, hold, transfer or facilitate any payment that it knows or suspects to represent the proceeds of criminal conduct, to be destined for the financing of terrorism or proliferation, or to be structured for the purpose of disguising its source, ownership or control.

1.2 The Company will not knowingly transact with any person, entity, vessel or jurisdiction subject to economic sanctions administered by the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC), nor with any entity owned fifty per cent or more, directly or indirectly, by one or more blocked persons.

1.3 Sanctions compliance is strict-liability in character. No commercial consideration, customer relationship or revenue outcome justifies an exception, and no person acting for the Company has authority to grant one.

02 · Regulatory position, stated plainly

2.1 What the Company is. The Company is a software business. It licenses its own charting, order-flow and drawing-tool products for the NinjaTrader 8 platform, sells subscriptions to its own services, operates an affiliate referral programme, and sells branded merchandise through third-party print and fulfilment partners.

2.2 What the Company is not. The Company does not accept deposits, transmit funds on behalf of any other person, exchange or deal in currency or virtual currency, issue or redeem stored value, cash instruments, hold client money, or take custody of any customer asset. On that basis it is not a money transmitter or other money services business within the meaning of 31 C.F.R. §1010.100(ff), and is not a “financial institution” required to maintain a Bank Secrecy Act compliance programme under 31 U.S.C. §5318(h). It is not registered with FinCEN and is not required to be.

2.3 Where the regulated obligations sit. Card, wallet and bank payments are processed by regulated third parties — Stripe and PayPal for sales, and Plaid for the verification of affiliate payout accounts. Each carries its own customer due diligence, sanctions screening and transaction monitoring obligations, applied to every payment that passes through it. The Company does not duplicate those programmes; it does not rely on them as a substitute for the controls in clause 5.

2.4 Obligations that apply regardless. Three sets of obligations bind the Company irrespective of its non-regulated status: U.S. sanctions law, which applies to all U.S. persons; the criminal money-laundering prohibitions of 18 U.S.C. §§1956 and 1957, which apply to any person; and the currency-reporting requirement of 26 U.S.C. §6050I, which would require the filing of IRS/FinCEN Form 8300 on receipt of more than US\$10,000 in cash or cash equivalents in one or related transactions. The Company does not accept cash, so no Form 8300 circumstance arises.

03 · Legal and regulatory framework considered

- ◆ **United States.** Bank Secrecy Act, 31 U.S.C. §5311 *et seq.*, and its implementing regulations at 31 C.F.R. Chapter X; the money-laundering offences at 18 U.S.C. §§1956–1957; the International Emergency Economic Powers Act and the sanctions regulations at 31 C.F.R. Chapter V; the USA PATRIOT Act.
- ◆ **United Kingdom.** Proceeds of Crime Act 2002, Parts 7 and 8; the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; the Sanctions and Anti-Money Laundering Act 2018 and the UK sanctions list maintained by OFSI. The Company is not a “relevant person” under the 2017 Regulations; the POCA principal offences nonetheless apply to any person.

- ♦ **European Union and Canada.** The EU anti-money-laundering framework as applied to obliged entities, EU restrictive measures, and Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act. The Company is not an obliged entity or reporting entity under these regimes; its sanctions screening covers the consolidated EU and Canadian lists as a matter of policy.
- ♦ **Adjacent obligations.** The UK Economic Crime and Corporate Transparency Act 2023 s.199 failure-to-prevent-fraud offence, and the card-network rules and acceptable-use policies of the Company's processors, which are treated as binding operational requirements.

04 · Business-wide risk assessment

4.1 Products. Low risk. Sales are of standardised, published-price digital licences and subscriptions. There is no mechanism in the Company's systems by which value can be moved between two third parties, stored for later withdrawal, or redeemed for anything other than the product purchased.

4.2 Channels. Low risk. All payment is card-present-equivalent or wallet-based through Stripe and PayPal on the Company's own checkout, with no cash, cheque, money order, bearer instrument, third-party wire or cryptocurrency accepted.

4.3 Customers and geography. Medium-low risk. Customers are individual retail traders worldwide. Geographic exposure is managed by sanctions screening at clause 6 rather than by a blanket country block.

4.4 Identified higher-risk vectors. Four are controlled specifically: (a) *card testing and stolen-card purchase*, where a digital good is bought to validate or monetise stolen credentials; (b) *refund and chargeback abuse*, including requests to refund to a different instrument than the one charged; (c) *affiliate payout abuse*, including self-referral, fabricated referrals and payout to an account that does not belong to the affiliate; and (d) *merchandise resale and reshipping*, where physical goods are ordered for onward shipment to a third party or a high-risk jurisdiction.

4.5 Conclusion. The Company's overall inherent exposure to money laundering is assessed as low, and its residual exposure after the controls in clause 5 as low. The assessment is documented, dated and reviewed under clause 11.

05 · Controls operated by the Company

- ◆ **5.1 Every payment corresponds to a real sale.** Each receipt is matched to a specific product, at a stated price, against an order record and an issued licence. There is no facility to accept a payment that is not a purchase, to overpay and request the balance back, or to credit an account for later withdrawal.
- ◆ **5.2 Accepted methods are closed and enumerated.** Card and wallet through Stripe and PayPal, and bank transfer where a processor supports it. Cash, cryptocurrency, gift cards, money orders, third-party cheques and payments from an account in a name unrelated to the customer are not accepted.
- ◆ **5.3 Refunds return to source.** A refund is issued only to the original instrument, for the amount paid, and never redirected to a different card, account or person. A request to do otherwise is treated as a red flag under Annex A.
- ◆ **5.4 Affiliate payouts follow verified sales.** Commission is calculated from actual referred sales, held for a defined clearance period to allow for refunds and chargebacks, and released only to a payout method verified in the affiliate's own name. Payout to a third party, to an unverified account, or in cash is prohibited. Self-referral and fabricated referral result in forfeiture and closure under the [Affiliate Program Terms](#).
- ◆ **5.5 No payment credentials are held.** Card numbers, bank routing and account numbers are never stored in Company systems. Payout details are held by the processor or verified through Plaid; the Company sees a status and a masked reference, not the underlying credential.
- ◆ **5.6 Escalation of unusual activity.** A pattern consistent with structuring, layering, card testing, or an attempt to move value through the platform without a genuine underlying sale is escalated to the relevant processor, and the account, order or affiliate is suspended pending review. The Company does not tip off the subject of such a review beyond telling them their account is suspended.
- ◆ **5.7 Right of refusal.** The Company may decline or reverse any order, cancel any licence and close any affiliate account where it is not satisfied as to the legitimacy of a payment, and is not obliged to explain the decision beyond what law requires.
- ◆ **5.8 Merchandise orders.** Physical orders are shipped to the purchaser's own verified address. Reshipping requests, mismatched billing and shipping jurisdictions, and bulk orders inconsistent with personal use are reviewed before fulfilment.

06 · Sanctions and export controls

6.1 Screening. The Company relies on the sanctions screening performed by its processors at the point of payment, and additionally screens any counterparty it contracts with directly — suppliers, fulfilment partners, contractors and affiliates paid above a nominal threshold — against the OFAC Specially Designated Nationals and Blocked Persons List, the OFAC consolidated non-SDN lists, the UK sanctions list, the EU consolidated list and the Canadian consolidated list.

6.2 The fifty-per-cent rule. An entity owned fifty per cent or more, in aggregate and whether directly or indirectly, by one or more blocked persons is treated as blocked whether or not it is itself listed.

6.3 Comprehensively sanctioned jurisdictions. The Company does not knowingly license, sell, ship or provide support to a person located in a jurisdiction subject to comprehensive U.S. sanctions. Where a licence, download or support request is identified as originating from such a jurisdiction, it is refused and, where already issued, revoked.

6.4 Export control. Company software is supplied consistently with the Export Administration Regulations, 15 C.F.R. Parts 730–774. The Company does not supply, and does not authorise a reseller or affiliate to supply, its products to a party on the Entity List, the Denied Persons List or the Unverified List.

6.5 Blocked property. Where a payment or account is identified as involving blocked property, the Company will freeze rather than return the relevant value, notify its processor, and take instruction from counsel before any disbursement.

07 · Customer and counterparty due diligence

7.1 Retail sales. Identity verification for a card sale is performed by the processor and the issuing bank. The Company does not collect identity documents from retail software customers, and says so rather than implying a verification programme it does not run.

7.2 Affiliates. Affiliates are identified before a first payout: legal name, country, tax status and a payout account verified in the same name. A U.S. affiliate provides a Form W-9; a non-U.S. affiliate provides the applicable Form W-8. Payouts are withheld until verification is complete.

7.3 Suppliers and partners. A direct counterparty is identified to entity level, with beneficial ownership established where the arrangement is material, and screened under clause 6. Payment is made to the contracting entity's own account in the jurisdiction of the contract.

7.4 Enhanced measures. Where a counterparty is connected to a higher-risk jurisdiction, is a politically exposed person, or presents any red flag in Annex A, the Company applies additional enquiry — documented source of funds or business rationale — or declines the relationship.

08 · Roles and responsibilities

8.1 Accountable officer. The Managing Member holds accountability for this policy, is the point of escalation for suspicious activity, and is the signatory for any communication with a processor, bank or authority on a financial-crime matter. The role is not delegated.

8.2 Channel. All financial-crime escalations, internal and external, are directed to legal@erianux.com.

8.3 Future staffing. Any employee or contractor with access to payment dashboards, refund authority or affiliate payout authority will be briefed on this policy and the Annex A red flags before that access is granted, and the briefing recorded.

09 · Reporting suspicion

9.1 Internal. Any person who suspects that a payment, refund, payout or order is connected to criminal property must report it to legal@erianux.com immediately and must not discuss it with the customer.

9.2 External. The Company reports the matter to the processor through which the funds moved, which carries the regulated reporting obligation, and will report directly to law enforcement — the Financial Crimes Enforcement Network, the Internet Crime Complaint Center, the UK National Crime Agency or the relevant national authority — where the circumstances warrant it or where an authority so requests.

9.3 Cooperation and no tipping-off. The Company cooperates fully with lawful requests from processors, regulators and law enforcement, including subpoenas and information orders, and will not alert the subject of an enquiry to its existence where doing so would prejudice an investigation.

10 · Records and retention

The Company retains order and licence records, refund and chargeback records, affiliate verification and payout records, sanctions-screening results for direct counterparties, escalations and their outcomes, and the dated risk assessment. Records are retained for not less than five years from the transaction or the end of the relationship, consistent with the period required of regulated institutions under 31 C.F.R. Chapter X, and are then securely destroyed. Records are produced in response to lawful process.

11 · Review and trigger events

This policy and the underlying risk assessment are reviewed at least annually, and immediately on any of the following: the addition of a payment method, in particular cryptocurrency or direct bank debit; the introduction of any stored balance, credit or wallet feature; the engagement of a reseller or distributor; a change of payment processor; the first employee with payment access; entry into a regulated activity; or any event that would change the Company's status under 31 C.F.R. §1010.100(ff). Each review is logged whether or not the text changes. Should the Company ever become a money services business or other obliged entity, it will register as required and implement a full BSA/AML programme — a written programme, a designated compliance officer, training, independent testing and suspicious-activity reporting — before commencing the activity, not after.

12 · Position on cryptocurrency and alternative value

12.1 Not accepted. The Company does not accept cryptocurrency, stablecoins, tokens, prepaid cards, gift cards, money orders or bearer instruments for any product, and does not pay affiliate commission in any of them.

12.2 Why the exclusion is deliberate. These instruments carry the two characteristics that make a payment useful for laundering: weak linkage between the payer and the funds, and limited reversibility. Excluding them removes a class of risk entirely rather than attempting to monitor it with controls the Company does not have.

12.3 If that changes. Any decision to accept crypto assets is a clause 11 trigger event. Before accepting any such payment the Company would take advice on its status under 31 C.F.R. §1010.100(ff), register if required, and implement blockchain-analytics screening and a written programme — in that order, and before the first transaction.

13 · Tax identification and payout reporting

13.1 Documentation before payment. No affiliate receives a payout until the Company holds the applicable tax documentation: Form W-9 for a U.S. person, or the applicable Form W-8 series certificate for a non-U.S. person. Documentation is collected because the Company must know who it is paying, not merely because the tax code requires it.

13.2 Consistency check. The name on the tax certificate, the name on the payout account and the name on the affiliate application must match. A mismatch stops the payout until it is explained.

13.3 Withholding and reporting. The Company withholds and reports as required by law, including information reporting on affiliate earnings where thresholds are met, and does not structure payouts to fall below a reporting threshold.

14 · Chargebacks, refunds and abuse handling

14.1 Chargeback as a signal. A chargeback is treated as information, not merely as a cost. A cluster of chargebacks sharing a card issuer, a device, an email pattern or an affiliate referral is investigated as a possible fraud pattern and reported to the processor.

14.2 Unauthorised-transaction reports. Where a cardholder reports that a purchase was not made by them, the licence is revoked, the payment is refunded or the chargeback accepted without dispute, and the order is recorded as suspected card fraud. The Company does not contest a genuine unauthorised-use claim in order to protect a revenue figure.

14.3 Licence revocation on reversal. A licence issued against a payment that is later reversed is revoked. This is what makes a stolen-card purchase of a digital good economically pointless, and it is the Company's principal control against that pattern.

14.4 Commission clawback. Commission attributable to a refunded, reversed or fraudulent sale is reversed. An affiliate whose referrals show an anomalous reversal rate is suspended pending review.

14.5 Refund policy is not a laundering channel. Refunds are honoured on their merits under the published terms, to source only, and the Company does not offer a cash, credit-balance or third-party alternative to a refund in any circumstance.

15 · Compensating controls in a single-member business

15.1 The structural weakness, named. Conventional financial-crime control depends on segregation of duties, and a business with one decision-maker cannot segregate them. The Company states this rather than describing an internal control environment it does not have.

15.2 What substitutes for it. Four externally held controls: payment processing through regulated third parties whose records the Company cannot alter; bank and processor statements reconciled by an external accountant; a published, closed list of accepted payment methods that removes discretion at the point of sale; and immutable order, licence and payout records generated by the system rather than entered by hand.

15.3 Independent review. Regulated institutions are required to obtain independent testing of their programme. The Company is not, but treats an annual external review of its reconciliations and of this policy as the substitute for the independence it cannot create internally, and will commission a full independent programme review before entering any regulated activity.

15.4 On first hire. When a person other than the Managing Member gains refund or payout authority, dual authorisation above a set threshold is introduced, and this clause is rewritten to describe genuine segregation rather than compensating controls.

Annex A · Red flags requiring escalation

Any of the following is escalated to legal@erianux.com before the transaction or payout completes: a series of small authorisations in rapid succession across many cards; multiple orders from different cards sharing one email, device or address; a purchase followed immediately by a request to refund to a different instrument; an offer to pay substantially more than the price with a request for the balance to be returned or forwarded; a customer indifferent to the product, its features or its delivery; an affiliate whose referred sales are refunded or charged back at an implausible rate; a payout instruction to a name or jurisdiction unconnected to the affiliate; a supplier invoice payable to a third party or an unrelated jurisdiction; a request to split an invoice to keep each part below a threshold; reluctance to provide basic identifying information for a payout or a supplier contract; and any request to accept cash, cryptocurrency or a gift card for a licence.

Annex B · Version history

VERSION	DATE	CHANGE
1.0	10	
	Sep 2026	First published.
2.0	11	Extended to sanctions and export control; regulatory status reasoned against 31
	Sep 2026	C.F.R. §1010.100(ff) and 31 U.S.C. §5318(h); UK, EU and Canadian frameworks addressed; documented risk assessment with four named higher-risk vectors; payment, refund, payout and merchandise controls; due diligence tiers; reporting, retention and trigger-based review; red-flag annex.

WHY THIS POLICY EXISTS

The Company maintains this policy ahead of any legal requirement to do so. It is a routine request from a bank or processor as transaction volume grows, and a business that has already reasoned through its own position is a better counterparty than one answering the question for the first time when asked. Enquiries from a financial institution, platform or authority may be sent to legal@erianux.com.