
Customer Due Diligence

Customer Identification Unit

Access Control

Related terms: Authentication, Authorization, Role-Based Access, Segregation of Duties

Definition: A set of policies and technical measures that restricts who can view or modify information within the Customer Identification Unit (Customer Identification Unit) and other CDD systems. Access control ensures that only authorized personnel can perform identity verification, update risk profiles, or approve exceptions.

Example: A compliance officer is granted read-only access to client records, while a senior analyst receives edit rights to approve high-risk customer onboarding.

Practical application: Implementing multi-factor authentication and role-based permissions reduces the chance of unauthorized data alteration.

Challenges: Balancing stringent controls with operational efficiency; regularly reviewing access rights as staff change roles.

Beneficial Owner

Related terms: Ultimate Owner, Shareholder, Ownership Structure, Transparency

Definition: The natural person who ultimately owns or controls a legal entity, either directly or indirectly, and who benefits from the entity's assets. Identifying the beneficial owner is a core requirement of the Customer Identification Unit to prevent hidden ownership used for illicit purposes.

Example: A shell company listed as the client may be owned 60% by an individual who is the true beneficial owner.

Practical application: Collecting ownership charts, shareholder registers, and passport copies to map control layers.

Challenges: Complex corporate structures, nominee shareholders, and jurisdictions with limited public registries can obscure true ownership.

Customer Due Diligence (CDD)

Related terms: Risk Assessment, KYC, Enhanced Due Diligence, Ongoing Monitoring

Definition: The process of collecting and evaluating information about a customer to determine their risk profile and to comply with anti-money-laundering (AML) regulations. The Customer Identification Unit is the operational hub where CDD data is gathered, verified, and stored.

Example: Before opening an account, a bank gathers identity documents, source-of-funds statements, and conducts watchlist screening.

Practical application: Using a risk-based approach to allocate resources—low-risk customers receive standard checks, while high-risk customers undergo deeper investigation.

Challenges: Maintaining data accuracy over time, integrating disparate data sources, and meeting differing

regulatory expectations across jurisdictions.

Customer Identification Unit (CIU)

Related terms: CDD Platform, Identity Verification, Compliance Hub, Data Repository

Definition: A dedicated functional area within a financial institution responsible for collecting, verifying, and maintaining customer identity information. The CIU orchestrates the flow of data from front-office onboarding, through verification engines, to risk-assessment modules, ensuring compliance with AML and counter-terrorism financing (CTF) obligations.

Example: When a new corporate client is onboarded, the CIU validates the entity's registration documents, confirms the beneficial owners, and cross-checks the data against sanctions lists.

Practical application: Centralizing identity data enables consistent application of risk models, facilitates rapid updates when regulatory changes occur, and supports audit trails for regulators.

Challenges: Integrating legacy systems, safeguarding sensitive personal data, and scaling processes to handle high-volume onboarding without compromising quality.

Customer Identification Program (CIP)

Related terms: CIU, Regulatory Requirements, Verification Procedures, Risk Management

Definition: A set of policies and procedures that a financial institution must implement to verify the identity of customers as part of AML compliance. The CIP is executed by the Customer Identification Unit and includes document collection, electronic verification, and record-keeping.

Example: A bank requires a new retail client to present a government-issued ID, a utility bill for address verification, and conducts a database check for known fraud indicators.

Practical application: Automating CIP steps with digital identity verification tools reduces onboarding time while maintaining compliance.

Challenges: Keeping pace with evolving identity-verification technologies and ensuring that automated decisions can be reviewed by human analysts when needed.

Data Quality Management

Related terms: Data Governance, Data Cleansing, Master Data Management, Accuracy

Definition: The systematic processes for ensuring that the information stored in the Customer Identification Unit is accurate, complete, and up-to-date. High data quality is essential for reliable risk scoring and regulatory reporting.

Example: Periodic batch jobs compare stored customer addresses against national postal databases and flag mismatches for review.

Practical application: Deploying data-validation rules at entry points prevents common errors such as transposed numbers or misspelled names.

Challenges: Reconciling conflicting data from multiple sources, handling legacy records, and managing data privacy constraints.

Enhanced Due Diligence (EDD)

Related terms: High-Risk Customer, Beneficial Owner, Ongoing Monitoring, Risk Mitigation

Definition: A deeper level of investigation applied to customers who present a higher risk of money laundering or terrorist financing. The Customer Identification Unit initiates EDD when risk indicators such as PEP status, complex ownership structures, or high-value transactions are detected.

Example: A politically exposed person from a high-risk jurisdiction requires source-of-wealth documentation, third-party references, and more frequent transaction reviews.

Practical application: EDD findings are documented in a dedicated risk file that is reviewed by senior compliance officers.

Challenges: Collecting sufficient evidence without imposing undue burden on legitimate customers, and maintaining proportionality in line with regulatory expectations.

Financial Crime

Related terms: Money Laundering, Terrorist Financing, Fraud, Corruption

Definition: Illegal activities that involve the misuse of financial systems for personal or organizational gain. The Customer Identification Unit serves as a frontline defense by ensuring that customers are properly identified before they can access the financial system.

Example: A criminal group attempts to launder proceeds through a series of shell companies; early identification of the beneficial owners can disrupt the scheme.

Practical application: Integrating transaction monitoring with CIU data enables early detection of suspicious patterns.

Challenges: Rapidly evolving tactics, cross-border coordination, and limited resources for comprehensive investigations.

Know Your Customer (KYC)

Related terms: CDD, Customer Identification, Risk Assessment, Verification

Definition: The collective set of procedures used to verify the identity of customers, understand the nature of their activities, and assess potential risks. KYC is the practical implementation of the policies overseen by the Customer Identification Unit.

Example: Collecting a passport, a recent utility bill, and a signed declaration of the purpose of the account.

Practical application: Digital KYC platforms can capture images of documents, perform optical character recognition, and instantly compare data against watchlists.

Challenges: Balancing thoroughness with user experience, especially for mobile-first customers.

Legal Entity Identifier (LEI)

Related terms: Global Identifier, Ownership Transparency, Regulatory Reporting, Beneficial Owner

Definition: A unique 20-character alphanumeric code assigned to legal entities that engage in financial transactions. The Customer Identification Unit uses the LEI to quickly retrieve public information about a client's registration and ownership.

Example: A multinational corporation's LEI is used to cross-reference its filings in the Global LEI System.

Practical application: LEI integration simplifies compliance with reporting standards such as the European Market Infrastructure Regulation (EMIR).

Challenges: Keeping LEI data synchronized with internal records and handling entities that have not yet obtained an LEI.

Money Laundering

Related terms: AML, Layering, Placement, Integration, Financial Crime

Definition: The process of disguising the origins of illicit funds to make them appear legitimate. Effective CDD, managed by the Customer Identification Unit, is essential to interrupt the placement and layering stages.

Example: A criminal deposits cash into a bank, then transfers the funds through multiple accounts to obscure the source.

Practical application: Monitoring for rapid movement of funds shortly after account opening can reveal placement activity.

Challenges: Detecting sophisticated laundering schemes that use multiple jurisdictions and complex corporate structures.

Negative News Screening

Related terms: Media Monitoring, Watchlist Screening, Reputation Risk, Adverse Media

Definition: The process of scanning public and proprietary news sources for adverse information about a customer or beneficial owner. The Customer Identification Unit incorporates negative-news results into the risk assessment.

Example: An article links a client's director to a fraud investigation; the CIU flags the record for further review.

Practical application: Automated feeds from reputable media databases provide real-time alerts.

Challenges: Filtering false positives, language barriers, and ensuring the relevance of older news items.

Ongoing Monitoring

Related terms: Transaction Surveillance, Risk Refresh, Periodic Review, Alert Management

Definition: Continuous assessment of a customer's activity and risk profile after initial onboarding. The Customer Identification Unit updates risk scores based on transaction patterns, changes in ownership, or new regulatory findings.

Example: A client who previously was low-risk starts receiving large, cross-border wire transfers; the CIU triggers a review.

Practical application: Rule-based engines automatically adjust risk levels and generate alerts for compliance analysts.

Challenges: Managing alert fatigue, ensuring timely review of high-volume alerts, and integrating new data sources without overloading the system.

Politically Exposed Person (PEP)

Related terms: Senior Government Official, Relatives and Close Associates, Risk Indicator, Enhanced Due Diligence

Definition: An individual who holds or has held a prominent public function, or their immediate family

members and close associates. PEP status raises the risk profile in the Customer Identification Unit and often triggers EDD.

Example: A former minister who now serves on the board of a private firm is identified as a PEP.

Practical application: Maintaining an up-to-date PEP database and automatically flagging any matches during onboarding.

Challenges: Determining the relevance of distant relatives, handling changes in political status, and complying with jurisdiction-specific definitions.

Risk Assessment

Related terms: Risk Scoring, Threat Modeling, Risk Appetite, Mitigation Strategies

Definition: The systematic evaluation of the likelihood and impact of potential financial-crime exposure posed by a customer. The Customer Identification Unit applies risk-assessment models to assign a rating that drives the depth of due-diligence procedures.

Example: A high-volume, cross-border client from a sanctioned country receives a high risk score and is subject to EDD.

Practical application: Using a weighted scoring matrix that incorporates geography, product type, transaction volume, and PEP status.

Challenges: Avoiding over-reliance on static scores, ensuring models are calibrated to emerging threats, and maintaining transparency for regulators.

Sanctions Screening

Related terms: OFAC List, UN Consolidated List, Embargoed Parties, Compliance Blocklist

Definition: The process of comparing customer names and identifiers against official sanctions lists to prevent prohibited transactions. The Customer Identification Unit performs initial and periodic sanctions checks as part of CDD.

Example: A client's name matches an entry on the U.S. Treasury's Specially Designated Nationals (SDN) list; the CIU blocks the account.

Practical application: Real-time screening during onboarding and batch screening for existing customers.

Challenges: Managing false positives due to common names, handling name variations across languages, and keeping watchlists up-to-date.

Source of Funds (SOF)

Related terms: Source of Wealth, Financial Transparency, Transaction Justification, Risk Indicator

Definition: The origin of the money used to fund a particular transaction or account. Verifying SOF is a key step for the Customer Identification Unit to assess legitimacy.

Example: A client provides a salary slip, tax return, and loan agreement to prove the source of a large deposit.

Practical application: Collecting supporting documents and cross-checking with known income profiles for the customer's occupation.

Challenges: Determining adequacy of documentation, dealing with informal economies, and balancing

privacy concerns.

Transaction Monitoring

Related terms: Suspicious Activity Reporting (SAR), Alert Generation, Behavioral Analytics, Real-Time Screening

Definition: Ongoing analysis of customer transactions to detect patterns that may indicate money laundering or other illicit activity. The Customer Identification Unit integrates monitoring outputs with risk scores to prioritize investigations.

Example: A sudden surge of high-value international wire transfers from a newly opened account triggers an alert.

Practical application: Deploying machine-learning models that adapt to evolving transaction behaviors.

Challenges: Reducing false positives, ensuring scalability, and aligning alerts with regulatory thresholds.

Unusual Transaction

Related terms: Anomaly Detection, Red Flag, Suspicious Activity, Transaction Pattern

Definition: A transaction that deviates significantly from a customer's normal behavior or from typical market practices, warranting further review. The Customer Identification Unit flags such transactions for analyst assessment.

Example: A retail client who usually conducts small domestic purchases suddenly initiates a multi-million offshore transfer.

Practical application: Setting dynamic thresholds based on historical activity and sector benchmarks.

Challenges: Differentiating genuine business needs from illicit motives, and avoiding unnecessary disruption for legitimate customers.

Verification Source

Related terms: Primary Document, Secondary Document, Third-Party Data, Authentication Provider

Definition: The origin of data used to confirm a customer's identity, such as government databases, credit bureaus, or biometric services. The Customer Identification Unit records the verification source to satisfy audit requirements.

Example: Using a national ID database to validate the authenticity of a passport scan.

Practical application: Prioritizing high-confidence sources (e.g., live facial recognition) over low-confidence ones (e.g., self-certified documents).

Challenges: Access restrictions, data latency, and varying reliability across jurisdictions.

Watchlist Screening

Related terms: Sanctions List, PEP List, Adverse Media, Risk Database

Definition: The systematic comparison of customer names against curated lists of individuals and entities that pose a compliance risk. The Customer Identification Unit conducts watchlist screening at onboarding and on a periodic basis.

Example: Matching a client's name against the United Nations Security Council sanctions list and flagging a potential hit.

Practical application: Employing fuzzy-matching algorithms to capture variations in spelling and transliteration.

Challenges: Managing high hit rates in common-name scenarios, ensuring timely updates, and documenting resolution steps for regulators.

Anti-Money Laundering (AML) Framework

Related terms: CDD, SAR, Regulatory Compliance, Risk Management

Definition: The collection of policies, procedures, and controls that an organization implements to detect, prevent, and report money-laundering activities. The Customer Identification Unit is a central component of the AML framework, handling identity verification and risk profiling.

Example: A bank's AML program outlines the steps for customer onboarding, ongoing monitoring, and reporting suspicious activity.

Practical application: Aligning CIU processes with the three-tiered AML approach (preventive, detective, corrective).

Challenges: Keeping pace with regulatory changes, integrating AML functions across business lines, and measuring effectiveness.

Beneficial Ownership Register

Related terms: Corporate Registry, Transparency Initiative, Ownership Disclosure, CIU Data Store

Definition: A publicly accessible database that records the natural persons who ultimately own or control a legal entity. The Customer Identification Unit references the register to verify the declared beneficial owners during onboarding.

Example: Consulting a national beneficial-ownership register to confirm that a listed director holds a 45 % stake in the client company.

Practical application: Automating API calls to the register for real-time verification.

Challenges: Incomplete coverage in some jurisdictions, data quality issues, and differing legal definitions of "control".

Compliance Audit Trail

Related terms: Record Keeping, Documentation, Regulatory Inspection, CIU Log

Definition: A chronological record of all actions taken within the compliance process, including data collection, verification decisions, and risk-assessment updates. The Customer Identification Unit maintains an audit trail to demonstrate adherence to AML and KYC regulations.

Example: A log entry shows that on 2024-05-12 the analyst approved an EDD file after reviewing supporting documents.

Practical application: Using immutable storage solutions to ensure tamper-evidence and easy retrieval during regulator examinations.

Challenges: Managing storage volume, ensuring privacy compliance, and providing searchable access for auditors.

Data Privacy

Related terms: GDPR, Personal Data, Confidentiality, Consent Management

Definition: The set of legal and operational requirements governing the collection, processing, and storage of personal information. The Customer Identification Unit must balance AML obligations with data-privacy rules to protect customer rights.

Example: Obtaining explicit consent before storing biometric data used for identity verification.

Practical application: Implementing data-minimization principles—collect only the information necessary for risk assessment.

Challenges: Reconciling conflicting mandates (e.g., AML data retention vs. GDPR right-to-erasure) and ensuring cross-border data transfers meet legal standards.

Electronic Identity Verification (eIDV)

Related terms: Digital KYC, Biometric Authentication, Document Validation, CIU Automation

Definition: The use of electronic tools and services to confirm a customer's identity remotely, often leveraging OCR, facial recognition, and database checks. The Customer Identification Unit integrates eIDV solutions to streamline onboarding and reduce manual effort.

Example: A client uploads a passport image; the system extracts data, validates the MRZ, and matches the selfie to the passport photo.

Practical application: Deploying eIDV for non-face-to-face onboarding in digital-only banking channels.

Challenges: Ensuring accuracy across document types, handling failures gracefully, and meeting regulatory acceptance criteria for electronic verification.

Financial Action Task Force (FATF)

Related terms: AML Standards, Recommendations, Global Compliance, Risk-Based Approach

Definition: An intergovernmental body that sets international standards to combat money laundering and terrorist financing. The Customer Identification Unit aligns its policies with FATF Recommendations, especially those concerning customer identification and risk assessment.

Example: FATF's "Risk-Based Approach" guidance informs the CIU's methodology for assigning risk scores.

Practical application: Conducting periodic gap analyses to ensure CIU processes meet FATF expectations.

Challenges: Interpreting ambiguous recommendations, adapting to evolving FATF guidance, and implementing standards across diverse jurisdictions.

Risk-Based Approach (RBA)

Related terms: Proportionality, Risk Appetite, Tiered Due Diligence, CIU Strategy

Definition: A methodology that allocates resources and scrutiny according to the assessed risk level of each customer. The Customer Identification Unit employs RBA to determine whether standard CDD, enhanced due diligence, or ongoing monitoring is required.

Example: Low-risk retail customers undergo automated checks, while high-risk corporate clients receive manual review.

Practical application: Configuring risk-scoring engines to automatically trigger appropriate workflows.

Challenges: Avoiding over-simplification that could miss hidden risks, and ensuring the risk model is

transparent to regulators.

Source of Wealth (SOW)

Related terms: Source of Funds, Wealth Accumulation, Financial Background, CIU Documentation

Definition: The overall origin of a customer's total net worth, as opposed to the immediate source of a specific transaction. Verifying SOW helps the Customer Identification Unit assess the legitimacy of large or unusual deposits.

Example: A client explains that their wealth derives from a family-owned manufacturing business, providing audited financial statements as evidence.

Practical application: Requiring SOW documentation for deposits exceeding a defined threshold, especially for high-risk jurisdictions.

Challenges: Obtaining reliable documentation, dealing with clients reluctant to disclose personal financial history, and assessing the credibility of self-declared information.

Suspicious Activity Report (SAR)

Related terms: SAR Filing, Regulatory Notification, Alert Escalation, CIU Investigation

Definition: A report filed by a financial institution to a designated authority when a transaction or behavior appears suspicious and may involve money laundering or other illicit activity. The Customer Identification Unit compiles the necessary information and coordinates the SAR submission.

Example: An analyst reviews a flagged international transfer, gathers supporting documents, and submits a SAR to the Financial Intelligence Unit (FIU).

Practical application: Using a SAR template that captures customer details, transaction description, and rationale for suspicion.

Challenges: Ensuring timely filing within statutory deadlines, maintaining confidentiality, and avoiding duplicate reporting.

Third-Party Data Provider

Related terms: External Vendor, Data Enrichment, API Integration, CIU Enrichment

Definition: An external service that supplies supplemental information—such as credit scores, sanctions data, or identity verification results—to enhance the quality of CDD. The Customer Identification Unit evaluates the reliability and compliance posture of third-party providers before integration.

Example: Subscribing to a global sanctions-screening service that updates daily with new entries.

Practical application: Implementing service-level agreements (SLAs) that guarantee data accuracy and uptime.

Challenges: Vendor risk management, data residency concerns, and ensuring that third-party data aligns with internal risk models.

Transaction Threshold

Related terms: Alert Rule, Risk Parameter, Monitoring Trigger, CIU Configuration

Definition: A predefined monetary value or volume that, when exceeded, initiates additional scrutiny or an alert. The Customer Identification Unit sets thresholds based on risk appetite and regulatory guidance.

Example: Any single cash deposit above USD 10,000 automatically generates a monitoring alert.

Practical application: Adjusting thresholds dynamically for high-risk customers to capture more granular activity.

Challenges: Balancing sensitivity to avoid alert overload, and ensuring thresholds comply with jurisdictional reporting requirements.

Unstructured Data Extraction

Related terms: OCR, Natural Language Processing, Document Parsing, CIU Data Capture

Definition: The process of retrieving relevant information from non-standardized sources such as scanned documents, emails, or PDFs. The Customer Identification Unit uses extraction tools to populate fields like name, address, and date of birth from uploaded identification documents.

Example: Applying OCR to a scanned utility bill to capture the address line for verification.

Practical application: Leveraging machine-learning models to improve extraction accuracy over time.

Challenges: Dealing with low-quality images, varied document layouts, and multilingual content.

Verification of Non-Financial Entities

Related terms: Corporate KYC, Entity Verification, Beneficial Owner Identification, CIU Scope

Definition: The process of confirming the legitimacy and ownership of entities that do not engage directly in financial activities but may be customers, such as NGOs or trusts. The Customer Identification Unit extends its due-diligence procedures to these non-financial entities to mitigate indirect risk.

Example: Verifying a charitable foundation's registration, board members, and source of donations.

Practical application: Using a risk matrix that assigns lower baseline scores to non-profit entities but increases scrutiny if linked to high-risk jurisdictions.

Challenges: Limited public information, diverse legal structures, and varying regulatory expectations.

Watchlist Maintenance

Related terms: List Update, Data Refresh, CIU Governance, Regulatory Change Management

Definition: The ongoing process of updating and validating the lists of individuals and entities used for screening, ensuring they reflect the latest sanctions, PEP, and adverse-media information. The Customer Identification Unit is responsible for schedule-driven maintenance.

Example: Quarterly ingestion of the latest OFAC SDN list into the screening engine.

Practical application: Automating the download and parsing of source files, with validation checks to detect format changes.

Challenges: Managing multiple source formats, handling data inconsistencies, and ensuring that updates do not disrupt ongoing screening operations.

Zero-Tolerance Policy

Related terms: Compliance Culture, Risk Appetite, CIU Enforcement, Sanctions Violation

Definition: An organizational stance that any breach of AML, sanctions, or KYC requirements is treated as unacceptable and subject to immediate remediation. The Customer Identification Unit enforces this policy by escalating violations and initiating corrective actions without delay.

Example: A single missed SAR filing triggers a formal investigation and remedial training for the responsible team.

Practical application: Embedding policy alerts into the CIU workflow to prompt mandatory approvals for high-risk decisions.

Challenges: Maintaining proportionality, avoiding punitive overreach that could hinder legitimate business, and ensuring consistent application across all business units.