AML CTF Policy

BC FINANCE LTD

Version: 1.7
Last Updated: 06.09.2024

Anti-Money Laundering and Counter-Terrorist Financing Policy

1. INTRODUCTION

The NinjasPay AML Policy is designed to prevent money laundering by meeting the UK and European standards on combating money laundering and terrorism financing, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime.

It is prohibited to provide any product or service or process any transaction for the benefit of individual or entity included in the international sanctions lists. As such, the adherence with applicable laws and regulations in relation to prevention of money laundering and terrorist financing, in particular the Anti-Money Laundering Regulation (AMLR) and the Anti-Money Laundering Directive (AMLD6), (hereinafter referred to as "AML") is mandatory and fundamental to NinjasPay strategy and program.

NinjasPay has strict and transparent standards and continuously strengthens its processes so as to ensure compliance with applicable AML laws and regulations.

NinjasPay reserves the right to reject any customer, payment or business that is not consistent with the NinjasPay AML policy, irrespective of the requirements of the applicable AML laws and regulations.

2. MAIN OBJECTIVES

- Combating and preventing money laundering and terrorist financing and taking all the necessary preventive measures;
- Preventing the misuse of the Company by anyone or anybody in illegitimate operations;
- Appointing a Money Laundering Reporting Officer (MLRO) who has a sufficient level of seniority and independence, and who has responsibility for oversight of compliance with the relevant legislation, regulations, rules and industry guidance;
- Establishing and maintaining a Risk-Based Approach (RBA) to the assessment and management of money laundering and terrorist financing risks faced by the firm;
- Establishing and maintaining risk-based Customer Due Diligence (CDD), identification, verification and Know Your Customer (KYC) procedures, including enhanced due diligence for customers presenting a higher risk, such as Politically Exposed Persons (PEPs);
- Establishing and maintaining risk-based systems and procedures for the monitoring of on-going customer activity;
- Establishing procedures for reporting suspicious activity internally and to the relevant law enforcement authorities;
- Maintaining appropriate records for the minimum prescribed periods;
- Training all employees on the rules and internal procedures which have to be observed, the risks that they and the Company face and how they can encounter

the risks of money laundering and terrorist financing through their operations from their positions.

3. COMPANY COMMITMENT

NinjasPay is committed to:

- Accept only those Customers whose identity can be established and verified and whose source of funds can be reasonably established to be legitimate;
- Not establish a business relationship, open accounts or maintain accounts for anonymous persons or those with fictitious names including anonymous accounts;
- Make every possible effort to know the identity of the customer and the real beneficiary (Beneficiary Owner) of the account (i.e. the full name, the place and date of birth and verifying the identity by using valid, official and accredited documents “identification data” issued by the official bodies), in addition to the data and information available from trusted independent sources;
- Apply a risk-based approach, and enhanced customer due diligence where required;
- Monitor and identify suspicious transactions and activities and ensure that reportable ones get reported;
- Provide regular and appropriate AML / CTF training and information to all employees to increase their awareness using various methods;
- Maintain records, which are appropriate to the nature and complexity of the customer’s business.

4. CUSTOMER DUE DILIGENCE

In terms of its obligations at law, NinjasPay is obliged to determine the applicant for business, the Customer or any beneficial owner, and to verify that such person is the person he purports to be, as well as to determine whether such person is acting on behalf of someone else, and to establish the purpose and intended nature of the business relationship and to monitor this relationship on an ongoing basis. In order to successfully adhere to its obligations, NinjasPay has developed Customer due diligence (“Due Diligence”) measures which must be implemented by NinjasPay and adhered to by its management and employees.

The Due Diligence measures assist NinjasPay in determining whether a particular Customer falls within their risk appetite, as well as helps the Company clearly understand the business activities of the Customer in such a way that any transactions which fall outside the business profile of the company may be investigated to determine whether any money laundering or funding of terrorism may be involved. This enables the Company to inform relevant authorities in a timely manner with adequate information on its Customer and their activities when such a request is made.

In summary, NinjasPay has adopted its Due Diligence policies in order to successfully carry out the following:

- identification and verification of the applicant for business

- identification and verification of the beneficial owner, where applicable
- identification and verification when the applicant for business does not act as principal
- obtaining information on the purpose and intended nature of the business relationship
- conducting ongoing monitoring of the business relationship
- establishing the source of wealth and source of funds
- setting up of a Customer acceptance policy and ensuring that the applicant for business meets the requirements set out in such policy
  NinjasPay is strictly prohibited from keeping anonymous accounts or accounts in fictitious names.

4.1. Prohibitions

NinjasPay has no AML risk appetite for customers who engage in any of the following activities:

- intentional or willfully negligent breaches of law, regulation or policy applicable to money laundering and terrorist financing risk;
- repeated unintentional or repeated accidental breaches of AML laws;
- misusing the account for the purpose of money laundering or terrorism financing;
- misusing the account for the purpose of other fraud;
- facilitating business activities which could be construed as a tax offence;
- refusing to provide sufficient information or documentation to demonstrate compliance with the standards outlined in NinjasPay AML policy.

The Company has no risk appetite for customers or transaction to or from jurisdictions which are identified as high-risk third countries on the lists of jurisdictions having serious deficiencies in their anti-money laundering regimes drawn up by the European Commission and the FATF and as amended from time to time, including but not limited, onboarding clients from or executing transaction to or from:
Afghanistan, Belarus, Burundi, Central African Republic, Democratic Republic of the Congo, Crimea Region, Cuba, Guinea, Guinea-Bissau, Haiti, Iran, Iraq, Democratic People's Republic of Korea, Lebanon, Libya, Mali, Myanmar, Nicaragua, Palestine, Russian Federation, Yemen, Somalia, South Sudan, Sudan, Syrian Arab Republic, Venezuela, Western Sahara.

NinjasPay intends to conduct business only with reputable customers who use their own products, services, and related accounts for legitimate purposes, and whose identities can be determined and verified. In keeping with that principle, the Company will not knowingly conduct business with customers that seek to process payments through the Company involving:

- **Sanctioned Entities:** Individuals or organizations on the United Nations, US OFAC, European Union, and UK HMT sanctions lists.
- **Unregulated Financial Services:** Including loan lenders, payday loan companies, and debt collection agencies.
- **Equity and Investment Funds:** Including mutual funds and similar entities.
- **Initial Coin Offering (ICO)**: Providers linking coins to shares or prepayment methods.
- **Speculative Mini-Bonds:** High-risk financial instruments.
- **Holding/Shell Companies:** Entities solely operating other subsidiaries.

- **Unregulated Funds:** Such as venture capital and similar investment vehicles.
- **Unregulated Forex Trading**
- **Pyramid or Ponzi schemes**
- **Special Purpose Vehicles (SPVs)**: Entities created for specific financial purposes.
- **Unregulated Custodial Wallets:** Providers lacking regulatory compliance.
- **Unregulated Crypto ATM Operators**: Providing cash-to-crypto exchange services without proper oversight.
- **Unregulated Cryptocurrency Providers:** Including brokers, exchanges, and mining services.
- **Unregulated Crypto Companies:** Businesses focused on crypto mining, investment, or trading.
- **Ramp-Up/Ramp-Down Service**s: Providers facilitating fiat-to-crypto exchanges.
- **Unlicensed lottery and gambling operations**
- **Digital Games:** Merchants distributing game keys and in-app purchases without proper licensing.
- **Sexual Services:** Any services associated with prostitution or escort services.
- **Dating Services:** Apps and matchmaking sites, including coaching and advice.
- **Adult Entertainment Services:** Any services sold or provided in-person.
- **Unregulated Medical Services:** Including Botox, acupuncture, and tattooing.
- **Invasive Medical Devices:** Non-compliant surgical tools, including needles and scalpels.
- **Alternative Medicines:** Including homeopathy and unregulated therapies.
- **Cannabinoids:** Products containing THC, CBD, and CBN without proper licensing.
- **Fake Goods:** Counterfeit consumer products.
- **Nicotine and Tobacco Products:** Including cigarettes, cigars, e-cigarettes, and vape liquids.
- **Non-Licensed Resellers:** Aftermarket goods without proper licensing.
- **Non-Licensed Branded Merchandise:** Unauthorized sales of branded products.
- **High-Value Online Reselling:** Products lacking quality certification (e.g., Rolex watches, limited edition sneakers).
- **Stolen Goods**: Including digital and virtual goods (fictitious social media likes, spam emails).
- **Illicit Drugs:** Including prescription drugs sold without licenses and illegal substances.
- **Precious Metals and Stones**: Extraction and trading activities without proper licensing.
- **Sale of government IDs or documents**
- **Multi-Level Marketing:** Products not sold directly by manufacturers, often using recruitment tactics.
- **Data Protection Violations:** Transaction activities displaying personal information against applicable laws (e.g., GDPR).
- **Political Organizations:** Any involvement in political activities.
- **Unregistered Charitable Foundations:** Non-compliant charitable entities.
- **Unregistered Non-Profit Organizations:** Charities lacking legal registration.
- **Cyberlocker Services:** File sharing and hosting platforms without proper licensing.
- **Chemicals:** Hazardous chemicals and allied products without proper licensing and safety measures.

Please note that the company may suspend or terminate business relationship with the customer subject to the requirements of applicable AML laws and regulations.

4.2. Sanctions

NinjasPay has no AML Risk Appetite for establishing or maintaining a customer or a counterparty relationship with a natural person or legal entity designated on any of the below lists or where otherwise prohibited by applicable law or regulation:

- the United Nations Security Council Sanctions List (UN);
- the Consolidated List of European Union Financial Sanctions (EU);
- the United Kingdom Sanctions List (UK)
- sanction lists administered by the United States Office of Foreign Assets Control (OFAC),
- including the List of Specially Designated Nationals and Blocked Persons;
- any other sanctions list.

In addition, NinjasPay pays particular attention to entities from countries which are on the list of noncooperative countries and territories drawn up by the Financial Action Task Force (FATF) and to monetary operations or transactions performed by or on behalf of them.

5. MONITORING FOR SUSPICIOUS ACTIVITY

NinasPay AML policy includes customer's and beneficial owner's due diligence and ongoing AML monitoring and AML reporting policies. At various points in time, NinasPay may request information regarding the transactions carried out through the customer's account opened at NinasPay and the parties of the respective payment. If the customer may not respond sufficiently or within a timely manner, NinasPay also reserves the right to reject any respective payments subject to the requirements of the applicable AML laws and regulations.