Prohibited Jurisdictions and Activities

ArtPay · Last updated 2026-07-07

1. INTRODUCTION AND SCOPE

1.1 Overview. To ensure the integrity, legality, and security of its platform, BUYEASY TECHNOLOGY CO., LTD, a corporation incorporated under the Canada Business Corporations Act (together with its subsidiaries and affiliates, collectively "BUYEASY," "ArtPay," "Company," "we," "us," or "our"), maintains this Prohibited Activities Policy ("Policy"). This Policy sets forth the types of businesses, transactions, jurisdictions, and activities that are prohibited or restricted on the Platform, including the website at https://artpay.co (the "Site"), mobile application (the "App"), and all services provided or facilitated thereby (collectively, the "Platform" or "Services").

1.2 Applicability. This Policy applies to all users, businesses, and transactions conducted on or through the Platform, together with the Terms and Conditions at https://legal.artpay.co/v1/terms-and-conditions. Users are responsible for ensuring that their activities comply with this Policy and all applicable laws and regulations in their respective jurisdictions.

1.3 Scope of Requirements. BUYEASY provides financial services across different currencies and payment rails (including USD and EUR accounts). BUYEASY, together with any custodians or other third parties it engages and the applicable regulators and payment networks, imposes compliance requirements on the use of these services. This Policy consolidates the restrictions applicable across all services to provide a comprehensive and unified compliance framework. Where a restriction applies to a specific service channel, it is noted accordingly.

1.4 Policy Updates. This Policy is subject to change based on regulatory, legal, and operational requirements, including updates from international bodies such as the Financial Action Task Force (FATF), the U.S. Office of Foreign Assets Control (OFAC), the European Union, and other relevant regulatory authorities. We reserve the right to update this Policy at any time without prior notice.

2. PROHIBITED BUSINESS TYPES

2.1 Universally Prohibited Businesses. The following categories of businesses or activities are strictly prohibited from accessing or using the Platform across all service channels: (a) any business engaged in illegal activities

or the sale of illegal products or services under applicable law; (b) production, distribution, or sale of controlled substances without valid licensing from the appropriate governmental authority; (c) human trafficking, forced labor, prostitution, escort services, or similar exploitative businesses; (d) manufacturing, distribution, or sale of counterfeit goods, pirated software, music, movies, or other intellectual property violations; (e) deceptive, misleading, or predatory business models, including pyramid schemes, Ponzi schemes, multi-level marketing schemes, get-rich-quick schemes, or fund aggregation and factoring services; (f) activities involving illegal content, including child sexual abuse materials (CSAM) or any form of exploitation of minors; (g) businesses promoting unlawful violence, terrorism, or extremism; and (h) shell banks or entities designed to obscure the beneficial ownership of funds.

2.2 Prohibited and Restricted Activities by Service Rail. In addition to the universally prohibited categories above, the following business activities are prohibited or restricted depending on the service rail used. Columns identify the applicable rail: Portage, OpenPayd / Clear bank, SSB, or Sutton Bank. A cross ( ) indicates the activity is prohibited on that service rail; a cross with an asterisk (*) indicates it may be permitted only on a case-by-case basis after enhanced due diligence and compliance approval; a blank cell indicates no specific restriction for that rail.

Activity	Portage	OpenPayd / Clear bank	SSB	Sutton Bank
Illegal Drugs & Drug Paraphernalia				
Fraudulent Identification		*		
Telecom Abuse & Cybercrime				
Violence, Human Trafficking & Exploitation		*		
Unlawful Products & Services				
Intellectual Property Infringement				
Unfair, Predatory, or Deceptive Practices				
Adult Content & Services				
Certain Legal Services				
Firearms, Explosives & Dangerous Materials				
Unlicensed Gambling & Cash-Intensive Businesses				
Cannabis & Marijuana				
Sanctions & Licensing Violations				
Money Laundering, Fraud & AML/KYC Control Failures				

Missions, Embassies & Consulates				
Wildlife / Cultural Artefact Trafficking				
Environmental Crime / Repeated Environmental Violations				
Political Fundraising / Campaign Financing				
Digital-Asset / Cryptocurrency Transactions				
Unauthorized Data Collection / Data Brokerage				

3. RESTRICTED BUSINESS ACTIVITIES

3.1 Enhanced Due Diligence. Certain types of businesses may be permitted to use the Platform only after enhanced due diligence and formal approval by the Company's Compliance Team. These include, but are not limited to: (a) money services businesses (MSBs); (b) cryptocurrency exchanges, wallets, brokers, or other digital asset service providers; (c) gambling, betting, fantasy sports, and skill-based gaming platforms; (d) charities, foundations, or other non-profit organizations; (e) adult content services, online tipping, or fan monetization platforms; (f) dealers in precious metals, gems, or high-value commodities; and (g) businesses operating in industries with elevated regulatory or financial crime risk.

3.2 Requirements. Entities in the restricted categories must demonstrate: (a) full licensing and registration with all applicable regulatory authorities; (b) compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) obligations; (c) robust risk management protocols, including customer due diligence programs; (d) audited financial statements or equivalent documentation; and (e) a clean compliance history with no unresolved regulatory actions.

3.3 Ongoing Monitoring. Restricted businesses that are approved for access to the Platform are subject to ongoing monitoring, periodic reviews, and enhanced transaction surveillance. The Company reserves the right to revoke access at any time if compliance standards are not maintained.

4. PROHIBITED TRANSACTIONS AND USAGE

4.1 Prohibited Transactions. The following types of transactions are not permitted on the Platform: (a) purchase or sale of illegal drugs, narcotics, or controlled substances without proper authorization from the relevant governmental

authority; (b) use of stolen, forged, or unauthorized financial instruments, identification documents, or credentials; (c) funding or engagement in cybercrime, malware distribution, hacking services, or dark-web-related payments; (d) purchase, sale, or distribution of weapons, ammunition, or explosives for unauthorized purposes; (e) operation of unlicensed online pharmacies or participation in illicit pharmaceutical trade; (f) unlawful access to, trafficking in, or sale of personally identifiable information (PII) or sensitive data; (g) offering payday loans, high-interest unlicensed lending, or debt collection without applicable licensing and compliance; (h) trade or sale of endangered species or products derived from them; (i) drug-related purchases, including drug paraphernalia and substances mimicking illegal drugs; and (j) any transaction designed to circumvent sanctions, export controls, or other regulatory restrictions.

4.2 Structuring and Evasion. Users are prohibited from structuring transactions to avoid reporting thresholds, circumventing internal controls, or engaging in any activity intended to evade compliance with applicable laws, regulations, or this Policy.

4.3 Sanctions Compliance. Users shall not engage in any transaction or activity involving: (a) individuals or entities designated on sanctions lists maintained by OFAC, the United Nations, or the European Union; (b) individuals or entities owned or controlled by sanctioned parties; or (c) any activity that would cause the Company to violate applicable sanctions laws.

5. GEOGRAPHIC RESTRICTIONS

5.1 Overview. The Company restricts access to its Services in certain jurisdictions subject to sanctions, regulatory restrictions, or elevated financial crime risks. Restrictions vary by service rail. The table below consolidates restricted jurisdictions by rail. Columns identify the applicable rail: Portage, OpenPayd / Clear bank, SSB, or Sutton Bank. A cross ( ) indicates that we are unable to provide that service to the jurisdiction; a cross with an asterisk (*) indicates that the service may be possible on a case-by-case basis after enhanced due diligence and compliance approval; a blank cell indicates no restriction specific to that service rail.

Jurisdiction	Portage	OpenPayd / Clear bank	SSB	Sutton Bank
Afghanistan				
Albania				
Algeria	*			
Angola	*			

Armenia				
Azerbaijan				
Barbados				
Belarus				
Bolivia	*			
Bosnia and Herzegovina				
Botswana				
Bulgaria	*			
Burkina Faso				
Burundi				
Cambodia				
Cameroon	*			
Central African Republic				
China				
Côte d’Ivoire	*			
Cuba				
Cyprus				
Democratic Republic of the Congo (DRC)	*			
Eritrea				
Ethiopia				
Ghana				
Guinea				
Guinea-Bissau				
Haiti	*			
Iran				
Iraq				
Jamaica				
Japan				
Jordan				
Kazakhstan				
Kenya	*			
Kuwait				
Kyrgyzstan				
Laos	*			
Lebanon	*			
Liberia				
Libya				
Mali				
Monaco	*			
Morocco				
Mozambique				
Myanmar (Burma)				

Namibia	*			
Nepal	*			
Nicaragua				
North Korea (DPRK)				
North Macedonia				
Pakistan				
Palestine / West Bank				
Panama				
Papua New Guinea				
Russia				
Saudi Arabia				
Senegal				
Sierra Leone				
Somalia				
Somaliland				
South Sudan	*			
Sudan				
Syria				
Tajikistan				
Tanzania				
Transnistria				
Trinidad & Tobago				
Tunisia				
Turkmenistan				
Uganda				
Ukraine				
United States				
Uzbekistan				
Vanuatu				
Venezuela	*			
Vietnam	*			
British Virgin Islands	*			
Yemen	*			
Zimbabwe				
Any unrecognised or occupied territory (Crimea, Abkhazia, Zaporizhie, South Ossetia, Nagorno-Karabakh, Luhansk (LNR), Donetsk (DNR), Kherson occupied areas, Kosovo)				

—we are unable to provide the service to the jurisdiction. * — the service may be possible on a case-by-case basis after enhanced due diligence and compliance approval. A blank cell indicates no restriction specific to that service rail.

5.2 Ukraine — Specific Regions. For all service channels where Ukraine is listed as restricted, restrictions specifically include the Crimea, Donetsk, and Luhansk regions. Certain service channels may restrict all of Ukraine; others may restrict only these specific regions. Users should contact the Compliance Team for clarification regarding permissible activity involving Ukrainian counterparties.

5.3 Changes to Restricted Jurisdictions. The Company reserves the right to add or remove jurisdictions from this list at its sole discretion, including in response to updates from FATF, OFAC, the European Union, the Central Bank of the UAE, or other relevant regulatory authorities. Users will be notified of material changes to the restricted jurisdictions list through Platform notifications or email.

5.4 User Responsibility. Users are responsible for ensuring that they do not use the Platform in violation of geographic restrictions applicable to their accounts. The Company reserves the right to immediately suspend or terminate any account that is found to be operating from, or facilitating transactions to or from, a restricted jurisdiction.

6. ENFORCEMENT AND MONITORING

6.1 Monitoring. The Company employs automated and manual monitoring systems to detect potential violations of this Policy. Monitoring includes, but is not limited to: (a) transaction monitoring for suspicious activity; (b) sanctions screening of users, counterparties, and transactions; (c) periodic reviews of user accounts and business activities; and (d) analysis of usage patterns for potential circumvention of restrictions.

6.2 Investigation and Remediation. The Company reserves the right to investigate any suspected violation of this Policy. During an investigation, the Company may: (a) suspend the user's account and freeze funds; (b) request additional documentation or information from the user; (c) restrict access to certain features or services; and (d) engage external counsel or forensic specialists as necessary.

6.3 Consequences of Violation. Violations of this Policy may result in: (a) immediate suspension or termination of the user's account; (b) forfeiture of funds in accordance with applicable law and the Company's Terms and Conditions;

(c) reporting to applicable regulatory bodies, law enforcement authorities, or financial intelligence units; and (d) pursuit of civil or criminal remedies as appropriate.

6.4 Cooperation with Authorities. The Company cooperates fully with law enforcement agencies, regulatory authorities, and judicial bodies in connection with investigations of violations of this Policy, applicable laws, or regulations. The Company shall provide information as required by lawful requests, court orders, and regulatory inquiries.

7. USER OBLIGATIONS

7.1 Compliance. Users are required to: (a) comply with this Policy and all applicable laws and regulations; (b) provide accurate and complete information to the Company during onboarding and throughout the relationship; (c) promptly notify the Company of any changes to their business activities, ownership structure, or regulatory status; and (d) cooperate with the Company's compliance inquiries and requests for information.

7.2 Reporting. Users who become aware of any activity on the Platform that may violate this Policy are encouraged to report such activity to the Compliance Team at legal@artpay.co. Reports may be made confidentially.

8. CONTACT INFORMATION

Compliance Inquiries:

Email: legal@artpay.co

General Support:

Email: support@artpay.co

For questions regarding permitted business models, specific service channel restrictions, or compliance inquiries, please contact the BUYEASY TECHNOLOGY CO., LTD. Compliance Team using the contact information above.