Policy Name	Customer Identification Program (CIP)
Responsible Party	David Trost
Contact	support@compto.com
Status	Under Review
Effective Date	March 1, 2025
Revision Date	February 2025

Compto Public Benefit Corporation Customer Identification Program (CIP): Compliance and Supervisory Procedures

1. Introduction and Purpose

a. Background and Regulatory Basis

Compto Public Benefit Corporation ("the Company") is committed to preventing the use of its services for money laundering, terrorist financing, or other illicit activities. In compliance with 31 CFR 1022.210 (the "AML Laws"), and as part of our broader Anti-Money Laundering (AML) Program, Compto has established this Customer Identification Program (CIP).

The CIP outlines how Compto will:

1. Collect required customer identification information;
2. Verify the identity of customers using documentary and non-documentary methods;
3. Maintain clear records of both identification data and verification procedures; and
4. Compare customer information with government watchlists (as necessary).

b. Alignment With AML Program

The CIP is a critical component of the Company's larger AML Policy and program, as outlined in the Compto Public Benefit Corporation Anti-Money Laundering (AML) Program: Compliance and Supervisory Procedures ("AML Documentation"). This CIP directly supports the Know Your Customer (KYC) and compliance controls required by our AML Policy.

2. Scope and Applicability

a. Covered Products and Services

The CIP applies to all new customer relationships or accounts established with the Company, whether directly or through electronic channels, as well as to existing customers

whose information merits ongoing verification.

b. Individuals and Entities

The CIP covers Individuals (U.S. and non-U.S. persons) and Legal Entities, including corporations, partnerships, trusts, and other organizational clients

c. Exemptions

Any potential exemptions or special considerations (e.g., reliance on another financial institution's CIP for certain products) must be evaluated and approved by the Company's AML Compliance Officer.

3. Customer Identification Requirements

a. Required Customer Information

Pursuant to Section 5(a) of the AML Documentation, the following minimum identifying information must be collected before opening an account or establishing a relationship:

1. Full Legal Name
2. Date of Birth (for individuals)
3. Address
    - Residential or business street address (for individuals)
    - Principal place of business, local office, or other physical location (for non-individuals)
4. Government-Issued Identification Number
    - U.S. persons: Taxpayer Identification Number (TIN)
    - Non-U.S. persons: One or more of the following: Passport number and country of issuance, alien identification card number, or any other government-issued document evidencing nationality/residence and bearing a photograph or similar safeguard

b. Customers Who Refuse to Provide Information

If a customer refuses to provide the required CIP information or appears to have intentionally provided misleading data: The account will not be opened (for new customers), or the existing account may be closed after consulting with the AML Compliance Officer.

Additionally, we will assess whether a Suspicious Activity Report (SAR-SF) should be filed (see AML Documentation, Section 9).

4. Methods of Verification

a. Documentary Verification

Where feasible, the Company will verify identity using unexpired, government-issued identification documents that bear a photograph or similar safeguard (e.g., driver's license or passport). For legal entities, we may use certified articles of incorporation, a government-issued business license, or a partnership agreement (AML Documentation, Section 5(c)).

b. Non-Documentary Verification

In situations where valid documentary evidence is unavailable or insufficient, we will employ one or more of the following non-documentary methods to ensure a reasonable belief of the customer's true identity (AML Documentation, Section 5(c)):

1. Contacting the customer directly via phone or email
2. Comparing information against external databases (consumer reporting agencies, public records)
3. Checking references from other financial institutions
4. Requesting a financial statement

c. Enhanced Due Diligence (EDD)

For higher-risk entities and situations—such as foreign legal entities, politically exposed persons (PEPs), or jurisdictions designated as non-cooperative—additional steps may include:

1. Beneficial Ownership Verification (collecting and verifying information on the ultimate owners).
2. Third-Party Verification (using independent services to confirm registration status).
3. Additional Financial Documentation (e.g., recent audited financial statements).

5. Handling Discrepancies and Inability to Verify

If we cannot form a reasonable belief regarding a customer's identity (AML Documentation, Section 5(d)), the Company may:

1. Refuse to open the account;
2. Restrict account activity while verification is pending;
3. Close the account; and/or
4. File a Suspicious Activity Report (SAR-SF) if necessary.

Any decision under this section requires notification of and approval by the AML Compliance Officer.

6. Recordkeeping

a. Types of Records

We will maintain detailed records on:

1. All identifying information obtained from the customer (e.g., names, addresses, ID documents).
2. Verification methods and results (whether documentary or non-documentary).
3. Descriptions of any substantive discrepancy and how it was resolved.

b. Retention Period

Identity Verification Records: At least five (5) years after the account is closed.

Supporting Documentation (e.g., internal forms, verification steps): At least five (5) years after the record is made (AML Documentation, Section 5(e)).

7. Comparison With Government Lists

a. OFAC and Other Watchlists

As outlined in AML Documentation, Section 4 and Section 5(f), Compto checks new customers and periodically screens existing customers against: The Office of Foreign Assets Control (OFAC) Specifically Designated Nationals (SDN) List and other government or law enforcement lists as designated by the Treasury or federal regulators.

b. Procedures for Matches

If a potential match is found:

1. Consult the AML Compliance Officer.
2. Block transactions or freeze the account if required by OFAC or other federal directives.
3. File any required forms (e.g., Blocked Assets or Rejected Transaction form with OFAC).

8. Reliance on Third Parties

a. Conditions for Reliance

Under certain circumstances, the Company may rely on another financial institution's CIP to verify a customer's identity (AML Documentation, Section 5(h)). This is permissible only if:

1. Such reliance is reasonable given the specific circumstances.
2. The other institution is subject to AML compliance requirements and is regulated by a federal functional regulator.
3. The other institution contractually agrees to certify annually that it has an AML program and will perform specified CIP requirements.

b. Documentation

Any reliance arrangement must be documented via a written agreement and approved by the AML Compliance Officer.

9. CIP Notice to Customers

In accordance with Section 5(g) of the AML Documentation, we will provide all new customers with a CIP Notice explaining that we will request identifying information to verify their identity. This notice is prominently displayed on our website, mobile application, and as part of the account opening process.

Sample CIP Notice:

Important Information About Procedures for Opening a New Account

> To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.
>
> What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

10. Training and Awareness

All relevant personnel receive initial and ongoing training on the Company's CIP requirements. This training is part of Compto's broader AML training program (AML Documentation, Section 12). Training topics include:

1. Identifying red flags during the customer onboarding process

2. Proper handling of identity documents and verification results
3. Escalation procedures when CIP requirements are not met

Records of training completion, including dates and attendee lists, are maintained by the AML Compliance Officer or a designee.

11. Monitoring, Reporting, and Updates

a. Monitoring CIP Effectiveness

The AML Compliance Officer will periodically review the CIP's effectiveness, including:

1. Random checks of new account files
2. Verification of CIP record completeness
3. Assessment of third-party reliance agreements (if any)

b. Reporting to Senior Management

Findings and potential improvements are summarized annually (at minimum) and presented to senior management, as part of the broader AML review process.

c. Ongoing Updates

The CIP will be updated to reflect changes in:

1. Regulatory requirements
2. Compto's business model, products, or services
3. Industry best practices

All updates must be approved by the AML Compliance Officer and communicated to affected employees.

12. Approval and Governance

I have reviewed and approved this CIP as reasonably designed to achieve and monitor Compto Public Benefit Corporation's compliance with the identification and verification requirements under the AML Laws.

Signed: Name: David Trost Title: AML Compliance Officer Date:

Revisions

Revision	Revision Date	Description of Changes	Approved By
v1.0	January 2025	Initial Release	David Trost

Revision	Revision Date	Description of Changes	Approved By
v1.1	February 2025	Switch to md, add revisions	

Appendix A: Quick Reference Checklist

Collect Required Information

- Full Name
- Date of Birth (for individuals)
- Address (residential or business)
- Government-issued ID number (TIN, passport, etc.)

Verify Identity

- Documentary verification (driver's license, passport, etc.)
- Non-documentary verification (database checks, references)

Recordkeeping

- Maintain records of identification and verification for 5 years from account closure.

Watchlist Screening

- Check against OFAC SDN list and other government lists.

Approval / Escalation

- AML Compliance Officer to approve deviations.
- Escalate suspicious refusals or discrepancies for possible SAR-SF filing.