Financial Crime Research: Threat Profiling of Fraud, Corruption, and Money Laundering

A Comprehensive Analysis of High-Impact Threat Scenarios and STIX Attributes for Detection

Created by:
Fraud, Corruption and AML Research Team
Njordium Cyber Group AB

Version:

1.1A

Publish Date:
2025-07-16

"This page is intentionally left blank."

Table of Contents

1 Introduction

Financial crime, encompassing fraud, corruption, and money laundering, represents one of the most significant challenges to the integrity of global economies, financial systems, and societal trust. These three domains, while distinct in their mechanisms, are deeply interconnected, forming a complex web of illicit activities that exploit vulnerabilities in institutions, technology, and governance structures. Fraud, characterised by deceptive practices for unlawful gain, targets individuals and organisations through schemes such as phishing, identity theft, and investment scams. Corruption, the abuse of entrusted power for private benefit, manifests in bribery, embezzlement, and nepotism, undermining public and private sector operations. Money laundering, the process of disguising illicit funds to integrate them into the legitimate economy, enables the proceeds of fraud, corruption, and other crimes to fuel further criminal enterprises. Together, these activities impose staggering economic costs—estimated by the International Monetary Fund to account for 2–5% of global GDP, or $2–5 trillion annually for money laundering alone—and erode confidence in financial and governance systems worldwide.

The interconnected nature of fraud, corruption, and money laundering amplifies their impact, creating a cycle where one crime facilitates another. For instance, fraudulent schemes often generate illicit proceeds that require laundering, while corruption within institutions can enable both fraud and money laundering by weakening oversight and accountability. Globalisation, technological advancements, and the rise of digital financial systems have further complicated the landscape, providing criminals with sophisticated tools to exploit cross-border transactions, anonymised cryptocurrencies, and regulatory gaps. The complexity and scale of these threats necessitate a robust, proactive approach to detection, tracking, and mitigation, underscoring the critical role of financial threat intelligence.

Financial threat intelligence—the systematic collection, analysis, and dissemination of data on financial crime patterns, actors, and tactics—is a cornerstone of effective defence against these threats. Within organisations, such as financial institutions, corporations, and government agencies, detection and tracking systems leverage advanced analytics, machine learning, and frameworks like Structured Threat Information Expression (STIX) to identify suspicious patterns, such as anomalous transactions, spoofed communications, or irregular procurement processes. These systems enable organisations to respond swiftly to emerging threats, minimising financial losses, reputational damage, and operational disruptions. For example, real-time monitoring of transactional data can flag high-risk activities like large, unreported cash transfers or complex layering through shell companies, allowing institutions to intervene before significant harm occurs.

Equally important is the sharing of financial threat intelligence between organisations, including banks, regulatory bodies, law enforcement, and international agencies. Collaborative intelligence-sharing platforms, such as those facilitated by the Financial Action Task Force (FATF) or INTERPOL, enable the aggregation of data on threat actors, criminal networks, and evolving methodologies. This collective approach enhances the ability to detect cross-border schemes, such as trade-based money laundering or international bribery networks, which often evade single-organisation detection systems. By sharing indicators of compromise, such as malicious IP addresses, suspicious account patterns, or known fraud typologies, organisations can build a unified front against financial crime, closing gaps that criminals exploit. Public-private partnerships further amplify this impact,

combining regulatory oversight with industry expertise to create comprehensive threat profiles and response strategies.

The importance of detection, tracking, and sharing financial threat intelligence cannot be overstated. Within organisations, these efforts strengthen internal controls, protect assets, and ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations. Between organisations, intelligence sharing fosters a global ecosystem of resilience, disrupting the financial lifelines of organised crime, terrorist groups, and corrupt entities. However, challenges remain, including data privacy concerns, varying regulatory standards across jurisdictions, and the rapid evolution of criminal tactics. To address these, organisations must invest in interoperable systems, standardised data formats like STIX, and cross-sector collaboration to ensure timely and actionable intelligence. This report explores the high-impact threat scenarios across fraud, corruption, and money laundering, providing detailed profiles and actionable STIX attributes to support detection and prevention. By prioritising financial threat intelligence, stakeholders can safeguard economic stability, uphold governance, and protect societal trust in an increasingly complex financial landscape.

2 Purpose and Scope

The purpose of this research report is to provide a comprehensive analysis of the most prevalent and high-impact threat scenarios across the domains of fraud, corruption, and money laundering, which collectively undermine global financial systems, governance, and societal trust. By detailing 30 threat profiles - 10 for each domain - with in-depth descriptions, impact assessments, cognitive structures, linked criminal networks, and real-world media examples, the report aims to enhance understanding of these financial crimes. It integrates Structured Threat Information Expression (STIX) attributes to map threat behaviours, enabling organisations to detect and track illicit activities effectively. The document serves as a resource for financial institutions, regulators, and policymakers to strengthen detection, prevention, and response strategies through actionable financial threat intelligence. By fostering intra- and inter-organisational intelligence sharing, the report seeks to promote collaborative efforts to disrupt criminal networks, ensure regulatory compliance, and safeguard economic stability.

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. **Data Collection**: The initial step involved reviewing a comprehensive list of threat profiles for fraud, corruption, and money laundering, each detailing threat descriptions, impacts, criminal network links, cognitive structures, media examples, and STIX attributes. These profiles included specific threats like phishing attacks, bribery in public procurement, and cryptocurrency laundering, among others. The task was to identify patterns and common approaches, grouping them into use cases that reflect similar methods. To enhance the analysis, additional research was conducted using web sources to verify and expand on these patterns, ensuring alignment with recognized financial crime trends.
4. **Categorisation Process**: The categorization process began by grouping threats into three main categories: fraud, corruption, and money laundering, based on their primary nature. From there, common methods were identified, such as the use of shell companies, document manipulation, and digital asset misuse, leading to the creation of eight use cases. Each use case was refined using insights from web sources, including Wikipedia, FBI testimonies, FATF reports, and others, to ensure a robust and comprehensive framework.
5. **STIX Compatibility**: Ensuring compatibility with STIX Version 2.1 for seamless integration with existing threat intelligence platforms including with proposed STIX-AML extension.

4 Key Considerations and Dependencies for Effective Financial Threat Intelligence

The success of financial threat intelligence (FTI) in combating fraud, corruption, and money laundering hinges on a robust framework of considerations and dependencies, particularly around data availability, export and import capabilities for intra- and inter-organisational collaboration, and effective threat intelligence reporting. These elements are critical for enabling organisations—such as financial institutions, regulatory bodies, and law enforcement agencies—to detect, track, and mitigate financial crimes. Below, we outline the key considerations and dependencies, addressing technical, operational, and regulatory requirements to ensure FTI systems deliver actionable outcomes. The bottom-line and crucial to remember is the fact that the effectiveness of financial threat intelligence in combating fraud, corruption, and money laundering depends on robust data availability, seamless export and import capabilities for intra- and inter-organisational collaboration, and high-quality threat intelligence reporting. By addressing these considerations, ensuring data quality, standardisation, security, and compliance, organisations can build resilient FTI frameworks. Dependencies on technology, skilled personnel, and trusted networks underscore the need for strategic investment and collaboration. Through these efforts, stakeholders can disrupt criminal networks, enhance regulatory compliance, and safeguard the integrity of global financial systems.

4.1 Data Availability

Data availability is the cornerstone of effective FTI, as it underpins the ability to identify, analyse, and respond to threat patterns across fraud, corruption, and money laundering.

Key considerations include:

Data Sources and Quality: Comprehensive FTI relies on diverse, high-quality data sources, including transactional records, customer profiles, know-your-customer (KYC) data, public records, and external threat intelligence feeds (e.g., from INTERPOL or the Financial Action Task Force). Data must be accurate, timely, and complete to enable precise detection of suspicious activities, such as anomalous transfers or shell company transactions. Incomplete or outdated data can lead to false negatives, allowing threats to go undetected.

Data Standardisation: To facilitate analysis, data must be structured in standardised formats, such as Structured Threat Information Expression (STIX) 2.1, which supports objects like Indicators, Observables, and Attack Patterns. For example, STIX attributes like [transaction:amount > 10000] or [url:value MATCHES '.phish.'] enable consistent threat profiling. Non-standardised data formats hinder integration and analysis, reducing FTI effectiveness.

Data Accessibility: Organisations must ensure data is accessible to authorised personnel and systems while complying with privacy regulations (e.g., GDPR, CCPA). Secure data storage solutions, such as encrypted databases, and access controls (e.g., role-based access) are critical to prevent unauthorised access while enabling real-time analysis.

Real-Time Data: Financial crimes evolve rapidly, necessitating real-time or near-real-time data feeds. For instance, monitoring blockchain transactions for cryptocurrency laundering or detecting high-frequency fund transfers in investment scams requires low-latency data pipelines. Delays in data availability can allow criminals to complete transactions before detection.

Dependency on External Data: Internal data (e.g., bank transaction logs) must be supplemented with external sources, such as dark web marketplaces, sanctions lists, or global trade records. Dependencies on third-party providers, such as threat intelligence vendors, require reliable APIs and service-level agreements (SLAs) to ensure consistent data availability.

Export and Import Capabilities for Intra-Organisational Collaboration Intra-organisational collaboration—within a single entity, such as a bank or government agency—requires seamless export and import capabilities to share FTI across departments (e.g., compliance, fraud detection, IT security). Key considerations include:

Data Export Formats: FTI systems must export data in interoperable formats like STIX/TAXII (Trusted Automated eXchange of Indicator Information) to ensure compatibility across internal tools. For example, exporting phishing indicators ([url:value MATCHES '.phish.']) in STIX format allows the fraud team to integrate them into monitoring systems. Proprietary formats can create silos, hampering collaboration.

Data Import Integration: Internal systems, such as anti-money laundering (AML) platforms or customer relationship management (CRM) tools, must support importing FTI data. This requires APIs or middleware to parse and integrate STIX objects into existing workflows. For instance, importing suspicious transaction patterns ([transaction:status = 'unreported']) into a bank's transaction monitoring system enables real-time alerts.

Automation and Scalability: Intra-organisational FTI sharing benefits from automated export/import pipelines to handle large data volumes. For example, a bank processing millions of transactions daily needs automated systems to export and import threat indicators without manual intervention. Scalable cloud-based solutions, such as AWS or Azure, can support this requirement.

Data Security: Exporting and importing sensitive data (e.g., customer PII or transaction details) within an organisation requires encryption (e.g., AES-256) and secure transfer protocols (e.g., HTTPS, SFTP). Weak security measures risk data breaches, undermining trust and compliance.

Dependency on Internal Infrastructure: Effective intra-organisational collaboration depends on robust IT infrastructure, including data lakes, secure APIs, and analytics platforms. Legacy systems lacking modern integration capabilities can hinder FTI sharing, necessitating upgrades or middleware solutions.

4.2 Export and Import Capabilities for Inter-Organisational Collaboration

Inter-organisational collaboration - between banks, regulators, law enforcement, and international bodies—is critical for tackling cross-border financial crimes like trade-based money laundering or bribery networks.

Key considerations include:

Standardised Protocols: Inter-organisational FTI sharing relies on standardised protocols like STIX/TAXII or ISACs (Information Sharing and Analysis Centres). For example, a bank sharing indicators of a romance scam ([transaction:amount > 1000]) with a regulator via TAXII ensures compatibility. Lack of standardisation fragments intelligence efforts.

Secure Sharing Mechanisms: Sharing sensitive FTI between organisations requires secure platforms, such as encrypted TAXII servers or blockchain-based ledgers, to protect data integrity and

confidentiality. Public-private partnerships, like the Financial Services ISAC (FS-ISAC), provide trusted channels for sharing threat indicators.

Data Anonymisation: To comply with privacy regulations, exported FTI must often be anonymised, removing sensitive details like customer names while retaining threat patterns (e.g., [crypto-address:value MATCHES '*']). Tools like data masking or pseudonymisation are essential to balance privacy and utility.

Cross-Jurisdictional Challenges: Inter-organisational sharing across borders faces regulatory hurdles, such as differing AML/CTF (Counter-Terrorism Financing) requirements. Harmonising data-sharing agreements, as promoted by FATF, is critical to ensure compliance while enabling collaboration.

Dependency on Trust Networks: Effective inter-organisational sharing depends on trusted relationships, often facilitated by organisations like FATF, INTERPOL, or regional ISACs. Establishing trust frameworks, including SLAs and legal agreements, is essential to ensure reliable data exchange.

Threat Intelligence Reporting Effective threat intelligence reporting transforms raw FTI into actionable insights for stakeholders within and across organisations. Key considerations include:

Report Structure and Clarity: Reports must be structured, concise, and tailored to the audience (e.g., compliance officers, executives, or law enforcement). For example, a report on procurement fraud should include threat descriptions, STIX attributes ([transaction:recipient MATCHES '*']), and media examples to contextualise risks. Unclear or overly technical reports reduce usability.

Timeliness: Timely reporting is critical to address fast-evolving threats like phishing or cryptocurrency laundering. Automated reporting tools, integrated with FTI platforms, can generate real-time alerts or periodic summaries to keep stakeholders informed.

Actionable Insights: Reports must provide actionable recommendations, such as updating detection rules or flagging specific accounts. For instance, a report on cash smuggling should include STIX indicators ([transaction:type = 'cash']) and suggested monitoring thresholds to guide response efforts.

Visualisation and Accessibility: Effective reports leverage visualisations, such as graphs of transaction flows or heatmaps of threat patterns, to enhance understanding. Accessible formats, like PDF or HTML, ensure reports can be shared across systems and organisations.

Dependency on Analytics Tools: High-quality reporting relies on advanced analytics platforms (e.g., Splunk, Palantir) to process FTI data and generate insights. Dependencies on skilled analysts and visualisation tools are critical to produce meaningful reports.

4.3 Additional Considerations and Dependencies

Regulatory Compliance: FTI systems must comply with global and regional regulations, such as AML/CTF laws, GDPR, and FATF recommendations. Non-compliance risks fines and reputational damage, making legal expertise a key dependency.

Skilled Workforce: Effective FTI requires trained analysts, data scientists, and compliance officers to interpret and act on intelligence. Dependencies on training programs and talent acquisition are critical to address skill shortages.

Technology Integration: FTI systems depend on integration with existing technologies, such as transaction monitoring systems, blockchain analytics tools, and machine learning models. Compatibility issues can disrupt workflows, requiring robust IT support.

Scalability and Resilience: As financial crimes evolve, FTI systems must scale to handle increasing data volumes and adapt to new threats, such as AI-driven fraud. Cloud infrastructure and modular architectures are essential dependencies.

Cost Considerations: Implementing FTI systems, including data platforms, analytics tools, and sharing protocols, involves significant costs. Organisations must balance investment with expected outcomes, often relying on cost-sharing models in inter-organisational collaborations.

5 How to use this document

This research report, titled "Financial Crime Research: Threat Profiling of Fraud, Corruption, and Money Laundering" provides a comprehensive analysis of 30 high-impact threat scenarios across fraud, corruption, and money laundering, complete with detailed threat descriptions, impact assessments, cognitive structures, linked criminal networks, media examples, and Structured Threat Information Expression (STIX) attributes. Designed for financial institutions, regulatory bodies, law enforcement agencies, policymakers, and other stakeholders, the document serves as a critical resource for enhancing financial threat intelligence (FTI). Below is a guide on how to use this report constructively to strengthen detection, prevention, and collaboration efforts in combating financial crime. This research report is a versatile tool for combating financial crime, offering actionable insights for detection, prevention, and collaboration. By leveraging its threat profiles, STIX attributes, and real-world examples, stakeholders can enhance intra- and inter-organisational efforts, strengthen compliance, and build resilience against fraud, corruption, and money laundering. Constructive use of the document involves integrating its findings into operational workflows, sharing intelligence with trusted partners, and fostering a culture of vigilance and continuous improvement. Through these efforts, organisations can protect financial systems, uphold governance, and safeguard societal trust.

5.1 Understanding the Threat Landscape

Objective: Gain a comprehensive understanding of fraud, corruption, and money laundering threats to inform risk management and strategic planning.

Application: Review the "Common Problem Description" section to grasp the interconnected nature of these crimes and their impacts on financial systems, governance, and societal trust. Use the 10 threat scenarios per domain (30 total) in sections 3, 4, and 5 to identify specific risks relevant to your organisation. For example, financial institutions can focus on fraud scenarios like phishing attacks or payment card fraud, while government agencies may prioritise corruption threats like bribery in public procurement.

Action Steps:

Map the listed threat scenarios to your organisation’s operations to assess exposure. For instance, banks can evaluate their vulnerability to invoice fraud or cryptocurrency laundering.

Use the cognitive structure (intention, purpose, threatful action, negative outcome) for each threat to understand criminal motivations and anticipate attack vectors.

Reference media examples (e.g., the 2023 PayPal phishing campaign or the 2021 Equifax breach) to contextualise real-world implications and benchmark against known cases.

5.2 Leveraging STIX Attributes for Detection

Objective: Enhance detection capabilities by integrating STIX attributes into monitoring and analytics systems.

Application: Each threat scenario includes STIX 2.1 attributes (Indicators, Observables, Attack Patterns) tailored to specific behaviours, such as [url:value MATCHES '.phish.'] for phishing or [transaction:amount > 1000000] for real estate laundering. These attributes can be incorporated

into transaction monitoring systems, cybersecurity platforms, or AML software to flag suspicious activities.

Action Steps:

1. Import STIX attributes into your organisation's threat detection tools, such as Splunk, Palantir, or custom AML platforms, to create rules for real-time monitoring. For example, configure alerts for [transaction:type = 'cash'] to detect cash smuggling.
2. Use Observables (e.g., email headers, blockchain transactions) to enrich existing datasets and improve pattern recognition.
3. Map Attack Patterns (e.g., T1566 for phishing, T1657 for financial theft) to the MITRE ATT&CK framework to align with industry-standard cybersecurity practices.

5.3 Strengthening Intra-Organisational Collaboration

Objective: Foster collaboration across internal departments to enhance response to financial crime.

Application: Share the report's threat profiles and STIX attributes with relevant teams, such as compliance, fraud detection, IT security, and risk management, to align efforts. For example, the procurement fraud scenario can inform both the compliance team (to update vendor vetting processes) and the IT team (to monitor for anomalous transaction patterns).

Action Steps:

1. Distribute relevant sections of the report to department heads, ensuring they understand specific threats (e.g., payroll fraud for HR, insider trading for finance teams).
2. Use the report's structured format to create internal training materials, highlighting cognitive structures to educate staff on criminal tactics.
3. Implement automated workflows to share STIX-based indicators across internal systems, ensuring seamless integration into existing tools like CRM or transaction monitoring platforms.

5.4 Facilitating Inter-Organisational Collaboration

Objective: Enhance cross-organisational intelligence sharing to combat complex, cross-border financial crimes.

Application: The report's STIX attributes and threat profiles can be shared with external partners, such as other financial institutions, regulators, or law enforcement, via platforms like TAXII or FS-ISAC. For instance, sharing indicators of trade-based money laundering ([invoice:value MATCHES '*']) with other banks can help disrupt international cartels.

Action Steps:

1. Export STIX attributes to trusted sharing platforms (e.g., TAXII servers) to contribute to industry-wide threat intelligence. Ensure data is anonymised to comply with privacy regulations like GDPR.
2. Participate in public-private partnerships or ISACs to share and receive threat intelligence, using the report's media examples to align with known cases.
3. Collaborate with international bodies like FATF or INTERPOL, referencing the report's examples (e.g., 2023 Cyprus bank case) to support joint investigations.

5.5 Enhancing Threat Intelligence Reporting

Objective: Use the report as a template for creating actionable, high-quality FTI reports.

Application: The report's structure—combining threat descriptions, impacts, and STIX attributes—provides a model for generating internal and external FTI reports. Stakeholders can adapt this format to document new threats or update existing ones, ensuring clarity and actionability.

Action Steps:

1. Use the report's layout to create periodic FTI reports, incorporating visualisations like transaction flow diagrams or risk heatmaps to enhance stakeholder understanding.
2. Tailor report sections to specific audiences (e.g., executives for high-level summaries, analysts for technical STIX details).
3. Reference the report's bibliography to source credible data for your own reports, ensuring alignment with authoritative sources like IMF or FATF.

5.6 Supporting Policy and Compliance Efforts

Objective: Inform regulatory compliance and policy development to strengthen anti-financial crime frameworks.

Application: The report's detailed threat profiles and references (e.g., FATF's 2012 Methods and Trends) can guide compliance teams in updating AML/CTF policies. Policymakers can use the report to advocate for stronger regulations targeting emerging threats like cryptocurrency laundering.

Action Steps:

1. Align internal AML/CTF policies with the report's threat scenarios, ensuring coverage of risks like hawala systems or charity laundering.
2. Use the report's STIX attributes to demonstrate compliance with regulatory requirements for threat monitoring and reporting.
3. Leverage media examples to support advocacy for stricter regulations, citing cases like the 2022 London property laundering scandal to highlight real-world impacts.

5.7 Training and Awareness

Objective: Build organisational capacity to recognise and respond to financial crime threats.

Application: The report's comprehensive threat descriptions and cognitive structures can be used to develop training programs for employees, from frontline staff to senior management. For example, the romance scam scenario can inform customer-facing teams about social engineering tactics.

Action Steps:

1. Create training modules based on the report's threat profiles, emphasising real-world examples to illustrate risks.
2. Use cognitive structures to train staff on recognising criminal intent and outcomes, enhancing vigilance against threats like extortion or insider trading.
3. Conduct tabletop exercises using the report's scenarios to simulate responses to threats like phishing or procurement fraud.

5.8 Continuous Improvement and Adaptation

Objective: Use the report as a foundation for ongoing FTI refinement and adaptation to evolving threats.

Application: The report's structure and STIX attributes provide a baseline for monitoring new and emerging threats. Organisations can update threat profiles as criminal tactics evolve, such as adapting to new cryptocurrency laundering techniques.

Action Steps:

1. Regularly update STIX indicators based on new intelligence, ensuring detection systems remain current.
2. Monitor media and industry reports to identify new cases, adding them to the report's framework to maintain relevance.
3. Use the report's conclusion on the value of FTI to advocate for sustained investment in analytics, training, and collaboration tools.

6 Fraud Scenarios

Fraud represents a pervasive threat to individuals, businesses, and financial systems worldwide, characterised by deceptive practices aimed at securing unlawful financial or personal gain. This multifaceted crime encompasses a range of activities, from phishing and identity theft to investment scams and invoice fraud, exploiting trust and technological vulnerabilities. The global impact of fraud is staggering, with losses amounting to billions annually, eroding consumer confidence and straining institutional resources. Understanding the tactics, motivations, and networks behind fraudulent activities is essential for developing effective detection and prevention strategies, safeguarding economic stability and public trust. Below are ten threat profiles of fraud which can be identified, tracked and reported.

6.1 Phishing Attacks

Threat Description: Phishing attacks involve cybercriminals sending fraudulent emails, texts, or other communications posing as legitimate entities to steal sensitive information like login credentials or financial details.

Impact Explanation: These attacks compromise personal and organisational data, leading to financial losses and identity theft. In 2021, phishing caused $5.8 billion in consumer losses in the U.S. alone.

Link to Criminal Network: Organised cybercrime syndicates.

Cognitive Structure:

- Intention: Steal sensitive information.
- Purpose: Gain unauthorised access to financial accounts or sell data.
- Threatful Action: Distribute malicious links or attachments.
- Negative Outcome: Financial loss, data breaches, and identity theft. Media Example: In 2023, a phishing campaign targeting PayPal users stole millions in credentials.

STIX Attributes:

- Indicator: Malicious URLs or email addresses (pattern: [url:value MATCHES '*.phish.*']).
- Observable: Email headers, IP addresses of C2 servers.
- Attack Pattern: T1566 (Phishing).

6.2 Identity Theft

Threat Description: Criminals steal personal information to impersonate victims for financial gain.

Impact Explanation: Victims face unauthorised transactions and credit damage, while institutions incur fraud losses.

Link to Criminal Network: Dark web marketplaces.

Cognitive Structure:

- Intention: Obtain personal data.
- Purpose: Execute unauthorised transactions.
- Threatful Action: Use stolen credentials for purchases or loans.
- Negative Outcome: Financial loss and reputational damage. Media Example: The 2021 Equifax breach exposed 147 million identities.

STIX Attributes:

- Indicator: Stolen PII on dark web (pattern: [user-account:credential MATCHES '*']).
- Observable: Unauthorised account access logs.
- Attack Pattern: T1078 (Valid Accounts).

6.3 Payment Card Fraud

Threat Description: Criminals use stolen credit card details for unauthorised transactions.
Impact Explanation: Financial institutions face chargeback costs, and consumers lose trust.
Link to Criminal Network: Carding rings.
Cognitive Structure:

- Intention: Acquire card details.
- Purpose: Conduct fraudulent purchases.
- Threatful Action: Use stolen cards online or in-store.
- Negative Outcome: Financial losses and eroded trust. Media Example: 2022 Target card skimming attack.

STIX Attributes:

- Indicator: Card data sales on dark web (pattern: [credit-card:number MATCHES '*']).
- Observable: POS terminal tampering.
- Attack Pattern: T1557 (Man-in-the-Middle).

6.4 Investment Scams

Threat Description: Fraudsters promote fake investment opportunities promising high returns.
Impact Explanation: Victims lose life savings, destabilising personal finances.
Link to Criminal Network: Ponzi scheme operators.
Cognitive Structure:

- Intention: Deceive investors.
- Purpose: Collect funds for personal gain.
- Threatful Action: Promote fraudulent schemes.
- Negative Outcome: Massive financial losses. Media Example: Bernie Madoff Ponzi scheme, 2008.

STIX Attributes:

- Indicator: Fake investment websites (pattern: [url:value MATCHES '*.invest.*']).
- Observable: High-frequency fund transfers.
- Attack Pattern: T1657 (Financial Theft).

6.5 Romance Scams

Threat Description: Scammers build fake romantic relationships to extort money.
Impact Explanation: Emotional and financial harm to victims, often elderly.
Link to Criminal Network: Human trafficking-linked groups.
Cognitive Structure:

- Intention: Exploit trust.
- Purpose: Extract funds.
- Threatful Action: Manipulate victims via communication.
- Negative Outcome: Financial and emotional distress. Media Example: 2024 INTERPOL-reported romance scams.

STIX Attributes:

- Indicator: Suspicious payment requests (pattern: [transaction:amount > 1000]).
- Observable: Fake social media profiles.
- Attack Pattern: T1566.002 (Spearphishing Link).

6.6 Invoice Fraud

Threat Description: Fraudsters send fake invoices to businesses for payment.
Impact Explanation: Businesses lose funds, disrupting operations.
Link to Criminal Network: Business email compromise (BEC) groups.
Cognitive Structure:

- Intention: Deceive accounts payable.
- Purpose: Divert funds.
- Threatful Action: Send fraudulent invoices.
- Negative Outcome: Financial loss. Media Example: 2023 BEC scam targeting U.S. firms.

STIX Attributes:

- Indicator: Spoofed email domains (pattern: [email:from MATCHES '*.fake.*']).
- Observable: Altered bank details in emails.
- Attack Pattern: T1566.001 (Spearphishing Attachment).

6.7 Insurance Fraud

Threat Description: False claims filed to obtain insurance payouts.
Impact Explanation: Increased premiums and insurer losses.
Link to Criminal Network: Organised fraud rings.
Cognitive Structure:

- Intention: Fabricate claims.
- Purpose: Obtain payouts.
- Threatful Action: Submit false documentation.
- Negative Outcome: Financial strain on insurers. Media Example: 2021 Home Health Care fraud case.

STIX Attributes:

- Indicator: Fake medical claims (pattern: [document:type = 'claim']).
- Observable: Inconsistent medical records.
- Attack Pattern: T1657 (Financial Theft).

6.8 Cryptocurrency Fraud

Threat Description: Scammers exploit crypto platforms for theft or scams.
Impact Explanation: Loss of investor funds and market instability.
Link to Criminal Network: Crypto scam networks.
Cognitive Structure:

- Intention: Exploit crypto anonymity.
- Purpose: Steal digital assets.
- Threatful Action: Create fake exchanges or wallets.
- Negative Outcome: Financial loss and market distrust. Media Example: 2023 Binance fraud allegations.

STIX Attributes:

- Indicator: Fake wallet addresses (pattern: [crypto-address:value MATCHES '*']).
- Observable: Suspicious blockchain transactions.
- Attack Pattern: T1496 (Resource Hijacking).

6.9 Payroll Fraud

Threat Description: Employees or insiders manipulate payroll systems for personal gain.
Impact Explanation: Organisational losses and internal trust erosion.
Link to Criminal Network: Insider threat actors.
Cognitive Structure:

- Intention: Manipulate payroll records.
- Purpose: Divert funds.
- Threatful Action: Alter employee data.
- Negative Outcome: Financial loss. Media Example: 2022 corporate payroll scam.

STIX Attributes:

- Indicator: Unauthorised payroll changes (pattern: [database:change = 'unauthorized']).
- Observable: Anomalous payroll transactions.
- Attack Pattern: T1078 (Valid Accounts).

6.10 Procurement Fraud

Threat Description: Collusion or manipulation in procurement processes to Favor certain vendors.
Impact Explanation: Inflated costs and poor-quality services.
Link to Criminal Network: Corrupt corporate insiders.
Cognitive Structure:

- Intention: Rig procurement.
- Purpose: Secure kickbacks.
- Threatful Action: Manipulate bidding processes.
- Negative Outcome: Financial waste and inefficiency. Media Example: 2021 public procurement scandal.

STIX Attributes:

- Indicator: Anomalous vendor payments (pattern: [transaction:recipient MATCHES '*']).
- Observable: Irregular bidding patterns.
- Attack Pattern: T1657 (Financial Theft).

4. Corruption Threat Scenarios

7 Corruption Scenarios

Corruption, defined as the abuse of entrusted power for private gain, undermines the foundations of governance, economic development, and societal equity. Manifesting through bribery, embezzlement, nepotism, and other illicit practices, corruption distorts public and private sector operations, misallocates resources, and erodes trust in institutions. Its consequences are profound, often exacerbating inequality and hindering sustainable development. Addressing corruption requires a comprehensive understanding of its mechanisms and the networks that perpetuate it, enabling targeted interventions to promote transparency and accountability. Below are ten threat profiles of corruption which can be identified, tracked and reported.

7.1 Bribery in Public Procurement

Threat Description: Public officials accept bribes to favour specific vendors.
Impact Explanation: Loss of public funds, estimated at 10–25% of contract value.
Link to Criminal Network: Organised crime and corrupt officials.
Cognitive Structure:

- Intention: Influence decisions.
- Purpose: Secure contracts.
- Threatful Action: Offer bribes.
- Negative Outcome: Misallocated public resources. Media Example: 2021 UN procurement corruption.

STIX Attributes:

- Indicator: Large payments to officials (pattern: [transaction:amount > 10000]).
- Observable: Suspicious contract awards.
- Attack Pattern: T1657 (Financial Theft).

7.2 Embezzlement of Public Funds

Threat Description: Officials divert public funds for personal use.
Impact Explanation: Undermines public services and trust.
Link to Criminal Network: Corrupt government insiders.
Cognitive Structure:

- Intention: Misappropriate funds.
- Purpose: Personal enrichment.
- Threatful Action: Divert funds to personal accounts.
- Negative Outcome: Reduced public services. Media Example: Sani Abacha case, Nigeria.

STIX Attributes:

- Indicator: Unauthorised fund transfers (pattern: [transaction:destination MATCHES '*']).
- Observable: Anomalous budget withdrawals.
- Attack Pattern: T1657 (Financial Theft).

7.3 Kickbacks in Contracting

Threat Description: Contractors pay officials to secure contracts.
Impact Explanation: Inflated costs and poor project quality.
Link to Criminal Network: Corporate-corrupt official networks.

Cognitive Structure:

- Intention: Secure contracts.
- Purpose: Gain undue advantage.
- Threatful Action: Pay kickbacks.
- Negative Outcome: Financial waste. Media Example: 2023 Dutch bank bribery case.

STIX Attributes:

- Indicator: Suspicious contractor payments (pattern: [transaction:amount MATCHES '*']).
- Observable: Non-competitive contract awards.
- Attack Pattern: T1657 (Financial Theft).

7.4 Nepotism in Hiring

Threat Description: Officials hire unqualified relatives or associates.
Impact Explanation: Inefficiency and reduced organisational performance.
Link to Criminal Network: Insider patronage networks.
Cognitive Structure:

- Intention: Favor associates.
- Purpose: Consolidate power.
- Threatful Action: Appoint unqualified individuals.
- Negative Outcome: Poor governance. Media Example: 2022 government hiring scandal.

STIX Attributes:

- Indicator: Anomalous hiring records (pattern: [employee:relation MATCHES '*']).
- Observable: Unqualified appointee profiles.
- Attack Pattern: T1078 (Valid Accounts).

7.5 Extortion by Officials

Threat Description: Officials demand payments for services or permits.
Impact Explanation: Increased costs for businesses and citizens.
ink to Criminal Network: Corrupt bureaucracies.
Cognitive Structure:

- Intention: Extract payments.
- Purpose: Personal gain.
- Threatful Action: Demand bribes.
- Negative Outcome: Economic inefficiency. Media Example: 2023 Mexico extortion case.

STIX Attributes:

- Indicator: Suspicious cash payments (pattern: [transaction:type = 'cash']).
- Observable: Coerced payment records.
- Attack Pattern: T1657 (Financial Theft).

7.6 Abuse of Power

Threat Description: Officials misuse authority for personal benefit.
Impact Explanation: Erodes public trust and governance.
Link to Criminal Network: Political elites.
Cognitive Structure:

- Intention: Exploit authority.
- Purpose: Gain benefits.

- Threatful Action: Misuse public resources.
- Negative Outcome: Governance failure. Media Example: 2021 IMF-reported abuse case.

STIX Attributes:

- Indicator: Misuse of public assets (pattern: [asset:use = 'unauthorized']).
- Observable: Irregular resource allocation.
- Attack Pattern: T1078 (Valid Accounts).

7.7 Favouritism in Licensing

Threat Description: Officials grant licenses to favoured parties.
Impact Explanation: Unfair market competition and inefficiency.
Link to Criminal Network: Corporate-political networks.
Cognitive Structure:

- Intention: Favor allies.
- Purpose: Gain loyalty or payments.
- Threatful Action: Issue licenses unfairly.
- Negative Outcome: Market distortion. Media Example: 2022 licensing scandal.

STIX Attributes:

- Indicator: Non-competitive licenses (pattern: [license:award MATCHES '*']).
- Observable: Irregular licensing patterns.
- Attack Pattern: T1657 (Financial Theft).

7.8 Fraudulent Audits

Threat Description: Auditors falsify reports to conceal corruption.
Impact Explanation: Undetected fraud and regulatory failures.
Link to Criminal Network: Collusive audit firms.
Cognitive Structure:

- Intention: Conceal misconduct.
- Purpose: Protect corrupt entities.
- Threatful Action: Falsify audit records.
- Negative Outcome: Regulatory gaps. Media Example: 2023 Italian health sector case.

STIX Attributes:

- Indicator: Falsified audit reports (pattern: [document:authenticity = 'false']).
- Observable: Inconsistent financial records.
- Attack Pattern: T1078 (Valid Accounts).

7.9 Insider Trading

Threat Description: Officials use privileged information for stock trading.
Impact Explanation: Market unfairness and investor losses.
Link to Criminal Network: Financial insiders.
Cognitive Structure:

- Intention: Exploit information.
- Purpose: Personal profit.
- Threatful Action: Trade on insider data.
- Negative Outcome: Market instability. Media Example: 2022 insider trading case.

STIX Attributes:

- Indicator: Suspicious stock trades (pattern: [trade:timing MATCHES '*']).
- Observable: Anomalous trading patterns.
- Attack Pattern: T1657 (Financial Theft).

7.10 Patronage Systems

Threat Description: Officials distribute resources to loyalists.
Impact Explanation: Inefficient resource allocation and governance failures.
Link to Criminal Network: Political networks. Cognitive Structure:

- Intention: Reward loyalty.
- Purpose: Maintain power.
- Threatful Action: Allocate resources unfairly.
- Negative Outcome: Public resource misuse. Media Example: 2021 political patronage case.

STIX Attributes:

- Indicator: Biased resource allocation (pattern: [allocation:recipient MATCHES '*']).
- Observable: Unequal resource distribution.
- Attack Pattern: T1078 (Valid Accounts).

8 Money Laundering Scenarios

Anti-money laundering (AML) efforts are critical to combating the processes that disguise the origins of illicit funds, enabling criminals to integrate proceeds into the legitimate economy. Money laundering, often linked to fraud, corruption, and organised crime, threatens financial system integrity and facilitates further criminal activity. With global estimates suggesting money laundering accounts for 2–5% of GDP, robust AML frameworks are essential for detecting and disrupting illicit financial flows. By leveraging intelligence, technology, and international cooperation, AML initiatives aim to protect economies and uphold regulatory standards. Below are ten threat profiles of money laundering which can be identified, tracked and reported.

8.1 Layering through Shell Companies

Threat Description: Criminals use shell companies to obscure illicit funds.
Impact Explanation: Enables crime by hiding proceeds.
Link to Criminal Network: Organised crime syndicates.
Cognitive Structure:

- Intention: Conceal fund origins.
- Purpose: Legitimise illicit funds.
- Threatful Action: Create shell entities.
- Negative Outcome: Financial system abuse. Media Example: 2023 Cyprus bank case.

STIX Attributes:

- Indicator: Shell company transactions (pattern: [company:status = 'shell']).
- Observable: Complex fund transfers.
- Attack Pattern: T1657 (Financial Theft).

8.2 Trade-Based Money Laundering

Threat Description: Over- or under-invoicing trade to move illicit funds.
Impact Explanation: Distorts trade data and evades taxes.
Link to Criminal Network: International trade cartels.
Cognitive Structure:

- Intention: Disguise funds.
- Purpose: Move money across borders.
- Threatful Action: Manipulate trade invoices.
- Negative Outcome: Economic distortion. Media Example: 2021 trade laundering case.

STIX Attributes:

- Indicator: Inconsistent trade invoices (pattern: [invoice:value MATCHES '*']).
- Observable: Irregular trade patterns.
- Attack Pattern: T1657 (Financial Theft).

8.3 Cash Smuggling

Threat Description: Physically moving cash across borders to avoid detection.
Impact Explanation: Bypasses financial oversight.
Link to Criminal Network: Drug cartels.
Cognitive Structure:

- Intention: Avoid detection.

- Purpose: Move illicit funds.
- Threatful Action: Smuggle cash.
- Negative Outcome: Untracked illicit funds. Media Example: 2022 Mexico cash smuggling.

STIX Attributes:

- Indicator: Large cash movements (pattern: [transaction:type = 'cash']).
- Observable: Border cash seizures.
- Attack Pattern: T1657 (Financial Theft).

8.4 Cryptocurrency Laundering

Threat Description: Using cryptocurrencies to anonymise illicit funds.
Impact Explanation: Challenges regulatory oversight.
Link to Criminal Network: Cybercrime groups.
Cognitive Structure:

- Intention: Anonymise funds.
- Purpose: Evade tracking.
- Threatful Action: Use crypto mixers.
- Negative Outcome: Untraceable proceeds. Media Example: 2023 Binance case.

STIX Attributes:

- Indicator: Crypto mixer transactions (pattern: [crypto-transaction:destination MATCHES '*']).
- Observable: Blockchain anomalies.
- Attack Pattern: T1496 (Resource Hijacking).

8.5 Real Estate Laundering

Threat Description: Purchasing property with illicit funds to legitimise them.
Impact Explanation: Inflates property markets and hides crime proceeds.
Link to Criminal Network: Organised crime.
Cognitive Structure:

- Intention: Legitimise funds.
- Purpose: Invest illicit proceeds.
- Threatful Action: Buy high-value properties.
- Negative Outcome: Market distortion. Media Example: 2022 London property case.

STIX Attributes:

- Indicator: High-value property purchases (pattern: [transaction:amount > 1000000]).
- Observable: Anonymous property buyers.
- Attack Pattern: T1657 (Financial Theft).

8.6 Casino Laundering

Threat Description: Using casinos to convert illicit cash into chips and back.
Impact Explanation: Facilitates crime proceeds integration.
Link to Criminal Network: Gambling syndicates.
Cognitive Structure:

- Intention: Cleanse funds.
- Purpose: Legitimise proceeds.
- Threatful Action: Exchange cash for chips.
- Negative Outcome: Untraceable funds. Media Example: 2021 casino laundering case.

STIX Attributes:

- Indicator: Large casino transactions (pattern: [transaction:location = 'casino']).
- Observable: High-frequency chip exchanges.
- Attack Pattern: T1657 (Financial Theft).

8.7 Hawala Systems

Threat Description: Informal value transfer systems to move funds without records.
Impact Explanation: Bypasses AML controls.
Link to Criminal Network: Terrorist financing groups.
Cognitive Structure:

- Intention: Move funds covertly.
- Purpose: Avoid detection.
- Threatful Action: Use hawala networks.
- Negative Outcome: Untracked illicit funds. Media Example: 2023 hawala terror financing.

STIX Attributes:

- Indicator: Informal transfers (pattern: [transaction:method = 'hawala']).
- Observable: Unrecorded fund movements.
- Attack Pattern: T1657 (Financial Theft).

8.8 Charity Laundering

Threat Description: Donating illicit funds to charities for clean returns.
Impact Explanation: Exploits nonprofit trust.
Link to Criminal Network: Terrorist financing networks.
Cognitive Structure:

- Intention: Cleanse funds.
- Purpose: Legitimise proceeds.
- Threatful Action: Donate to complicit charities.
- Negative Outcome: Misused charitable funds. Media Example: 2022 charity laundering case.

STIX Attributes:

- Indicator: Suspicious donations (pattern: [transaction:destination = 'charity']).
- Observable: Anomalous charity transactions.
- Attack Pattern: T1657 (Financial Theft).

8.9 Luxury Goods Laundering

Threat Description: Purchasing luxury goods with illicit funds for resale.
Impact Explanation: Integrates proceeds into legitimate markets.
Link to Criminal Network: Organised crime.
Cognitive Structure:

- Intention: Legitimise funds.
- Purpose: Convert proceeds to assets.
- Threatful Action: Buy high-value goods.
- Negative Outcome: Market distortion. Media Example: 2021 luxury watch laundering.

STIX Attributes:

- Indicator: High-value purchases (pattern: [transaction:amount > 50000]).
- Observable: Resale of luxury goods.

- Attack Pattern: T1657 (Financial Theft).

8.10 Bank Complicity Laundering

Threat Description: Banks knowingly facilitate illicit fund transfers.
Impact Explanation: Undermines financial system integrity.
Link to Criminal Network: Corrupt financial institutions.
Cognitive Structure:

- Intention: Facilitate laundering.
- Purpose: Earn fees or complicity.
- Threatful Action: Process illicit transactions.
- Negative Outcome: Systemic instability. Media Example: 2023 Cypriot bank case.

STIX Attributes:

- Indicator: Suspicious bank transactions (pattern: [transaction:status = 'unreported']).
- Observable: Unreported large transfers.
- Attack Pattern: T1657 (Financial Theft).

9 Conclusion

The interconnected nature of fraud, corruption, and money laundering demands a robust, proactive approach to financial threat intelligence, with structured frameworks like STIX playing a pivotal role. By mapping threat behaviours to STIX attributes, such as [url:value MATCHES '.phish.'] for phishing or [transaction:amount > 1000000] for real estate laundering, organisations can enhance pattern detection, streamline intelligence sharing, and mitigate risks effectively. The proposed STIX-AML extension, championed by Njordium, represents a transformative step forward. This extension introduces specialised data structures, including `x-suspiciousactivities`, `x-kycindividual`, and `x-kybbusiness`, tailored to AML, know-your-customer, and know-your-business requirements. These structures enable machine-readable, standardised data formats that improve interoperability across cyber threat intelligence platforms, facilitating seamless collaboration within and between organisations. For instance, STIX-AML can standardise transaction patterns and risk indicators, enabling real-time detection of complex threats like cyber-enabled laundering or synthetic identities, while reducing false positives through precise, automated analysis.

By fostering a unified data model, STIX-AML bridges gaps between fraud, cybersecurity, and compliance teams, supporting compliance with EU directives (AMLD5, AMLD6) and FATF standards. This holistic approach, combining data analytics, machine learning, and cross-border collaboration, is essential for disrupting sophisticated criminal networks. However, success hinges on overcoming challenges like data quality, regulatory compliance, and resource limitations.

Organisations should prioritise high-quality, standardised data collection, leveraging frameworks like STIX and STIX-AML to foster intra- and inter-organisational collaboration through secure platforms like TAXII. Regular updates to comply with evolving regulations, investment in skilled personnel and scalable technologies, and proactive monitoring of emerging criminal tactics will strengthen detection and prevention efforts. By adopting Njordium's STIX-AML framework, stakeholders can build resilience against evolving financial crime threats, safeguarding global economies and societal trust.

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 Nomenclature and Abbreviation List

This nomenclature and abbreviation list provides definitions and translations for complex terms and acronyms used in the research report on financial crime, encompassing fraud, corruption, and money laundering. The list is designed to enhance understanding for all stakeholders, including financial institutions, regulatory bodies, law enforcement, and policymakers, by clarifying technical terminology and standardising references to key concepts and frameworks.

This list ensures that complex terms and acronyms are clearly defined, facilitating effective use of the financial crime research report. Stakeholders can reference this nomenclature to interpret technical details, align with industry standards, and enhance collaboration in combating financial crime.

Full format	Acronym	Explanation
Anti-Money Laundering	AML	A set of laws regulations and procedures aimed at preventing criminals from disguising illegally obtained funds as legitimate income involving transaction monitoring customer due diligence and reporting suspicious activities to disrupt illicit financial flows.
Anti-Money Laundering Directive	AMLD	A series of EU directives (e.g. AMLD5 AMLD6) establishing AML and CFT regulations harmonising rules across member states for financial crime prevention.
Attack Pattern		A STIX object describing the tactics techniques and procedures (TTPs) used by threat actors such as T1566 for phishing or T1657 for financial theft based on frameworks like MITRE ATT&CK.
Bank Secrecy Act	BSA	A U.S. law requiring financial institutions to report suspicious activities and maintain records to assist in detecting and preventing money laundering and fraud.
Beneficial Owner	BO	An individual who ultimately owns or controls a business entity or benefits from its activities critical for KYB transparency under AML regulations.
Beneficial Ownership Information	BOI	Data identifying individuals who ultimately own or control a business entity critical for KYB compliance and transparency under AML regulations.
Blockchain Analytics		The use of specialised tools to analyse blockchain transactions for patterns indicative of money laundering or fraud particularly in cryptocurrency-related crimes.
Bribery		The act of offering giving or receiving something of value to influence the actions of an official or other person in a position of power often linked to corruption in public or private sectors.
Business Email Compromise	BEC	A type of fraud where cybercriminals impersonate legitimate business entities via email to deceive organisations into transferring funds or sensitive

Full format	Acronym	Explanation
		information often through fake invoices or spoofed email domains.
California Consumer Privacy Act	CCPA	A U.S. state law that enhances privacy rights and consumer protection for California residents impacting how organisations handle personal data in financial threat intelligence processes.
Cellule de Traitement des Informations Financières - Cel voor Financiële Informatieverwerking	CTIF-CFI	The Belgian FIU responsible for analysing SARs and coordinating AML efforts referenced in the draft for cross-border collaboration.
Command and Control	C2	Infrastructure used by cybercriminals to manage and direct compromised systems or networks often associated with phishing attacks or malware distribution enabling remote control of illicit activities.
Corporate Transparency Act	CTA	A U.S. law requiring certain businesses to report BOI to FinCEN referenced in the draft for KYB processes involving U.S.-related entities.
Countering the Financing of Terrorism	CFT	Measures to prevent and detect the funding of terrorist activities often integrated with AML frameworks to monitor and report suspicious financial flows.
Credit Industry Fraud Avoidance System	CIFAS	A UK-based fraud prevention service that maintains a database of fraudulent activities used by financial institutions to share and mitigate fraud risks.
Cryptocurrency		A digital or virtual currency secured by cryptography increasingly used in financial crimes like fraud and money laundering due to its potential for anonymity.
Currency Transaction Report	CTR	A report filed with a Financial Intelligence Unit (FIU) for transactions exceeding a certain threshold (e.g. $10
Customer Due Diligence	CDD	A core component of AML and KYC involving the collection and verification of customer information to assess risks and ensure compliance with regulatory requirements.
Cyber Resilience Act	CRA	An EU regulation aimed at ensuring cybersecurity for digital products relevant to secure data management in financial crime prevention systems.
Dark Web		A hidden part of the internet accessible only through special software often used for illegal activities like trading stolen data or facilitating fraud and money laundering.
Data Anonymisation		The process of removing or obscuring personally identifiable information from datasets to protect privacy while allowing threat intelligence sharing critical for compliance with GDPR and CCPA.

Full format	Acronym	Explanation
Digital Operational Resilience Act	DORA	An EU regulation enhancing cybersecurity and operational resilience for financial entities complementing AML data protection requirements.
Drug Enforcement Administration	DEA	A U.S. agency focused on combating drug trafficking and related money laundering often involved in AML investigations.
Embezzlement		The misappropriation of funds or property entrusted to an individual typically by public officials or corporate employees for personal gain a common form of corruption.
Enhanced Due Diligence	EDD	Additional verification measures applied to high-risk customers or transactions such as PEPs or complex business structures to mitigate AML and fraud risks.
European Banking Authority	EBA	An EU agency promoting regulatory convergence in banking including AML/CFT compliance and issuing guidelines for financial institutions.
European Securities and Markets Authority	ESMA	An EU agency overseeing securities markets ensuring AML/CFT compliance and investor protection in financial markets.
European Union Agency for Law Enforcement Cooperation	EUROPOL	An EU agency coordinating cross-border investigations including financial crimes supporting AML and fraud prevention efforts.
Fifth Anti-Money Laundering Directive	AMLD5	An EU directive strengthening AML regulations including enhanced transparency for beneficial ownership and virtual currency transactions effective from 2020.
Financial Action Task Force	FATF	An intergovernmental organisation that sets global standards for combating money laundering terrorist financing and other financial crimes promoting policies and intelligence sharing.
Financial Conduct Authority	FCA	The UK's financial regulatory body enforcing AML fraud prevention and consumer protection standards in financial services.
Financial Crime Prevention	FCP	A broad term encompassing AML CFT fraud prevention and other measures to protect financial systems from illicit activities.
Financial Crimes Enforcement Network	FinCEN	A U.S. agency under the Treasury Department that collects and analyses financial intelligence including BOI and SARs to combat financial crimes.
Financial Industry Regulatory Authority	FINRA	A U.S. non-governmental organisation regulating broker-dealers enforcing AML compliance and fraud prevention in the securities industry.
Financial Intelligence Unit	FIU	A national agency responsible for receiving analysing and disseminating SARs other financial intelligence to combat money laundering and terrorist financing (e.g. FIU-NL in the Netherlands).

Full format	Acronym	Explanation
Financial Supervisory Authority	FSA	A national regulator overseeing financial institutions' compliance with AML KYC and other regulations (e.g. Finansinspektionen in Sweden).
Financial Threat Intelligence	FTI	The systematic collection analysis and dissemination of data on financial crime patterns actors and tactics to detect prevent and mitigate threats like fraud corruption and money laundering.
Financing of Terrorism	FT	Another term for terrorist financing used interchangeably with TF in AML/CFT regulations to describe funding for terrorist activities.
Finansinspektionen	FI	Sweden's Financial Supervisory Authority responsible for overseeing AML and financial compliance in the Swedish financial sector.
Fraud Risk Assessment	FRA	A process to evaluate and mitigate risks of fraudulent activities often integrated with AML and KYC processes to identify suspicious patterns.
General Data Protection Regulation	GDPR	An EU regulation governing data protection and privacy requiring secure and compliant handling of personal data in AML KYC KYB and financial threat intelligence processes.
Informal Value Transfer System	Hawala	An informal trust-based system for transferring money without physical movement often exploited for money laundering or terrorist financing due to its anonymity.
Information Sharing and Analysis Centre	ISAC	A collaborative organisation that facilitates the sharing of cyber and financial threat intelligence among members such as the Financial Services ISAC (FS-ISAC) to enhance collective defence.
Insider Trading		The illegal practice of trading stocks or other securities based on non-public material information often linked to corruption in financial or corporate settings.
International Bank Account Number	IBAN	A standardised format for identifying bank accounts internationally used to document banking relationships in KYC KYB and suspicious activities.
International Criminal Police Organisation	INTERPOL	An international organisation facilitating global police cooperation including investigations of money laundering and terrorist financing.
Joint Investigation Team	JIT	A collaborative team of law enforcement agencies from multiple jurisdictions often formed for complex financial crime investigations under EU frameworks like Eurojust.
Know Your Business	KYB	The process of verifying the identity and structure of business entities including beneficial owners to ensure compliance with AML and fraud prevention regulations.
Know Your Customer	KYC	The process of verifying the identity of customers during onboarding serving as the first step in AML

Full format	Acronym	Explanation
		compliance typically involving a one-time verification (with potential updates based on risk).
Law Enforcement Agency	LEA	A government agency responsible for investigating financial crimes such as fraud and money laundering often collaborating with FIUs (e.g. FBI NCA).
Layering		A stage in money laundering where illicit funds are moved through complex transactions or shell companies to obscure their origin making it difficult to trace the funds back to criminal activities.
Monetary Authority of Singapore	MAS	Singapore's central bank and financial regulator enforcing AML/CFT regulations and promoting financial stability.
Money Laundering	ML	The process of concealing the origins of illegally obtained funds often through layering to make them appear legitimate; synonymous with AML in regulatory contexts.
National Crime Agency	NCA	The UK's lead agency for combating serious and organised crime including money laundering and fraud collaborating with FIUs and international partners.
National Security Agency	NSA	A U.S. agency responsible for signals intelligence occasionally involved in financial crime investigations related to national security and terrorist financing.
Nepotism		The practice of favouring relatives or associates in appointments or resource allocation often in public or corporate settings leading to inefficiency and corruption.
Network and Information Security Directive 2	NIS2	An EU directive strengthening cybersecurity across sectors relevant to secure data handling in AML and KYC processes.
Office of Foreign Assets Control	OFAC	A U.S. agency administering economic sanctions programs including the SDN list used globally to screen customers and transactions for compliance.
Personally Identifiable Information	PII	Data that can be used to identify an individual such as names addresses or financial details often targeted in fraud schemes like identity theft and protected under privacy laws.
Phishing		A fraudulent practice where cybercriminals send deceptive communications (e.g. emails texts) posing as legitimate entities to steal sensitive information like login credentials or financial details.
Politically Exposed Person	PEP	An individual with a prominent public role subject to enhanced scrutiny in AML processes due to higher risks of corruption or money laundering.
Ponzi Scheme		A fraudulent investment scam where returns are paid to earlier investors using funds from newer investors creating the illusion of profitability until the scheme collapses.

Full format	Acronym	Explanation
Sanctions List		A list of individuals entities or countries subject to restrictions or penalties used by organisations to screen transactions and prevent dealings with prohibited parties.
Securities and Exchange Commission	SEC	A U.S. regulatory agency overseeing securities markets enforcing compliance with AML and fraud prevention regulations for financial institutions.
Shell Company		A non-operational company used to conceal ownership or financial transactions often employed in money laundering to obscure the source of illicit funds.
Simplified Customer Due Diligence	SCDD	A streamlined due diligence process applied to low-risk customers or transactions requiring less extensive verification under AML regulations.
Sixth Anti-Money Laundering Directive	AMLD6	An EU directive further harmonising AML rules introducing stricter penalties and expanding criminal liability effective from 2021.
Society for Worldwide Interbank Financial Telecommunication	SWIFT	A global network for secure financial messaging with SWIFT codes used to identify banks in transaction and banking relationship data.
Specially Designated Nationals	SDN	A list maintained by OFAC identifying individuals and entities subject to sanctions used in AML and KYC screening to prevent illicit financial activities.
Structured Threat Information Expression	STIX	A standardised machine-readable format for sharing cyber and financial threat intelligence using objects like Indicators Observables and Attack Patterns to describe threats (e.g. [url:value MATCHES '.phish.'] for phishing).
Suspicious Activity Report	SAR	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.
Suspicious Transaction Report	STR	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.
Terrorist Financing	TF	The provision or collection of funds to support terrorist activities closely monitored under AML/CFT frameworks; synonymous with FT.
Trade-Based Money Laundering	TBML	A form of money laundering that uses trade transactions such as over- or under-invoicing to disguise illicit funds often requiring enhanced monitoring.
Transaction Monitoring		The process of analysing financial transactions in real-time or retrospectively to detect suspicious patterns indicative of fraud money laundering or other illicit activities.

Full format	Acronym	Explanation
Trusted Automated Exchange of Intelligence Information	TAXII	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.
Anti-Money Laundering	AML	A set of laws regulations and procedures aimed at preventing criminals from disguising illegally obtained funds as legitimate income involving transaction monitoring customer due diligence and reporting suspicious activities to disrupt illicit financial flows.
Anti-Money Laundering Directive	AMLD	A series of EU directives (e.g. AMLD5 AMLD6) establishing AML and CFT regulations harmonising rules across member states for financial crime prevention.
Attack Pattern		A STIX object describing the tactics techniques and procedures (TTPs) used by threat actors such as T1566 for phishing or T1657 for financial theft based on frameworks like MITRE ATT&CK.
Bank Secrecy Act	BSA	A U.S. law requiring financial institutions to report suspicious activities and maintain records to assist in detecting and preventing money laundering and fraud.
Beneficial Owner	BO	An individual who ultimately owns or controls a business entity or benefits from its activities critical for KYB transparency under AML regulations.

11 References

- **Association of Certified Fraud Examiners (ACFE)**
  - Payroll Fraud Case: https://www.acfe.com
- **DataDome**
  - Fraud Risk Management Principles, https://datadome.co
- **Emerald Insight**
  - Journal of Financial Crime: https://www.emerald.com
- **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/
- **International Monetary Fund (IMF)**
  - Anti-Money Laundering and Combating the Financing of Terrorism: https://www.imf.org
- **INTERPOL**
  - Financial Fraud Assessment: https://www.interpol.int
- **Kroll, LCC**

  - Global Fraud and Risk Report: https://www.kroll.com
- **MISP Threat Sharing**
  - https://www.misp-project.org
- **Njordium Cyber Group**
  - Harmonising AML Attributes for Effective Financial Crime Prevention: https://njordium.com/2025/07/10/harmonising-aml-attributes-for-effective-financial-crime-prevention/
- **OASIS**
  - STIX Version 2.1 Specification: https://www.oasis-open.org/standard/6426/
- **ScienceDirect**
  - Auditing for Fraud and Corruption: https://www.sciencedirect.com
- **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
- **US State Department**
  - Money Laundering and Financial Crimes: https://2009-2017.state.gov