STIX-AML Extension Proposal: Structured Intelligence for Financial Compliance

Created by:
Kim Haverblad
Njordium Cyber Group AB

Version:
1.1A

Publish Date:
2025-07-09

“This page is intentionally left blank.”

Table of Contents

1 Introduction

Preventing financial crimes, such as money laundering and fraud, is critical to maintaining the integrity of the European Union's financial systems. Recent audits across EU member states have exposed significant deficiencies in Anti-Money Laundering (AML) supervision, including inconsistent practices, limited inspection coverage, poor data quality in registers, and knowledge gaps among supervised entities. These challenges not only hinder AML efforts but also impact fraud prevention, as the two crimes are often interconnected. The Structured Threat Information Expression (STIX) framework, originally developed for cyber threat intelligence, offers a machine-readable format to standardise AML, Know Your Customer (KYC), Know Your Business (KYB), and fraud-related data. STIX-AML is a proposed approach that leverages an existing, proven technology—STIX—to help overcome current barriers to effective AML information sharing. The STIX-AML extension aims to address these gaps by enabling seamless data sharing, automated risk assessments, and compliance with EU regulations like AMLD5 and AMLD6, as well as international standards set by the Financial Action Task Force (FATF).

KYC and AML are distinct yet complementary processes critical to financial crime prevention. KYC focuses on user identification, serving as the first step toward anti-money laundering by helping verify the identity of the customer during the onboarding stage of validation. This typically involves a one-time verification process, though frequent updates may be required based on the customer's role or risk profile as part of ongoing monitoring. AML, in contrast, centers on user behaviour, helping verify the customer's financial activity through an ongoing check process. As the next step after knowing the user's identity, AML involves follow-up validation to detect suspicious patterns, such as unusual transactions or links to illicit activities. The STIX-AML extension integrates these processes by providing standardised objects (`x-suspiciousactivities`, `x-kycindividual`, `x-kybbusiness`) to capture both identity and behavioural data, enabling financial institutions, supervisory authorities, and law enforcement to collaborate effectively in combating financial crimes.

1.1 The Need for AML-Attribute Harmonisation

Effective AML supervision requires consistent data collection, reporting, and analysis across financial institutions, supervisory authorities, and law enforcement agencies. Recent EU audits have highlighted critical weaknesses, such as uneven supervisory practices, inadequate inspection scope, and poor register quality, which undermine the fight against financial crimes. The absence of a consolidated list of AML attributes or standardised, machine-readable formats, as confirmed by EU authorities, exacerbates these issues, leading to inefficiencies and missed opportunities for cross-border cooperation. Harmonising AML attributes is essential to ensure data consistency, reduce discrepancies, and improve the ability to detect and prevent illicit activities.
The STIX-AML extension addresses these challenges by providing a standardised framework for AML, KYC, and KYB data. By leveraging STIX's extensible and machine-readable structure, it facilitates seamless information exchange, enhances automated risk analysis, and supports compliance with EU directives like AMLD6 Article 10(6), which mandates access to account and transaction details. This harmonisation fosters collaboration among stakeholders, aligning with ongoing EU-FATF efforts to strengthen data standards and improve the effectiveness of AML supervision across member states.

1.2 AML vs. Fraud: Key Differences and Challenges

Fraud and money laundering are distinct yet interconnected financial crimes, each with unique motivations, tactics, and impacts. Understanding these differences is crucial for developing a comprehensive approach to financial crime prevention.

- **Definitions and Objectives**: Fraud involves intentional deception to gain financial advantage or cause loss, often through tactics like false representation (e.g., imposter scams), bank fraud (e.g., unauthorised account access), insurance fraud (e.g., falsified claims), or chargeback fraud (e.g., fraudulent refund claims). Its primary goal is immediate financial gain at the victim's expense. Money laundering, conversely, focuses on concealing the origins of illegally obtained funds to make them appear legitimate, enabling criminals to use these funds without detection. Common scenarios include laundering proceeds from drug trafficking, terrorism financing, or arms dealing.
- **Operational and Tactical Differences**: Fraud relies on direct deception, such as phishing, identity theft, or falsified documents, to exploit victims quickly. Money laundering employs complex processes, like layering funds through multiple accounts, using shell companies, or creating fictitious transactions, to obscure the illicit source of funds. For example, funds from a fraudulent bank scam may be laundered through offshore accounts to evade scrutiny.
- **Impact and Scale**: Fraud typically causes immediate financial and emotional harm to individual or business victims, such as losses from stolen bank funds or scams. Money laundering, however, has broader societal consequences, enabling serious crimes like drug trafficking and terrorism, which undermine financial systems and pose long-term risks to national and global economies.
- **Regulatory and Enforcement Challenges**: Fraud prevention emphasises rapid detection and resolution, with victims reporting to local law enforcement, national agencies (e.g., Internet Crime Complaint Center), or industry bodies, allowing for swift action and compensation. AML efforts, governed by regulations like the EU's AMLD5 and AMLD6, are more complex, involving long-term investigations, compliance monitoring, and reporting to Financial Intelligence Units (FIUs). The complexity of AML investigations often results in slower feedback and adaptation compared to fraud prevention, as noted in recent audits highlighting inefficiencies in supervisory processes.
- **Interconnection and Shared Challenges**: Fraud and money laundering often intersect, as fraudulent activities generate illicit proceeds that require laundering. For instance, a chargeback fraud scheme may feed into a money laundering network to disguise the funds' origins. The lack of standardised data formats, as identified in EU audits, complicates the detection of both crimes, particularly when sharing data across jurisdictions. Inconsistent practices and poor register quality further hinder efforts to trace fraudulent transactions or laundered funds.

The STIX-AML extension addresses these challenges by incorporating attributes for both AML and fraud, such as `suspicious_activity_type`, `aml_flags`, and `transaction_patterns`, enabling financial institutions and authorities to share structured data on suspicious activities. This unified approach supports automated analysis, improves detection of interconnected fraud and money laundering schemes, and aligns with regulatory requirements, offering a path to more effective financial crime prevention.

2 Purpose and Scope

The STIX-AML extension is designed to address the critical need for standardised, machine-readable data formats to enhance the prevention and detection of financial crimes, including money laundering and fraud, across the European Union and beyond. The lack of consolidated AML and fraud attributes and standardised formats, as confirmed by EU authorities, creates significant barriers to effective data sharing and pattern recognition. Financial crimes often evolve over time: what may initially be flagged as a potential fraud insight (e.g., an unusual chargeback pattern) can later be confirmed as a fraud incident and, upon further investigation, revealed as part of a larger money laundering scheme involving complex layering or shell companies. This interconnected nature of fraud and AML underscores the need for a unified framework that supports seamless data exchange and robust pattern recognition.

The primary purpose of the STIX-AML extension is to:

- **Facilitate Internal and External Data Sharing**: By providing a structured, machine-readable format, STIX-AML enables financial institutions, supervisory authorities, and Financial Intelligence Units (FIUs) to share AML, KYC, KYB, and fraud-related data efficiently. This fosters collaboration within organisations (e.g., between compliance and fraud teams) and externally across borders, aligning with EU initiatives like Eurojust for cross-jurisdictional investigations.
- **Enable AML and Fraud Pattern Recognition**: The extension incorporates attributes like `suspicious_activity_type`, `aml_flags`, and `transaction_patterns` to capture indicators of both fraud (e.g., chargeback fraud, identity theft) and money laundering (e.g., layered transactions, offshore connections). This allows organisations to track the evolution of suspicious activities, from initial fraud insights to confirmed incidents and potential AML schemes, using automated analysis to identify patterns such as unusual transaction volumes or jurisdictions involved.
- **Ensure Regulatory Compliance**: The extension aligns with EU regulations, such as AMLD5 and AMLD6 Article 10(6), which mandate access to account and transaction details, as well as FATF Recommendations for beneficial ownership transparency. It supports compliance by standardising data for reporting to FIUs and supervisory authorities, reducing discrepancies and enhancing auditability.
- **Enhance Automated Risk Assessment**: By structuring data in a machine-readable format, STIX-AML enables automated tools to analyse risk scores, detect high-risk entities (e.g., Politically Exposed Persons, sanctioned individuals), and identify patterns that may indicate broader AML schemes, improving efficiency and accuracy in financial crime detection.
- **Foster Collaboration with Stakeholders**: The extension encourages collaboration with EU technology vendors, financial institutions, and regulators to refine and adopt standardised data formats, addressing the harmonisation gaps noted in EU-FATF discussions and supporting global efforts to combat financial crimes.

The scope of the STIX-AML extension includes defining three custom STIX objects (`x-suspicioustransaction`, `x-kycindividual`, `x-kybbusiness`) with attributes tailored for customer identification, transaction monitoring, risk assessment, and reporting. These objects are designed to capture both AML and fraud-related data, enabling organisations to address the full spectrum of financial crimes. The extension is applicable to financial institutions (e.g., banks, payment providers), non-financial sectors (e.g., real estate, casinos), and supervisory authorities across the EU and aligned jurisdictions like Switzerland, ensuring flexibility and scalability for diverse compliance needs.

3 Methodology

The development process involved:

1. **Regulatory Review**: Reviewing FATF Recommendations, EU AML directives (AMLD5, AMLD6), and national regulations to identify required attributes for AML and fraud prevention.
2. **Stakeholder Engagement**: Consulting with financial institutions, EU supervisory authorities, and technology vendors to ensure practical applicability and alignment with operational needs.
3. **Attribute Mapping**: Identification of essential attributes for compliance and risk management, mapped to STIX's extensible framework.
4. **STIX Compatibility**: Ensuring compatibility with STIX Version 2.1 for seamless integration with existing threat intelligence platforms.

4 STIX AML/KYC/KYB Object Definitions

4.1 Suspicious Activities (x-suspiciousactivities)

The `x-suspiciousactivities` object captures details of suspicious transactions, aligning with requirements for Suspicious Activity Reports (SARs) and AMLD6 Article 10(6). The term "Suspicious Activities" is used instead of "AML Suspicious Activities" to reflect its broader scope, encompassing both money laundering and fraud-related activities. This change acknowledges the interconnected nature of these financial crimes, where an activity initially flagged as a potential fraud insight (e.g., an unusual chargeback pattern or unauthorised account access) may later be confirmed as a fraud incident and, through further investigation, revealed as part of a larger money laundering scheme involving complex layering or shell companies. By adopting a generic term, the STIX-AML extension ensures that the object captures a wide range of suspicious indicators, facilitating standardised data sharing and pattern recognition across internal compliance teams, financial institutions, and external authorities like Financial Intelligence Units (FIUs).

This unified approach enhances the ability to track the evolution of suspicious activities over time. For example, a transaction flagged for suspected fraud due to inconsistent customer behaviour can be analysed alongside other transactions to identify patterns indicative of money laundering, such as transfers to high-risk jurisdictions or the use of fictitious entities. The `x-suspiciousactivities` object includes attributes like `suspicious_activity_type`, `aml_flags`, and `transaction_patterns` to support automated analysis and cross-border collaboration, aligning with EU regulations and FATF standards. This enables organisations to share structured, machine-readable data with authorities (e.g., FIU-NL, CTIF-CFI, BaFin) and improve the detection of complex financial crime schemes, ultimately strengthening the integrity of the financial system.

Attribute	Type	Description
type	string	Fixed as "x-suspiciousactivities" to indicate a custom STIX object.
spec_version	string	STIX specification version, set to "2.1".
id	string	Unique identifier for the object, following STIX UUID format.
created	timestamp	Timestamp when the object was created.
modified	timestamp	Timestamp when the object was last modified.
transaction_id	string	Unique identifier for the transaction.
transaction_date	timestamp	Date and time of the transaction.
amount	float	Amount of the transaction.
currency	string	Currency code (e.g., EUR, USD).
transaction_type	string	Type of transaction (e.g., wire transfer, cash deposit).
suspicious_activity. type	string	Type of suspicious activity (e.g., money laundering, fraud, structuring).
suspicious_activity. domain	string	Type of sub-activity (e.g., fraud synthetic identity, money laundering layering offshore, structuring atm smurfing, suspicious activity terror financing NGO donations, money laundering crypto mixer, corruption pep procurement, VAT fraud.)
suspicious_activity. indicator	string	IP address of a mule account login, high-risk IBAN, or BTC wallet. Business value, signals known fraud infrastructure or payment vectors.
suspicious_activity. observable	string	Repeated logins from unusual geolocation; login + withdrawal pairing. Business value, captures behavioural patterns and anomalies in transaction data

Attribute	Type	Description
suspicious_activity. pattern	string	Smurfing, layering, trade-based laundering, invoice fraud. Business value, encodes known AML tactics and M.O.s for correlation and enrichment.
suspicious_activity. threat_actor	string	Human trafficker syndicate, ransomware cartel, or money mule network. Business value, Identifies organised groups behind the laundering/fraud scheme
suspicious_activity. intrusion_set	string	Credential stuffing attacks that lead to unauthorised transfers. Business value, associates cyber entry points with financial impact.
suspicious_activity. attack_vector	string	Dridex, TrickBot, or keyloggers used to hijack accounts. Provides linkage between malware and fraud activity.
suspicious_activity. infrastructure	string	Compromised ATM network, bulletproof hosting, mixer services. Business value, Points to enabling tech behind fraud or laundering
suspicious_activity. relationship	string	Links between mule accounts, shell companies, and fake invoices. Business value, connects entities to uncover hidden ownership and collusion
suspicious_activity. device_fingerprint	string	Multiple accounts accessed from the same device (e.g., mule farm or synthetic identity ring)
suspicious_activity. ip_geo_behavior	string	Anomalies in login locations, TOR usage, offshore routing, or “impossible travel” behaviour
merchant_category_code	string	Laundering via charities, casinos, or real estate flagged as high-risk sectors
crypto_wallet_address	string	Cryptocurrency wallet address involved in the transaction.
blockchain_reference	string	Blockchain transaction ID or hash.
originator_name	string	Name of the transaction originator.
originator_account	string	Account number of the originator.
originator_address	string	Address of the originator.
beneficiary_name	string	Name of the beneficiary.
beneficiary_account	string	Account number of the beneficiary.
beneficiary_address	string	Address of the beneficiary.
customer_id	string	ID of the customer associated with the transaction.
customer_name	string	Name of the customer.
customer_address	string	Address of the customer.
customer_phone_number	string	Contact phone number for the individual, organisation, or account holder involved in the transaction
customer_dob	date	Date of birth of the customer (if individual).
customer_nationality	string	Nationality of the customer.
customer_type	string	Type of customer (e.g., individual, company).
beneficial_owner	array	List of beneficial owners (names or IDs).
pep_status	boolean	Whether the customer is a Politically Exposed Person (PEP).
sanctions_status	boolean	Whether the customer is on a sanctions list.
sanctions_list_checked	array	Sanctions lists screened (e.g., OFAC SDN, UN Sanctions).
risk_score	float	Risk score for the transaction, typically 0 to 1.
risk_factors	array	List of factors contributing to the risk score (e.g., high value, unusual pattern).
flag_status	string	Status of the transaction (e.g., suspicious, high-risk).
report_status	string	Whether the transaction was reported (e.g., reported, not reported).
report_date	timestamp	Date when the transaction was reported to the FIU.
fiu_reference	string	Reference number from the FIU, if applicable.

Attribute	Type	Description
Internal_handling	string	Internal actions for the transaction (e.g., "Escalated to compliance").
notes	string	Additional notes or comments for internal use.
regulatory_references	array	List of applicable AML directives or regulations (e.g., AMLD5, AMLD6).

4.2 Suspicious Activities Sample JSON Representation

The following JSON example illustrates the structure and attributes of the `x-suspiciousactivities` object, demonstrating how it captures key details for suspicious transactions, including both AML and fraud indicators, to support standardised data sharing and compliance.

```
json
{
  "type": "x-suspiciousactivities",
  "id": "x-suspiciousactivities--123e4567-e89b-12d3-a456-426614174000",
  "created": "2025-06-27T10:31:00.000Z",
  "modified": "2025-06-27T10:31:00.000Z",
  "transaction_id": "TXN12345",
  "transaction_date": "2025-06-26T15:30:00.000Z",
  "amount": 100000.00,
  "currency": "EUR",
  "transaction_type": "wire transfer",
  "suspicious_activity_type": "money laundering",
  "hypothesis": "Multiple high-value transactions from a single account
with no apparent legitimate purpose.",
  "originator_name": "John Doe",
  "originator_account": "123456789",
  "originator_address": "123 Main St, Stockholm, Sweden",
  "beneficiary_name": "Jane Smith",
  "beneficiary_account": "987654321",
  "beneficiary_address": "456 Elm St, Gothenburg, Sweden",
  "customer_id": "CUST001",
  "customer_name": "John Doe",
  "customer_address": "123 Main St, Stockholm, Sweden",
  "customer_phone_number": "+46701234567",
  "customer_dob": "1980-01-01",
  "customer_nationality": "SE",
  "customer_type": "individual",
  "beneficial_owner": ["John Doe"],
  "pep_status": false,
  "sanctions_status": false,
  "sanctions_list_checked": ["OFAC SDN", "UN Sanctions"],
  "risk_score": 0.8,
  "risk_factors": ["high transaction volume", "unusual transaction
pattern"],
  "flag_status": "suspicious",
  "report_status": "reported",
  "report_date": "2025-06-27T09:00:00.000Z",
  "fiu_reference": "FIU-REF-001",
  "internal_handling": "Escalated to compliance team for enhanced due
diligence",
```

```
  "notes": "Transaction flagged due to inconsistency with customer's
known business activities.",
  "regulatory_references": ["AMLD6", "Penningtvättslagen 2017:630"]
}
```

4.3 KYC – Individual (x-kycindividual)

This object captures data for individual customer due diligence, aligning with KYC requirements.

Attribute	Type	Description
type	string	Fixed as "x-kycindividual" to indicate a custom STIX object.
spec_version	string	STIX specification version, set to "2.1".
id	string	Unique identifier for the object, following STIX UUID format.
created	timestamp	Timestamp when the object was created (e.g., "2025-06-27T10:31:00.000Z").
modified	timestamp	Timestamp when the object was last modified (e.g., "2025-06-27T10:31:00.000Z").
monitoring_frequency	string	Frequency of ongoing monitoring (e.g., daily, monthly, event-based).
customer_id	string	Unique identifier for the individual customer.
full_name	string	Full legal name of the individual.
date_of_birth	date	Date of birth of the individual (YYYY-MM-DD).
identification_number	string	Personal identification number (e.g., SSN, ITIN, CPR, PNR)
nationality	string	Nationality of the individual (ISO 3166-1 alpha-2 code).
address	object	Residential address of the individual.
address.street	string	Street address.
address.city	string	City of residence.
address.country	string	Country of residence (ISO 3166-1 alpha-2 code).
address.postal_code	string	Postal code.
phone_number	string	Contact phone number for the individual.
identification_document	object	Details of the identification document used for verification.
identification_document.type	string	Type of identification document (e.g., passport, national ID).
identification_document.number	string	Document number.
identification_document.issue_date	date	Issue date of the document.
identification_document.expiry_date	date	Expiry date of the document.
identification_document.issuing_authority	string	Authority that issued the document.
tax_domicile	string	Country of tax residence (ISO 3166-1 alpha-2 code).
pep_status	boolean	Indicates if the individual is a Politically Exposed Person (PEP).
sanctions_status	boolean	Indicates if the individual is on a sanctions list.
sanctions_list_checked	array	List of sanctions lists screened against (e.g., OFAC SDN, UN Sanctions).
customer_onboarding_anomalies	string	Synthetic IDs, mismatched documents, high-velocity account creation
risk_score	float	Risk score for the individual (0 to 1), based on AML risk assessment.

Attribute	Type	Description
risk_factors	array	Factors contributing to the risk score (e.g., high-risk country, unusual activity).
aml_flags	array	Risk indicators (e.g., "layered transactions", "offshore connections").
verification_status	string	Status of KYC verification (e.g., verified, pending, rejected).
verification_date	timestamp	Date and time when the KYC verification was completed.
verification_method	string	Method used to verify identity (e.g., document check, third-party database).
edd_actions	array	List of enhanced due diligence actions taken (e.g., site visits, court records).
source_of_funds	string	Declared source of funds (e.g., salary, investments).
purpose_of_relationship	string	Purpose of the business relationship (e.g., savings, investment).
banking_relationship	object	Details of the customer's banking relationship.
banking_relationship.bank_name	string	Name of the bank (e.g., "Nordic Bank AB").
banking_relationship.iban	string	International Bank Account Number (IBAN).
banking_relationship.swift	string	SWIFT code of the bank.
banking_relationship.account_open_date	string	Date the account was opened (YYYY-MM-DD).
transaction_patterns	object	Typical transaction behaviour of the customer.
transaction_patterns.avg_monthly_volume	float	Average monthly transaction volume.
transaction_patterns.currency	string	Currency of transactions (e.g., SEK).
transaction_patterns.jurisdictions_involved	array	Jurisdictions involved in transactions (ISO 3166-1 alpha-2 codes).
internal_handling	string	Internal actions for the customer (e.g., "Additional KYC verification requested").
notes	string	Additional notes or comments for internal use.
regulatory_references	array	Applicable AML directives or regulations (e.g., AMLD5, AMLD6).

4.4 KYC – Individual Sample JSON Representation

The following JSON example demonstrates the structure and attributes of the `x-kycindividual` object, illustrating how it captures detailed customer identification data for KYC compliance, including fraud-related attributes, to support standardised onboarding and verification processes.

```
json
{
  "type": "x-kycindividual",
  "spec_version": "2.1",
  "id": "x-kycindividual--987fcdeb-12d3-4e5f-6789-1234567890ab",
  "created": "2025-06-27T10:31:00.000Z",
  "modified": "2025-06-27T10:31:00.000Z",
  "monitoring_frequency": "monthly",
  "customer_id": "CUST001",
  "full_name": "John Doe",
  "date_of_birth": "1980-01-01",
  "identification_number": "19800101-1234",
  "nationality": "SE",
```

```
  "address": {
    "street": "123 Main St",
    "city": "Stockholm",
    "country": "SE",
    "postal_code": "111 52"
  },
  "phone_number": "+46701234567",
  "identification_document": {
    "type": "passport",
    "number": "A12345678",
    "issue_date": "2015-01-01",
    "expiry_date": "2025-01-01",
    "issuing_authority": "Swedish Police"
  },
  "tax_domicile": "SE",
  "pep_status": false,
  "sanctions_status": false,
  "sanctions_list_checked": ["OFAC SDN", "UN Sanctions"],
  "risk_score": 0.3,
  "risk_factors": ["low transaction volume"],
  "aml_flags": ["offshore connections"],
  "verification_status": "verified",
  "verification_date": "2025-06-27T09:00:00.000Z",
  "verification_method": "document check",
  "edd_actions": [],
  "source_of_funds": "salary",
  "purpose_of_relationship": "savings",
  "banking_relationship": {
    "bank_name": "Nordic Bank AB",
    "iban": "SE3550000000054910000003",
    "swift": "NDBASESS",
    "account_open_date": "2015-03-10"
  },
  "transaction_patterns": {
    "avg_monthly_volume": 200000.0,
    "currency": "SEK",
    "jurisdictions_involved": ["SE", "LU"]
  },
  "internal_handling": "Standard monitoring applied",
  "notes": "Customer verified with valid passport.",
  "regulatory_references": ["AMLD5", "Penningtvättslagen 2017:630"]
}
```


4.5 KYB – Business (x-kybbusiness)

This object captures data for business entity due diligence, aligning with KYB requirements.

Attribute	Type	Description
type	string	Fixed as "x-kybbusiness" to indicate a custom STIX object.
spec_version	string	STIX specification version, set to "2.1".
id	string	Unique identifier for the object, following STIX UUID format.
created	timestamp	Timestamp when the object was created (e.g., "2025-06-27T10:31:00.000Z").
modified	timestamp	Timestamp when the object was last modified (e.g., "2025-06-27T10:31:00.000Z").

Attribute	Type	Description
monitoring_frequency	string	Frequency of ongoing monitoring (e.g., daily, monthly, event-based).
business_id	string	Unique identifier for the business entity.
us_ein	string	Employer Identification Number (EIN) for the business.
legal_name	string	Legal name of the business.
registration_number	string	Business registration number.
country_of_registration	string	Country of business registration (ISO 3166-1 alpha-2 code).
address	object	Registered address of the business.
address.street	string	Street address of the business.
address.city	string	City of the business.
address.country	string	Country of the business (ISO 3166-1 alpha-2 code).
address.postal_code	string	Postal code.
phone_number	string	Contact phone number for the individual.
incorporation_date	date	Date of business incorporation (YYYY-MM-DD).
business_type	string	Type of business (e.g., corporation, LLC, partnership).
industry	string	Industry sector of the business (e.g., finance, manufacturing).
cta_boi_submission	boolean	Indicates whether beneficial ownership information was submitted to FinCEN.
cta_boi_reference	STRING	FinCEN reference number for CTA BOI submission.
beneficial_owners	array	List of beneficial owners with their details.
beneficial_owners.name	string	Name of the beneficial owner.
beneficial_owner_id_number	array	Identification numbers (e.g., SSN, ITIN, CPR, PNR) for beneficial owners.
beneficial_owner_date_of_birth	array	Date of birth for each beneficial owner.
beneficial_owner_address	array	Current residential address for each beneficial owner.
beneficial_owners.ownership_percentage	float	Percentage of ownership.
beneficial_owners.nationality	string	Nationality of the beneficial owner (ISO 3166-1 alpha-2 code).
beneficial_owners.pep_status	boolean	Indicates if the beneficial owner is a PEP.
beneficial_owners.sanctions_status	boolean	Indicates if the beneficial owner is on a sanctions list.
tax_domicile	string	Country of tax residence for the business (ISO 3166-1 alpha-2 code).
sanctions_status	boolean	Indicates if the business is on a sanctions list.
sanctions_list_checked	array	List of sanctions lists screened against (e.g., OFAC SDN, UN Sanctions).
risk_score	float	Risk score for the business (0 to 1), based on AML risk assessment.
risk_factors	array	Factors contributing to the risk score (e.g., high-risk industry, complex ownership).
aml_flags	array	Risk indicators (e.g., "layered transactions", "offshore connections").
verification_status	string	Status of KYB verification (e.g., verified, pending, rejected).
verification_date	timestamp	Date and time when the KYB verification was completed.
verification_method	string	Method used to verify business identity (e.g., corporate registry, database).

Attribute	Type	Description
edd_actions	array	List of enhanced due diligence actions taken (e.g., corporate structure analysis).
source_of_funds	string	Declared source of funds for the business (e.g., revenue, investments).
purpose_of_relationship	string	Purpose of the business relationship (e.g., corporate banking, trade finance).
banking_relationship	object	Details of the customer's banking relationship.
banking_relationship.bank_name	string	Name of the bank (e.g., "Nordic Bank AB").
banking_relationship.iban	string	International Bank Account Number (IBAN).
banking_relationship.swift	string	SWIFT code of the bank.
banking_relationship.account_open_date	string	Date the account was opened (YYYY-MM-DD).
transaction_patterns	object	Typical transaction behaviour of the customer.
transaction_patterns.avg_monthly_volume	float	Average monthly transaction volume.
transaction_patterns.currency	string	Currency of transactions (e.g., SEK).
transaction_patterns.jurisdictions_involved	array	Jurisdictions involved in transactions (ISO 3166-1 alpha-2 codes).
internal_handling	string	Internal actions for the customer (e.g., "Additional KYB verification requested").
banking_relationship	object	Details of the customer's banking relationship.
notes	string	Additional notes or comments for internal use.
regulatory_references	array	Applicable AML directives or regulations (e.g., AMLD5, AMLD6).

4.6 KYB – Business Sample JSON Representation

The following JSON example illustrates the structure and attributes of the x-kybbusiness object, demonstrating how it captures comprehensive business entity data for KYB compliance, including fraud-related attributes, to support standardized due diligence and verification processes.

```json
{
  "type": "x-kybbusiness",
  "spec_version": "2.1",
  "id": "x-kybbusiness--456fcdeb-12d3-4e5f-6789-9876543210cd",
  "created": "2025-06-27T10:31:00.000Z",
  "modified": "2025-06-27T10:31:00.000Z",
  "monitoring_frequency": "quarterly",
  "business_id": "BIZ001",
  "us_ein": "12-3456789",
  "legal_name": "Acme Corp",
  "registration_number": "556123-4567",
  "country_of_registration": "SE",
  "address": {
    "street": "789 Business Park",
    "city": "Stockholm",
    "country": "SE",
    "postal_code": "111 53"
  },
```

```
  "phone_number": "+46812345678",
  "incorporation_date": "2010-01-01",
  "business_type": "corporation",
  "industry": "finance",
  "cta_boi_submission": false,
  "cta_boi_reference": "",
  "beneficial_owners": [
    {
      "name": "Jane Smith",
      "identification_number": "19750101-5678",
      "date_of_birth": "1975-01-01",
      "address": "456 Elm St, Gothenburg, Sweden",
      "ownership_percentage": 30.0,
      "nationality": "SE",
      "pep_status": false,
      "sanctions_status": false
    }
  ],
  "tax_domicile": "SE",
  "sanctions_status": false,
  "sanctions_list_checked": ["OFAC SDN", "UN Sanctions"],
  "risk_score": 0.4,
  "risk_factors": ["complex ownership structure"],
  "aml_flags": ["offshore connections"],
  "verification_status": "verified",
  "verification_date": "2025-06-27T09:00:00.000Z",
  "verification_method": "corporate registry",
  "edd_actions": ["adverse media check"],
  "source_of_funds": "revenue",
  "purpose_of_relationship": "corporate banking",
  "banking_relationship": {
    "bank_name": "Nordic Bank AB",
    "iban": "SE3550000000054910000003",
    "swift": "NDBASESS",
    "account_open_date": "2015-03-10"
  },
  "transaction_patterns": {
    "avg_monthly_volume": 200000.0,
    "currency": "SEK",
    "jurisdictions_involved": ["SE", "LU"]
  },
  "internal_handling": "Standard monitoring applied",
  "notes": "Business verified via Bolagsverket.",
  "regulatory_references": ["AMLD5", "Penningtvättslagen 2017:630"]
}
```


5 Data Retention and Processing Constraints

As organisations increasingly exchange structured cyber threat intelligence enriched with anti-fraud and AML metadata, handling sensitive business and personal data within regulatory frameworks like GDPR, AMLD5, and NIS2 becomes critical.

The STIX 2.1 protocol does not natively support attributes for data retention, on-prem processing requirements, or sharing constraints. However, these gaps can be addressed using a combination of:

- STIX custom objects
- Marking definitions (built-in support for classification/handling rules)

- Integration with tag-based classification systems for defining legal basis, data retention, and processing constraints

5.1 Extend STIX for Data Governance

Core STIX focuses on the "what" of cyber threats — indicators, malware, actors — but omits metadata for **how** threat or business intelligence should be stored, handled, or retained. In AML and KYB scenarios, this becomes crucial:

Compliance Element	Relevance for AML/KYC/KYB
Data retention period	AML laws may mandate 5-10 years of storage
Processing location	GDPR may restrict non-EU cloud storage
Sharing policy	Consent or legal basis needed to disclosure
Legal references	Ties data to AMLD5, GDPR, FATF, etc.

5.2 Object Attributes (x-data-handling)

Attribute	Type	Description
type	string	Fixed as "x-data-handling". Specifies the object type per STIX 2.1 standards.
spec_version	string	STIX specification version set to "2.1".
id	string	Unique identifier (STIX UUID format).
created	timestamp	Timestamp of object creation.
modified	timestamp	Timestamp of last modification.
labels	array	Tags for classification (e.g. ["personal-data:retention=7y" "data-classification:restricted"]). Supports tag-based classification for retention legal basis and sharing constraints.
processing_constraints	object	Constraints on data processing including location and security requirements.
processing_constraints. processing_location	string	Location where data must be processed (e.g. "on-premises", "EU-cloud").
processing_constraints. encryption_required	boolean	Indicates if encryption is required for data storage or processing.
processing_constraints. access_limited_to_roles	array	Roles or entities allowed to access the data (e.g. ["aml_investigator" "FIU"]).
sharing_policy	object	Rules governing data sharing with other entities or jurisdictions.
sharing_policy. sharing_allowed	boolean	Indicates if data sharing is permitted (true/false).
sharing_policy. requires_consent	boolean	Indicates if explicit consent is required for sharing.
sharing_policy. legal_basis	string	Legal basis for processing or sharing (e.g. "GDPR Art. 6(1)(c) - legal obligation").
sharing_policy. exceptions	array	Exceptions allowing sharing without consent (e.g. ["regulatory_audit"]).
sharing_policy. allowed_jurisdictions	array	Jurisdictions permitted to receive data (e.g. ["EU" "CH"]).
retention_policy	object	Rules governing data retention duration and triggers.
retention_policy. retention_period	string	Duration data must be retained (e.g. "7 years").

Attribute	Type	Description
retention_policy. trigger_event	string	Event triggering retention period (e.g. "end_of_relationship" "transaction_completion").
retention_policy. retention_basis	string	Legal basis for retention (e.g. "AMLD5").
marking_refs	array	References to STIX marking-definition objects for handling instructions (e.g. ["marking-definition--d1f01e3c-222b-4a12-8547-4457fc310002"]).
related_object_refs	array	References to related STIX objects (e.g. ["x-kybbusiness--456fcdeb-12d3-4e5f-6789-9876543210cd"]).
notes	string	Additional notes for internal use (e.g. "On-prem only. Strict data lifecycle applied.").

5.3 Example: Custom STIX 2.1 Extension – x-data-handling

To formalise governance logic, we define a custom STIX object: `x-data-handling`.

JSON

```
{
  "type": "x-data-handling",
  "spec_version": "2.1",
  "id": "x-data-handling--94be1273-09d2-4e29-baaa-111db25c3f7d",
  "created": "2025-07-03T12:00:00.000Z",
  "modified": "2025-07-03T12:00:00.000Z",
  "labels": [
    "personal-data:retention=7y",
    "data-classification:restricted",
    "processing:legal-basis=6(1)(c)",
    "sharing:consent-required"
  ],
  "processing_constraints": {
    "processing_location": "on-premises",
    "encryption_required": true,
    "access_limited_to_roles": ["aml_investigator", "FIU"]
  },
  "sharing_policy": {
    "sharing_allowed": false,
    "requires_consent": true,
    "legal_basis": "GDPR Art. 6(1)(c) - legal obligation",
    "exceptions": ["regulatory_audit"],
    "allowed_jurisdictions": ["EU", "CH"]
  },
  "retention_policy": {
    "retention_period": "7 years",
    "trigger_event": "end_of_relationship",
    "retention_basis": "AMLD5"
  },
  "marking_refs": [
    "marking-definition--d1f01e3c-222b-4a12-8547-4457fc310002"
  ],
  "related_object_refs": [
    "x-kybbusiness--456fcdeb-12d3-4e5f-6789-9876543210cd"
  ],
  "notes": "On-prem only. Strict data lifecycle applied."
}
```

5.4 STIX Marking-Definition for Sharing Control

STIX provides the marking-definition object to describe how data can be handled. Here's how to declare a statement limiting sharing and processing:

```JSON
{
  "type": "marking-definition",
  "id": "marking-definition--d1f01e3c-222b-4a12-8547-4457fc310002",
  "created": "2025-07-03T12:45:00.000Z",
  "definition_type": "statement",
  "definition": {
    "statement": "This data must be processed on-premises only and cannot be shared externally without written consent."
  }
}
```

The object marking would be references like this:

```JSON
"object_marking_refs": [
  "marking-definition--d1f01e3c-222b-4a12-8547-4457fc310002"
]
```

5.5 Tag-based classification model

A tag-based classification model can complement this by enabling the identification and handling of personal and regulated data, which would be mirrored into STIX as Custom attributes, Object labels and Marketing-definitions:

Tag Example	Purpose
personal-data:retention="5y"	Indicates how long data must be kept
data-classification:restricted	Aligns with internal access policies
processing:legal-basis=6(1)(c)	Declares GDPR legal basis
sharing:consent-required	Consent must be obtained

The approach offers several key benefits. It enhances auditability by allowing clear definitions of who can access specific data and for how long. It supports compliance by documenting the lawful basis for processing and enforcing regulatory constraints such as those under EU legislation. Controlled sharing is enabled by embedding usage restrictions directly within the STIX format, ensuring that data handling policies travel with the data.

5.6 STIX Classification Example

```JSON
{
  "type": "bundle",
  "id": "bundle--e4e4aa67-1357-4f6c-b87a-019d0e4dcf01",
  "objects": [
```

```
    {
      "type": "x-kybbusiness",
      "id": "x-kybbusiness--456fcdeb-12d3-4e5f-6789-9876543210cd",
      "spec_version": "2.1",
      "created": "2025-06-27T10:31:00.000Z",
      "modified": "2025-06-27T10:31:00.000Z",
      "legal_name": "Acme Corp"
      // ... other KYB attributes
    },
    {
      "type": "x-data-handling",
      "id": "x-data-handling--94be1273-09d2-4e29-baaa-111db25c3f7d",
      "spec_version": "2.1",
      "created": "2025-07-03T12:00:00.000Z",
      "modified": "2025-07-03T12:00:00.000Z",
      "processing_constraints": {
        "processing_location": "on-premises",
        "encryption_required": true
      },
      "sharing_policy": {
        "sharing_allowed": false,
        "requires_consent": true,
        "legal_basis": "GDPR Art. 6(1)(c)",
        "exceptions": ["regulatory_audit"]
      },
      "retention_policy": {
        "retention_period": "7 years",
        "trigger_event": "end_of_relationship",
        "retention_basis": "AMLD5"
      },
      "marking_refs": [
        "marking-definition--d1f01e3c-222b-4a12-8547-4457fc310002"
      ],
      "related_object_refs": [
        "x-kybbusiness--456fcdeb-12d3-4e5f-6789-9876543210cd"
      ]
    }
  ]
}
```

6 Extensibility and Integration

The STIX framework's extensibility, as defined in STIX Version 2.1, allows for the addition of custom attributes using the "x-" prefix (e.g., x_custom_risk_indicator). Relationships can link these objects to other STIX objects, such as:

- **Identity**: To reference customers or beneficial owners.
- **Indicator**: To represent patterns of suspicious activity.
- **Threat Actor**: To identify individuals or entities involved in financial crimes.

This integration enables a holistic view, combining AML data with broader threat intelligence, enhancing detection and response capabilities. For example, an `x-suspiciousactivities` object can be linked to an `x-kycindividual` object via a related-to relationship to provide context about the customer involved.

7 Use Cases

The following use cases demonstrate practical applications of the STIX AML/KYC/KYB objects:

1. **Suspicious Activity Reporting (SAR)**:
   - Financial institutions use `x-suspiciousactivities` to compile SARs for submission to FIUs, such as the Swedish Police FIU. Attributes like `hypothesis`, `suspicious_activity_type`, and `internal_handling` ensure compliance with reporting requirements.
   - **Example**: A bank detects a series of high-value transactions inconsistent with a customer's KYC profile. An `x-suspiciousactivities` object is created, linked to an `x-kycindividual` object, and shared with the FIU for investigation.
2. **Customer Due Diligence (CDD)**:
   - During onboarding, institutions populate `x-kycindividual` or `x-kybbusiness` objects to verify customer identities and assess risks. Attributes like `identification_number`, `pep_status`, and `sanctions_list_checked` support compliance with AMLD5 and Swedish regulations.
   - **Example**: A fintech company verifies a new corporate client using `x-kybbusiness`, documenting beneficial owners and submitting BOI (Beneficial Owner Information
   - — this refers to identifying the ultimate beneficial owners (UBOs) of a company, i.e., the natural persons who ultimately own or control the legal entity) to Swedish Companies Registration Office, as required by AMLD6.
3. **Automated Risk Analysis**:
   - The `risk_score` and `risk_factors` attributes enable automated risk assessments, integrating with analytics platforms to flag high-risk customers or transactions.
   - **Example**: A payment processor uses `x-suspiciousactivities` to flag a cryptocurrency transaction with a high `risk_score` due to an unusual `crypto_wallet_address`, triggering enhanced due diligence.
4. **Cross-Organisational Data Sharing**:
   - Institutions share STIX objects with regulators or other entities via secure platforms, ensuring standardised data exchange.
   - **Example**: A bank shares an `x-suspiciousactivities` object with Europol's EFCC to support a cross-border money laundering investigation.

8 Derived Business Value

Adopting STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Intelligence Information) for fraud and anti-money laundering (AML) intelligence sharing can yield significant positive outcomes and business value, especially when framed through the lens of a fraud and AML proactive research and operations.

8.1 Enhanced Detection and Prevention Capabilities

Positive outcome:

- Faster and more accurate detection of fraud and AML patterns.

Business Value:

- Reduces financial losses due to fraud.
- Shortens time to action with real-time intelligence.
- Enables proactive risk mitigation instead of reactive responses.

8.2 Inter-Organisational Collaboration and Network Defence

Positive outcome:

- Secure, automated sharing of fraud typologies, mule account patterns, and money-laundering tactics across financial institutions and regulators.

Business Value:

- Fosters collective defence against emerging threats (e.g., synthetic identities, mule networks).
- Supports industry-wide pattern recognition, even for low-volume anomalies.
- Reduces false positives, enhancing operational efficiency.

8.3 Data Standardisation and Interoperability

Positive outcome:

- Common language and format for fraud and AML indicators using STIX objects (e.g., indicators, threat actors, observed data).

Business Value:

- Breaks down data silos between internal departments (fraud, cyber, compliance).
- Enables automated ingestion and processing by AML transaction monitoring systems or SIEMs.
- Simplifies integration with national FIUs, regulators, and threat intelligence platforms.

8.4 Regulatory Alignment and Compliance Support

Positive outcome:

- Easier documentation,
- Tracking, and sharing of suspicious activity aligned with FATF, EU AMLD, FinCEN, and DORA expectations.

Business Value:

- Enhances regulatory reporting consistency (e.g., STRs/SARs with threat context).
- Demonstrates proactive risk governance during audits.
- Supports cross-border investigations by using internationally accepted threat schemas.

8.5 Threat-Informed Risk Management

Positive outcome:

- Continuous mapping of fraud and AML threats to business processes, clients, and third parties.

Business Value:

- Informs due diligence and onboarding (e.g., detecting shell companies or high-risk geographies).
- Improves third-party risk assessments.
- Elevates risk-adjusted decision-making in product, market, and customer strategy.

8.6 Operational Efficiency and Cost Reduction

Positive outcome:

Automated threat ingestion and response playbooks for fraud/AML via orchestration tools.

Business Value:

- Reduces manual investigation time for fraud alerts.
- Improves case triaging and alert prioritisation.
- Frees up analyst capacity for complex typology exploration.

8.7 Cross-Domain Intelligence Fusion (Cyber + Fraud + AML)

Positive outcome:

- Linkage of cyber compromise (e.g., phishing, malware) to fraudulent transactions and laundering behaviour.

Business Value:

- Enables end-to-end attack chain visibility (from intrusion to cash-out).
- Facilitates joint investigations between fraud teams, SOC, and compliance.
- Mitigates sophisticated hybrid threats such as business email compromise (BEC) leading to international wire fraud.

8.8 The Strategic Business Case for STIX and TAXII in Fraud and Anti-Money Laundering Programs

As financial fraud and money laundering threats become increasingly complex and transnational, organisations must move beyond traditional, siloed approaches to detection and prevention. The evolving nature of financial crime — from synthetic identity fraud and coordinated mule networks to cyber-enabled laundering and AI-generated scams — demands a more agile, integrated, and intelligence-driven defence. In this context, adopting STIX and TAXII emerges not merely as a technical enhancement, but as a strategic investment with clear and compelling business outcomes. The first and most significant transformation enabled by STIX and TAXII is the shift from reactive, indicator-based monitoring to proactive, intelligence-led risk management. Traditional fraud and AML systems typically rely on static rules, thresholds, and blacklists — often unable to adapt to fast-evolving tactics. STIX enables organisations to structure and contextualise threat intelligence in a machine-readable, shareable format. This allows for real-time identification of patterns, behaviours, and entities associated with financial crime, long before damage occurs. The resulting improvement in fraud detection accuracy and speed directly reduces financial losses, enhances customer trust, and positions the organisation as a proactive steward of financial integrity.

Beyond detection, STIX and TAXII break down internal silos that typically divide cybersecurity, fraud, and compliance teams. These domains often operate on different platforms, under separate governance, and with limited shared context — despite facing a common adversary. STIX provides a shared language that allows these teams to integrate their intelligence feeds, enrich investigations, and coordinate responses around common entities such as bank accounts, cryptocurrency wallets, devices, IP addresses, or behavioural anomalies. This cross-functional visibility is critical in uncovering multi-stage attack chains, such as credential phishing followed by account takeover and subsequent laundering of stolen funds. From an operational standpoint, this integration leads to faster root cause identification, fewer missed links, and a more unified response to emerging threats.

Critically, STIX and TAXII also unlock the ability to collaborate at scale across the financial ecosystem. Threat actors do not limit themselves to a single bank, jurisdiction, or payment rail. A single mule network may span dozens of institutions and countries. TAXII enables secure, automated sharing of fraud and AML intelligence between financial institutions, information sharing groups (such as FS-ISAC), and public-sector partners like financial intelligence units (FIUs) and law enforcement. This level of collaboration — previously limited by legal, technical, or operational barriers — creates a collective defence posture in which early warnings can be disseminated, coordinated actions taken, and systemic risks contained. From a business perspective, such collaboration reduces the chance of being the “last to know,” and enhances the organisation’s resilience to industry-wide threats. Efficiency gains are another significant outcome of STIX/TAXII adoption. Today, fraud and AML teams are often overwhelmed by alerts, many of which are false positives or poorly prioritised. Manually triaging and investigating these alerts is time-consuming and resource-intensive. By ingesting structured threat intelligence in STIX format, systems such as SIEMs, transaction monitoring platforms, and case management tools can automatically correlate new activity with known fraud patterns, mule identifiers, or cyber compromise events. This automation enables triaged alerts to be pre-enriched with contextual intelligence, significantly reducing investigation time. High-confidence indicators can even trigger predefined actions, such as freezing a transaction, escalating a case, or requiring enhanced due diligence. These operational efficiencies translate into lower costs per case, better use of skilled analysts, and faster resolution times.

Lastly, and importantly, investing in STIX and TAXII supports regulatory alignment and audit readiness. Global frameworks such as the FATF Recommendations, EU’s AML Directives, FinCEN guidelines, and DORA increasingly emphasise intelligence sharing, early risk detection, and collaborative defence. Implementing STIX and TAXII demonstrates maturity in both governance and risk intelligence capabilities. It shows regulators that the organisation is taking concrete, structured steps to identify, assess, and mitigate emerging financial crime risks. Furthermore, it enhances the quality and timeliness of suspicious activity reporting (SARs/STRs), especially when combined with evidence drawn from shared intelligence sources.

9 Conclusion

The STIX-AML extension provides a standardised, machine-readable framework for sharing financial crime intelligence, aligning with global and regional regulations such as AMLD5, AMLD6, and FATF Recommendations. By incorporating attributes for both AML and fraud within objects like `x-suspiciousactivities`, `x-kycindividual`, and `x-kybbusiness`, it enables seamless data exchange among financial institutions, supervisory authorities (e.g., FIU-NL, CTIF-CFI, BaFin), and law enforcement, fostering cross-border collaboration. Benefits include improved interoperability, automated compliance processes, and enhanced pattern recognition to detect evolving financial crimes, from initial fraud insights to complex money laundering schemes.

Future directions for the STIX-AML extension include:

- **Incorporating Feedback**: Continue engaging with regulators, financial institutions, and technology vendors to refine attributes and ensure alignment with diverse compliance needs.
- **Expanding Technological Support**: Integrating support for emerging technologies, such as blockchain analytics, to enhance the tracking of cryptocurrency-related suspicious activities.
- **Promoting Community Adoption**: Encouraging widespread adoption through open collaboration with the AML and fraud prevention communities to establish a robust, standardised framework.

In conclusion, building STIX and TAXII infrastructure is not just a technical initiative — it is a high-leverage strategic investment. It strengthens the organisation's capacity to detect and prevent fraud and laundering, fosters integrated intelligence sharing across teams and institutions, reduces operational overhead, and supports compliance in a rapidly evolving regulatory environment. In a landscape where financial crime is increasingly sophisticated, fast-moving, and interconnected, the ability to act on timely, structured, and actionable intelligence is not optional — it is a critical differentiator for resilience, trust, and long-term value.

We invite organisations to review and contribute to this draft to ensure it meets the diverse needs of the financial crime prevention ecosystem. To provide feedback or collaborate, please reach out via our contact page at https://njordium.com/reach-out/ or email us at reachout@njordium.com. Your input is critical to shaping a framework that strengthens the fight against financial crimes across the EU and beyond.

10 Acronyms

Acronym	Full Form	Explanation
AML	Anti-Money Laundering	A set of regulations and processes aimed at preventing the concealment of illegally obtained funds, often involving ongoing monitoring of customer financial activities to detect suspicious behaviour.
AMLD	Anti-Money Laundering Directive	A series of EU directives (e.g., AMLD5, AMLD6) establishing AML and CFT regulations, harmonising rules across member states for financial crime prevention.
AMLD5	Fifth Anti-Money Laundering Directive	An EU directive strengthening AML regulations, including enhanced transparency for beneficial ownership and virtual currency transactions, effective from 2020.
AMLD6	Sixth Anti-Money Laundering Directive	An EU directive further harmonising AML rules, introducing stricter penalties and expanding criminal liability, effective from 2021.
BO	Beneficial Owner	An individual who ultimately owns or controls a business entity or benefits from its activities, critical for KYB transparency under AML regulations.
BOI	Beneficial Ownership Information	Data identifying individuals who ultimately own or control a business entity, critical for KYB compliance and transparency under AML regulations.
BSA	Bank Secrecy Act	A U.S. law requiring financial institutions to report suspicious activities and maintain records to assist in detecting and preventing money laundering and fraud.
CDD	Customer Due Diligence	A core component of AML and KYC, involving the collection and verification of customer information to assess risks and ensure compliance with regulatory requirements.
CFT	Countering the Financing of Terrorism	Measures to prevent and detect the funding of terrorist activities, often integrated with AML frameworks to monitor and report suspicious financial flows.
CIFAS	Credit Industry Fraud Avoidance System	A UK-based fraud prevention service that maintains a database of fraudulent activities, used by financial institutions to share and mitigate fraud risks.
CRA	Cyber Resilience Act	An EU regulation aimed at ensuring cybersecurity for digital products, relevant to secure data management in financial crime prevention systems.
CTA	Corporate Transparency Act	A U.S. law requiring certain businesses to report BOI to FinCEN, referenced in the draft for KYB processes involving U.S.-related entities.
CTIF-CFI	Cellule de Traitement des Informations Financières - Cel voor Financiële Informatieverwerking	The Belgian FIU responsible for analysing SARs and coordinating AML efforts, referenced in the draft for cross-border collaboration.
CTR	Currency Transaction Report	A report filed with a Financial Intelligence Unit (FIU) for transactions exceeding a certain threshold (e.g., $10,000 in the U.S.), mandated to monitor large cash movements.
DEA	Drug Enforcement Administration	A U.S. agency focused on combating drug trafficking and related money laundering, often involved in AML investigations.

Acronym	Full Form	Explanation
DORA	Digital Operational Resilience Act	An EU regulation enhancing cybersecurity and operational resilience for financial entities, complementing AML data protection requirements.
EBA	European Banking Authority	An EU agency promoting regulatory convergence in banking, including AML/CFT compliance, and issuing guidelines for financial institutions.
EDD	Enhanced Due Diligence	Additional verification measures applied to high-risk customers or transactions, such as PEPs or complex business structures, to mitigate AML and fraud risks.
ESMA	European Securities and Markets Authority	An EU agency overseeing securities markets, ensuring AML/CFT compliance and investor protection in financial markets.
EUROPOL	European Union Agency for Law Enforcement Cooperation	An EU agency coordinating cross-border investigations, including financial crimes, supporting AML and fraud prevention efforts.
FATF	Financial Action Task Force	An intergovernmental organisation that sets global standards for combating money laundering, terrorist financing, and other financial crimes, influencing EU and national regulations.
FCA	Financial Conduct Authority	The UK's financial regulatory body, enforcing AML, fraud prevention, and consumer protection standards in financial services.
FCP	Financial Crime Prevention	A broad term encompassing AML, CFT, fraud prevention, and other measures to protect financial systems from illicit activities.
FI	Finansinspektionen	Sweden's Financial Supervisory Authority, responsible for overseeing AML and financial compliance in the Swedish financial sector.
FinCEN	Financial Crimes Enforcement Network	A U.S. agency under the Treasury Department that collects and analyses financial intelligence, including BOI and SARs, to combat financial crimes.
FINRA	Financial Industry Regulatory Authority	A U.S. non-governmental organisation regulating broker-dealers, enforcing AML compliance and fraud prevention in the securities industry.
FIU	Financial Intelligence Unit	A national agency responsible for receiving, analysing, and disseminating SARs and other financial intelligence to combat money laundering and terrorist financing (e.g., FIU-NL in the Netherlands).
FRA	Fraud Risk Assessment	A process to evaluate and mitigate risks of fraudulent activities, often integrated with AML and KYC processes to identify suspicious patterns.
FSA	Financial Supervisory Authority	A national regulator overseeing financial institutions' compliance with AML, KYC, and other regulations (e.g., Finansinspektionen in Sweden).
FT	Financing of Terrorism	Another term for terrorist financing, used interchangeably with TF in AML/CFT regulations to describe funding for terrorist activities.
GDPR	General Data Protection Regulation	An EU regulation governing data protection and privacy, requiring secure and compliant handling of personal data in AML, KYC, and KYB processes.

Acronym	Full Form	Explanation
Hawala	Informal Value Transfer System	An informal, trust-based system for transferring money without physical movement, often used in regions with limited banking infrastructure, posing AML challenges.
IBAN	International Bank Account Number	A standardised format for identifying bank accounts internationally, used in the draft to document banking relationships in KYC, KYB, and suspicious activities.
INTERPOL	International Criminal Police Organisation	An international organisation facilitating global police cooperation, including investigations of money laundering and terrorist financing.
JIT	Joint Investigation Team	A collaborative team of law enforcement agencies from multiple jurisdictions, often formed for complex financial crime investigations under EU frameworks like Eurojust.
KYB	Know Your Business	The process of verifying the identity and structure of business entities, including beneficial owners, to ensure compliance with AML and fraud prevention regulations.
KYC	Know Your Customer	The process of verifying the identity of customers during onboarding, serving as the first step in AML compliance, typically involving a one-time verification (with potential updates based on risk).
LEA	Law Enforcement Agency	A government agency responsible for investigating financial crimes, such as fraud and money laundering, often collaborating with FIUs (e.g., FBI, NCA).
MAS	Monetary Authority of Singapore	Singapore's central bank and financial regulator, enforcing AML/CFT regulations and promoting financial stability.
ML	Money Laundering	The process of concealing the origins of illegally obtained funds, often through layering, to make them appear legitimate; synonymous with AML in regulatory contexts.
NCA	National Crime Agency	The UK's lead agency for combating serious and organised crime, including money laundering and fraud, collaborating with FIUs and international partners.
NGO	Non-Governmental Organisation	A non-profit, independent organisation that operates outside of government control, typically focused on humanitarian, social, environmental, or advocacy missions.
NIS2	Network and Information Security Directive 2	An EU directive strengthening cybersecurity across sectors, relevant to secure data handling in AML and KYC processes.
NSA	National Security Agency	A U.S. agency responsible for signals intelligence, occasionally involved in financial crime investigations related to national security and terrorist financing.
OFAC	Office of Foreign Assets Control	A U.S. agency administering economic sanctions programs, including the SDN list, used globally to screen customers and transactions for compliance.
PEP	Politically Exposed Person	An individual with a prominent public role, subject to enhanced scrutiny in AML processes due to higher risks of corruption or money laundering.
SAR	Suspicious Activity Report	A report filed with an FIU to document transactions or activities suspected of being related to money laundering or fraud, as mandated by AML regulations.
SCDD	Simplified Customer Due Diligence	A streamlined due diligence process applied to low-risk customers or transactions, requiring less extensive verification under AML regulations.

Acronym	Full Form	Explanation
SDN	Specially Designated Nationals	A list maintained by OFAC identifying individuals and entities subject to sanctions, used in AML and KYC screening to prevent illicit financial activities.
SEC	Securities and Exchange Commission	A U.S. regulatory agency overseeing securities markets, enforcing compliance with AML and fraud prevention regulations for financial institutions.
STIX	Structured Threat Information Expression	A standardised, machine-readable format for sharing cyber threat and financial crime intelligence, extended in this draft to support AML, KYC, KYB, and fraud data.
STR	Suspicious Transaction Report	Similar to SAR, a report filed with an FIU to document specific transactions suspected of being linked to money laundering or terrorist financing, used in many jurisdictions.
SWIFT	Society for Worldwide Interbank Financial Telecommunication	A global network for secure financial messaging, with SWIFT codes used in the draft to identify banks in transaction and banking relationship data.
TAXII	Trusted Automated Exchange of Intelligence Information	A protocol for securely sharing STIX-formatted threat intelligence, enabling automated and standardised exchange of AML, KYC, KYB, and fraud data among financial institutions and authorities.
TBML	Trade-Based Money Laundering	A form of money laundering that uses trade transactions, such as over- or under-invoicing, to disguise illicit funds, often requiring enhanced monitoring.
TF	Terrorist Financing	The provision or collection of funds to support terrorist activities, closely monitored under AML/CFT frameworks; synonymous with FT.

11 References

- **EU AMLA (Anti-Money Laundering Authority)**
  - https://www.amla.europa.eu/index_en
- **EU AML Package**
  - AMLD 6 - Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024: https://eur-lex.europa.eu/eli/dir/2024/1640/oj
  - AMLR - Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024: http://data.europa.eu/eli/reg/2024/1624/oj
  - AMLA-R - Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024: http://data.europa.eu/eli/reg/2024/1620/oj
- **Eurojust (European Union Agency for Criminal Justice Cooperation)**
  - https://www.eurojust.europa.eu/
- **European Banking Authority (EBA)**
  - Anti-Money Laundering and Countering the Financing of Terrorism: https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism
- **European Commission (EC)**
  - AML at EU level: https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-countering-financing-terrorism-eu-level_en
- **Financial Action Task Force (FATF)**
  - ALM Recommendations: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
- **Financial Supervisory Authority, Iceland**
  - Anti-Money laundering and Terrorist-Financing: https://www.government.is/topics/public-safety-and-security/aml-cft-policies/
- **Financial Supervisory Authority, Norway**
  - Money laundering and financing of terrorism: https://www.finanstilsynet.no/en/topics/money-laundering-and-financing-of-terrorism/
- **Financial Supervisory Authority, Sweden**
  - AML Guidelines: https://www.fi.se/en/bank/money-laundering/
  - Customer due diligence: https://www.fi.se/en/bank/money-laundering/process--work-method/customer-due-diligence/
- **MISP Threat Sharing**
  - https://www.misp-project.org
- **OASIS**
  - STIX Version 2.1 Specification: https://www.oasis-open.org/standard/6426/
- **Swedish NAO**
  - State supervision to combat money laundering Audit Report (2024-06-03): https://www.riksrevisionen.se/en/audits/audit-reports/2024/state-supervision-to-combat-money-laundering---deficient-in-scope-and-effectiveness.html
- **Swedish Police FIU**
  - https://polisen.se/om-polisen/polisens-arbete/finanspolisen/
- **US Financial Crimes Enforcement Network (FinCEN)**
  - https://www.fincen.gov/resources
  - Bank Secrecy Act: https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act

  - Corporate Transparency Act: https://www.fincen.gov/sites/default/files/shared/Corporate_Transparency_Act.pdf
  - Suspicious Activity Reports (SARs): https://www.fincen.gov/suspicious-activity-reports-sars
- **US Internal Revenue Service (IRS)**
  - List of approved KYC rules: https://www.irs.gov/businesses/international-businesses/list-of-approved-kyc-rules
- **US Office of the Comptroller of the Currency (OCC)**
  - Bank Secrecy Act: https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html