Association *of* Internet Research Specialists

International Money Laundering Schemes & Foreign Assets Detection

This combined Research Report and Training Guide provides a comprehensive examination of international money laundering schemes and the detection of hidden foreign assets.

June 05 2026

Submitted by:
Naveed Manzoor
Association of Internet Research Specialist | AOFIRS

USVA7777904052027

ASSOCIATION OF INTERNET RESEARCH SPECIALISTS
AOFIRS | CIRS™ Professional Training Series

RESEARCH REPORT & TRAINING GUIDE

International Money Laundering Schemes & Foreign Assets Detection

Training Module 10 | Unit 25

Series:	CIRS™ Advanced Financial Intelligence
Edition:	2025 — Revised & Expanded
Classification:	Professional Training Material
Publisher:	Association of Internet Research Specialists (AOFIRS)
Date:	June 2025
Copyright:	© 2019–2025 AOFIRS. All rights reserved.

This document is intended for Certified Internet Research Specialists (CIRS™) candidates and credentialed professionals. Unauthorized reproduction is prohibited.

Executive Summary

This combined Research Report and Training Guide provides a comprehensive examination of international money laundering schemes and the detection of hidden foreign assets. It is designed for Certified Internet Research Specialists (CIRS™) seeking advanced competency in financial crime intelligence — incorporating foundational methodology alongside the most current typologies, enforcement developments, and investigative tools available as of 2025.

Money laundering represents one of the most pervasive forms of financial crime globally, with the United Nations Office on Drugs and Crime (UNODC) estimating that 2–5% of global GDP — roughly USD 800 billion to USD 2 trillion — is laundered annually (UNODC, 2023). As criminal networks and corrupt political actors grow more sophisticated in their use of offshore jurisdictions, shell companies, trusts, and emerging digital asset platforms, the role of the internet research specialist in tracing illicit financial flows has never been more critical.

This report covers traditional three-stage money laundering theory; the Hawala system and informal value transfer networks; the mechanics of shell companies, offshore trusts, and financial havens; four primary laundering methodologies using corporate vehicles, third parties, professional facilitators, and international wire transfers; emerging 2024–2025 typologies including cryptocurrency laundering and Professional Money Laundering Networks (PMLNs); the ICIJ Offshore Leaks Database — now encompassing 810,000+ entities from Panama Papers, Paradise Papers, Bahamas Leaks, and Pandora Papers; the U.S. Corporate Transparency Act (CTA) and the latest FinCEN Beneficial Ownership Information (BOI) reporting developments; and a detailed investigative training framework for CIRS™ candidates.

A full APA reference list and subject index are provided at the close of the report.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Table of Contents

Executive Summary 4
Table of Contents 6
Chapter 1: Introduction to Money Laundering 9
1.1 Definition and Scope 9
1.2 The Three-Stage Model: Placement, Layering, Integration 9
1.3 Evolution of Money Laundering Typologies (2024–2025) 10
Chapter 2: Physical Money Transfer Methods 10
2.1 Physical Shipment of Money Abroad 10
2.2 The Hawala System 10
2.3 Trade-Based Money Laundering (TBML) 11
Chapter 3: Corporate Vehicles and Offshore Structures 11
3.1 Shell Companies Explained 11
3.2 Offshore Trusts and Their Functions 12
Types of Offshore Trusts 13
3.3 Financial Havens: Global Jurisdictions of Concern 13
Chapter 4: The Four Primary Laundering Methods 14
4.1 Method 1 — Use of Corporate Vehicles and Trusts (Local and Offshore) 14
4.2 Method 2 — Use of Third-Party Intermediaries 15
4.3 Method 3 — Use of Professional Facilitators 16
4.4 Method 4 — Use of International Funds Transfers 18
Chapter 5: Emerging Money Laundering Typologies (2024–2025) 19
5.1 Cryptocurrency and Virtual Asset Laundering 19
5.2 Professional Money Laundering Networks (PMLNs) 20
5.3 Real Estate as a Laundering Vehicle 20
5.4 AI-Generated Synthetic Financial Identities 21
Chapter 6: Investigative Leak Intelligence — The ICIJ Offshore Leaks Database 21
6.1 The Four Major Leak Investigations 21
Offshore Leaks (2013) 21
Panama Papers (2016) 22
Bahamas Leaks (2016) 22
Paradise Papers (2017–2018) 22
Pandora Papers (2021) — The Largest Leak in ICIJ History 22

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

6.2 Case Study: The Nawaz Sharif Family 23
Chapter 7: Global Regulatory Architecture 25
7.1 FATF Standards and 2024–2025 Updates 25
7.2 The U.S. Corporate Transparency Act (CTA) and BOI Reporting 26
7.3 International AML Compliance Architecture 26
Chapter 8: Framework for Investigating Hidden Assets 28
8.1 Key Information Required for Hidden Asset Verification 28
8.2 Piercing the Corporate Veil — Investigative Techniques 28
Step 1: Build the Family and Network Tree 28
Step 2: Identify Real Property Holdings 28
Step 3: Penetrate Corporate Structures 29
Step 4: Work Human Sources 29
8.3 Red Flags for Money Laundering — Investigator Checklist 29
Chapter 9: Research Tools, Databases, and Resources 29
9.1 Using the ICIJ Offshore Leaks Database — Step-by-Step Guide 29
Step 1: Download and Cross-Reference the Data 30
Step 2: Verify and Check for False Positives 30
Step 3: Explore Network Relationships Using the Relationship Chart 30
Step 4: Filter by Jurisdiction and Dataset 30
9.2 Additional OSINT and Investigative Resources 30
Chapter 10: Annexure — U.S. Fraud and Financial Crime Reporting Agencies 31
Chapter 11: Learning Objectives and Competency Assessment 32
References 33
Index 35

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

PART I: RESEARCH REPORT

Understanding International Money Laundering Schemes & Foreign Assets Detection

Chapter 1: Introduction to Money Laundering

1.1 Definition and Scope

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source (International Compliance Association [ICA], 2022). The processes by which criminally derived property may be laundered are extensive. Though criminal money may be successfully laundered without the assistance of the financial sector, the reality is that hundreds of billions of dollars of criminally derived money flows through financial institutions annually.

The nature of the services and products offered by the financial services industry — managing, controlling, and possessing money and property belonging to others — makes it inherently vulnerable to abuse by money launderers. Money is laundered whenever a person or business deals in any way with another person's benefit from crime. That can occur in a countless number of diverse ways.

According to Verafin (2024), an estimated USD 3.1 trillion in illicit funds flowed through the global financial system in 2024 alone, fueling a shadow economy operating outside regulatory control. The Financial Action Task Force (FATF, 2024) identifies fraud, corruption, drug trafficking, and tax crimes as the four leading predicate offences generating proceeds that enter the laundering cycle.

1.2 The Three-Stage Model: Placement, Layering, Integration

Traditionally, money laundering has been described as a process that takes place in three distinct stages. While this model is a simplification — since stages frequently overlap and, in cases of financial crime, the placement stage may be bypassed entirely — it provides a foundational conceptual framework for investigators (Financial Action Task Force [FATF], 2023).

Stage	Description	Common Methods
1. PLACEMENT	Introduction of criminally derived funds into the financial system — the most vulnerable stage for criminals.	Cash deposits, currency smuggling, cash-intensive businesses, Hawala transfers
2. LAYERING	Concealment of the origin and ownership of funds through a series of complex financial transactions.	Wire transfers, shell companies, offshore trusts, cryptocurrency, multiple jurisdictions
3. INTEGRATION	Re-introduction of laundered funds into the legitimate economy, now appearing as lawful income.	Real estate purchases, luxury assets, business investments, loan repayments

Table 1. The Three-Stage Model of Money Laundering (FATF, 2023; ICA, 2022)

This three-staged definition is highly simplistic. The reality is that the so-called stages often overlap and, in some cases, for example in cases of financial crimes, there is no requirement for the proceeds

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

of crime to be placed. When the sums become larger and law enforcement in the immediate jurisdiction is seen as particularly difficult to evade, the laundering process will more likely involve an international laundering scheme crossing multiple borders and financial systems (U4 Expert Answer, 2022).

1.3 Evolution of Money Laundering Typologies (2024–2025)

The typologies of money laundering — the patterns and techniques criminals use to conceal illicit funds — have continuously evolved in response to globalization, technological advancements, and increased regulatory scrutiny (Hellvig & Blanaru, 2023). Today's methods are more sophisticated, often involving complex corporate structures, digital assets, and the involvement of professional enablers such as lawyers and accountants, which together complicate efforts to detect and prevent illicit financial flows (Levi, 2022).

The FATF's 2024–2025 typologies reports have placed particular emphasis on Professional Money Laundering Networks (PMLNs) — organized groups that provide laundering services across multiple criminal enterprises. FATF guidance distinguishes these from traditional in-house laundering operations by their scale, cross-border reach, and use of legitimate professional intermediaries (FATF, 2025).

Concurrently, analysis of Suspicious Activity Report (SAR) trends across key jurisdictions reveals that structuring and smurfing — classic typologies documented for decades — remain the most frequently triggered detection rule categories. This underscores that despite regulatory emphasis on sophisticated emerging typologies, foundational financial crime patterns persist and require ongoing, well-calibrated detection systems (FATF, 2025).

Chapter 2: Physical Money Transfer Methods

2.1 Physical Shipment of Money Abroad

The first task in international money laundering is to move funds from the country of origin. This can be done by either sidestepping or working through the formal banking system. If the decision is made to sidestep the system, the most popular method is shipping money abroad in bulk cash (ICA, 2022). Sometimes items of high intrinsic value — diamonds, gold, precious stamps, or collectibles — are also used because they are physically easy to smuggle and relatively easy to reconvert into cash at the destination.

However, cash remains far more important than valuable commodities in terms of volume. Physical currency movements often rely on complicit couriers, diplomatic pouches, or cargo shipments disguised as legitimate trade goods. The FATF's 2015 report on the Physical Transportation of Cash documented that this method remains prevalent despite enhanced border monitoring technologies, because it bypasses the electronic audit trail that formal banking creates (FATF, 2015).

Various lateral transfer schemes — including compensating balances, a principle long used in legitimate trade with countries that have exchange controls or legally inconvertible currencies — are also used to export money without physically moving it (ICA, 2022).

2.2 The Hawala System

> **Key Concept: Informal Value Transfer**
> Hawala and similar informal value transfer systems (IVTS) operate entirely outside regulated financial channels. They leave no paper trail, no receipts, and no regulatory footprint — making them a highly favored tool for moving illicit funds across international borders.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Hawala remittance systems are a fast, safe, and cost-effective way to transfer funds both domestically and internationally without using formal financial institutions (ICA, 2022). A customer — usually a migrant worker — approaches a Hawala broker and gives him a sum of money to be transferred to a beneficiary — usually a relative — in another city or country.

The Hawala operator contacts their Hawala partner — usually a contact from their personal or business network — in the recipient city or country by phone, fax, or email. The operator instructs the partner to deliver the funds to the beneficiary, providing the amount, name, address, and telephone number of the recipient, and promises to settle the debt at a later stage. The customer is given an identification code for the transaction, and no receipt is issued. The recipient can receive the funds without producing identity documents other than the previously agreed code. There is no recorded agreement or written contract — the deal is secured entirely by trust between the parties (FATF, 2013).

The FATF's 2013 report on the role of Hawala and other similar service providers in money laundering and terrorist financing notes that these networks present particular challenges for financial intelligence units (FIUs) because: (a) transactions are settled through non-monetary reciprocal arrangements, (b) accounts are settled via reverse cash flows, commodity trade, or real estate, and (c) the informal nature means that even cooperative brokers may lack transactional records (FATF, 2013).

2.3 Trade-Based Money Laundering (TBML)

Trade-Based Money Laundering (TBML) represents a significant and growing methodology in which illicit value is transferred through the international trade system by manipulating trade transactions (U.S. Department of State, Bureau for International Narcotics and Law Enforcement Affairs [INL], 2024). TBML exploits the complexity of global trade flows, the volume of transactions, and the limited capacity of customs and trade compliance systems.

Common TBML techniques include: over-invoicing or under-invoicing of goods and services, multiple invoicing for the same shipment, falsely described goods or services, and phantom shipments of goods that never actually move. Trade Transparency Units (TTUs) address this by comparing export records from one country with corresponding import records from the receiving country — wide discrepancies are indicative of trade fraud and potential TBML (INL, 2024).

Chapter 3: Corporate Vehicles and Offshore Structures

3.1 Shell Companies Explained

Shell companies are non-traded corporations — meaning they are not listed on any stock exchange — that most often exist in name only, other than as a mailing address and a registered financial entity on paper (U.S. Securities and Exchange Commission [SEC], 2023). To become a shell corporation, an interested party typically files with the relevant regulatory authority. Examples are limited liability companies (LLCs) and trusts, provided that they are not comprised of physical properties.

The great strength of a shell company is that it can shield its owner's identity. On the legitimate end, a corporation may place its assets and profits into offshore shell companies — untaxed until they return onshore. In many instances, a private banker will set up a shell corporation for a client and open accounts in that company's name, in order to disguise the client's ownership of the account or certain assets.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

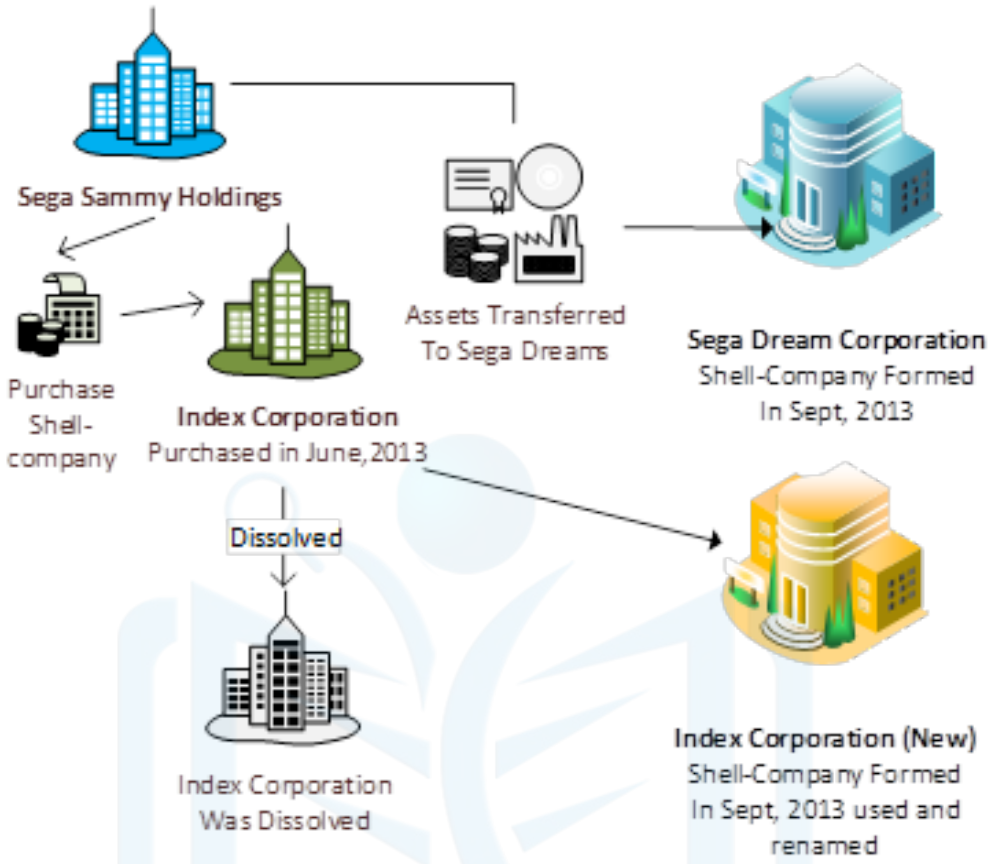

Figure 1. Illustration of shell company formation and asset transfer — the Sega Sammy Holdings/Index Corporation case (2013). Source: Original module imagery.

Criminal operations use shell companies to launder money throughout the world. So-called dirty money can be shuffled through a series of shell companies, coming out clean on the other end in the form of investments, bearer bonds, commodities, and other assets. Since these companies can be set up with **nominee directors** — usually lawyers and accountants — there is no straightforward way to trace the laundered assets back to the illegal activity that generated them (ICA, 2022).

Since nominee directors are typically professionals operating legally in their home jurisdictions, law enforcement must often navigate multiple layers of corporate secrecy law, attorney-client privilege, and cross-jurisdictional treaties before identifying the true beneficial owner of a shell entity.

Infrastructure companies are particularly active users of shell companies because they are required to pay bribes across a range of actors — from politicians to government officials to organized crime intermediaries. The infrastructure company pays the shell company via check, the funds are returned in cash, and the shell company records the outflow as payments to smaller shell companies — creating a circular paper trail that obscures the ultimate use of funds (ICA, 2022).

3.2 Offshore Trusts and Their Functions

Successful money laundering today probably requires working through a front business that has a credible explanation for its level of deposits and, critically, for moving funds abroad. Prior to sending money to a financial haven, the launderer will often engage a jurisdiction that offers rapid offshore

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

company formation — the Cayman Islands, British Virgin Islands, Liberia, and Panama are among the favorites. Such jurisdictions sell offshore corporations that are licensed to conduct business only outside the country of incorporation, are free of tax or regulation, and are protected by corporate secrecy laws (ICA, 2022).

Many laundering schemes add a third layer of cover through the offshore trust. Advantages of a trust include: (a) the owner irrevocably conveys asset ownership to the trust, preventing seizure by creditors; (b) offshore trusts are protected by secrecy laws; and (c) some include a flee clause permitting — indeed compelling — the trustee to shift the trust's domicile whenever it is threatened by war, civil unrest, or law enforcement investigation. The nominal disadvantage is the apparent loss of control — but practitioners devise arrangements that preserve effective control while satisfying the letter of trust law (ICA, 2022).

Types of Offshore Trusts

- Revocable Offshore Trust — can be liquidated or altered by the settlor according to the Trust Deed terms.
- Irrevocable Offshore Trust — may not be changed or liquidated by the settlor once established.
- Discretionary Offshore Trust — enables the trustee to decide on the distribution of profits among different classes of beneficiaries, maximizing flexibility.
- Fixed Trust — the distribution of income to beneficiaries is fixed and cannot be changed by the trustee, providing certainty.
- Hybrid Trust — includes elements of both discretionary and fixed trusts, tailored to specific asset protection objectives.

The three strongest offshore trust jurisdictions from an asset protection standpoint are the Cook Islands, Nevis, and Belize — each offering statutes specifically written to protect the assets of beneficiaries from foreign court orders and creditor claims (ICA, 2022). Almost any type of asset can be transferred into an offshore trust, including cash, real estate, securities, businesses, fine art, and gold.

3.3 Financial Havens: Global Jurisdictions of Concern

A financial haven is a jurisdiction offering one or more of the following features: minimal or zero taxation, strict bank secrecy laws, lax corporate registration requirements, limited exchange of information with foreign law enforcement, and the availability of nominee directorship and bearer share arrangements. While no jurisdiction will approve unrestricted law enforcement access to depositor lists, many jurisdictions — even those with bank secrecy laws — will permit access if the matter under investigation constitutes a crime in the host jurisdiction as well (ICA, 2022).

Region	Financial Haven Jurisdictions
Caribbean	Anguilla, Antigua, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Cayman Islands, Costa Rica, Netherlands Antilles, Panama, Saint Kitts & Nevis, Saint Lucia, Saint Vincent & the Grenadines, Turks & Caicos Islands
Europe	Andorra, Campione, Cyprus, Gibraltar, Guernsey, Ireland (Dublin), Isle of Man, Jersey, Liechtenstein, Luxembourg, Madeira, Malta, Monaco, Sark, Switzerland
Asia & Pacific	Cook Islands, Hong Kong SAR, Labuan, Macao, Marianas, Marshall Islands, Nauru, Niue, Samoa, Singapore, Vanuatu
Middle East	Bahrain, Dubai (UAE), Lebanon

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Region	Financial Haven Jurisdictions
Africa	Liberia, Mauritius, Seychelles

Table 2. Key Financial Haven Jurisdictions by Region. Source: ICA (2022); FATF (2024).

Chapter 4: The Four Primary Laundering Methods

The following four methods represent the core operational approaches by which money launderers — particularly those associated with political corruption and bribery — move, conceal, and integrate illicit funds. Each method is illustrated with a diagrammatic case scenario and supported by investigative guidance.

4.1 Method 1 — Use of Corporate Vehicles and Trusts (Local and Offshore)

Illicit funds held in the name of a company, shell company, or trust distance the beneficiary from ownership of the funds, with control vested in the hands of third parties. This avoids any direct or indirect links to the funds. In the example below, companies in foreign jurisdictions are used to receive cash deposits, which are subsequently sent to other jurisdictions.

Scenario: 'Joe' is a politician in Country 1; 'Tom' is a businessperson in Country 2. Joe provides confidential information to Tom about an upcoming privatization of a lucrative business so that Tom can bid on its sale. This information requires a payment from Tom to Joe through offshore kickback arrangements. Joe does not want the money trail to connect with him; he therefore asks Tom to send the kickback funds through a series of bank accounts and trusts that can circle back the funds to him.

- Tom is instructed to deposit USD 100,000 into Shell Company X's bank account in Country 2.
- Shell Company X's Country 2 account is controlled by its main account in Country 3 — a tax-free haven with strict privacy laws (e.g., Panama, Cayman Islands, Bermuda, Singapore, Dubai).
- The money deposited in Bank Account 100 is remitted into several accounts of Company X in Country 3 (Bank Accounts 101, 102, 103).
- The funds are later transferred to Country 1, within the cloak of an offshore trust in which Joe is the beneficiary.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

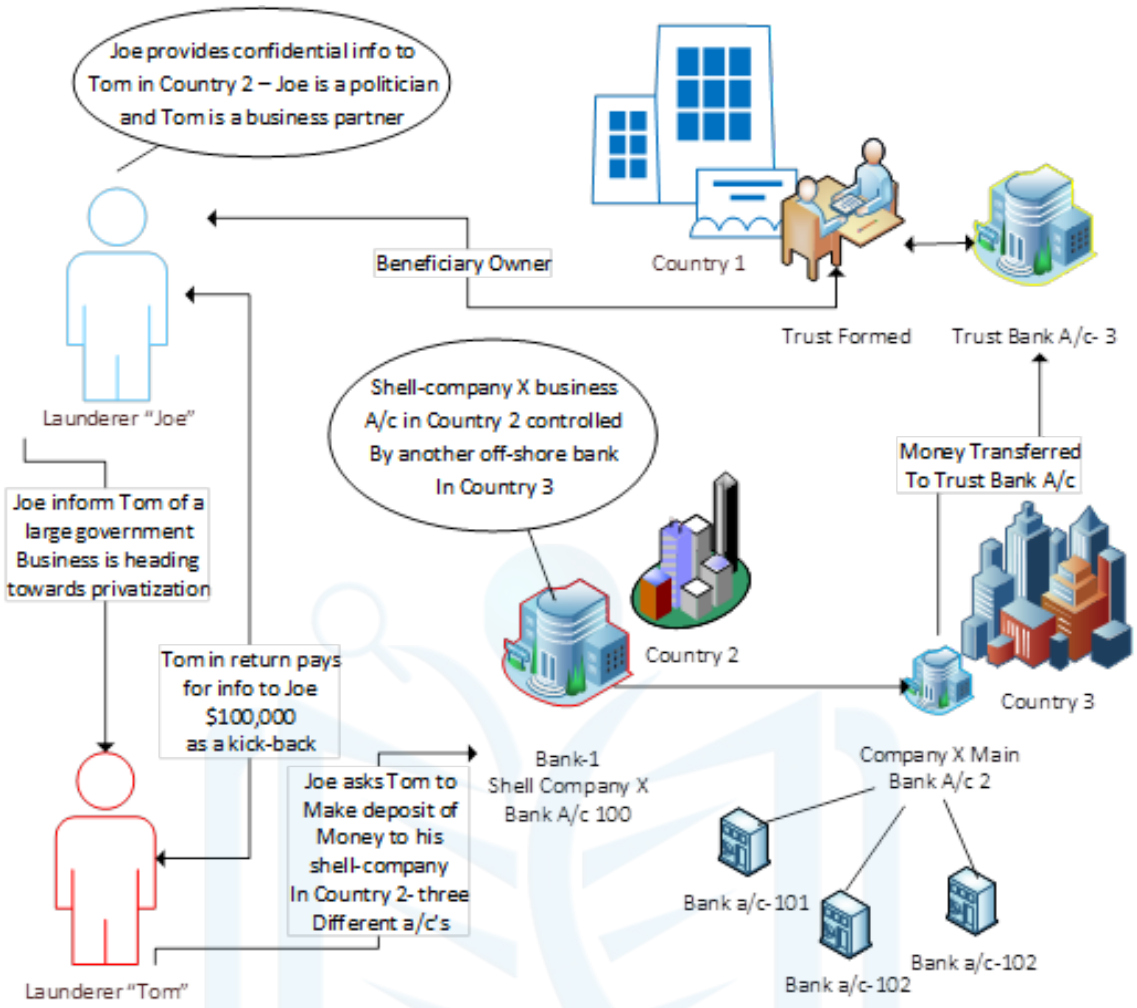

Figure 2. Method 1: Use of corporate vehicles and offshore trusts to channel bribery payments. Shell company accounts in multiple jurisdictions create layers that obstruct law enforcement tracing. Source: Original module diagram.

Because the funds in the trust are transferred via Country 3, it is difficult for authorities in Country 1 to trace the source of funds back to Tom. The use of a shell company in Country 2 further complicates the money trail by adding an additional jurisdictional layer (ICA, 2022; AUSTRAC, 2021).

4.2 Method 2 — Use of Third-Party Intermediaries

In the following example, a business associate in a second country is used to transfer money into anonymous offshore trust accounts in a third country. The trust then makes disbursements to Joe's family members in their offshore personal accounts. The use of a third-party distances corruption money from the illicit activities, disguises ownership of assets, and complicates confiscation efforts by authorities (AUSTRAC, 2021).

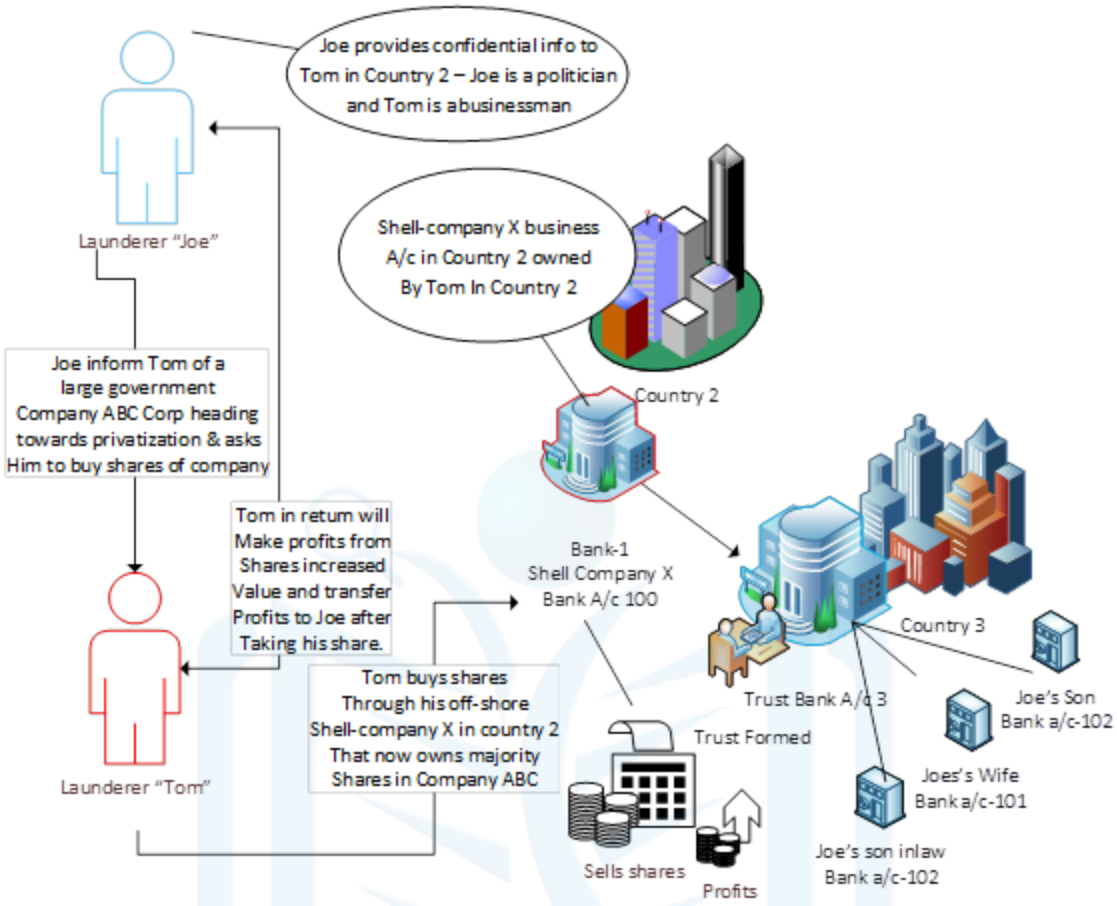

Figure 3. Method 2: Third-party intermediaries, shell companies, and offshore trusts used to channel bribery proceeds to family members in overseas accounts. Source: Original module diagram.

Corrupt officials often hide their wealth through companies, accounts, and assets owned by family members — typically spouses, partners, children, and siblings. A corruption investigation almost always begins with constructing a family tree and then tracing companies and properties found in the names of the official's relatives (Coronel, 2012). This investigative approach was validated in the Hong Kong Next Magazine's investigation into Bo Xilai's family, where reporters identified Hong Kong companies registered in the names of Bo's sister-in-law holding over USD 100 million in shares of a listed Shenzhen company.

4.3 Method 3 — Use of Professional Facilitators

Professionals — lawyers, accountants, real estate agents, financial advisors, and trust and company service providers — are known as gatekeepers because they provide the entry point for those seeking to access financial products and services, purchase real estate, and establish companies and trusts. Professional facilitators are commonly featured in international cases involving corruption and money laundering (AUSTRAC, 2021).

The following scenario illustrates how professional facilitators are used to launder corruption proceeds:

1. Suspect A is a senior government official in Country X.

2. Company ABC is based in Country Y and wants to secure a lucrative government infrastructure contract in Country X.
3. Suspect A receives cash bribes from Company ABC in return for securing the contract.
4. Suspect A gives the cash bribe to their legal practitioner (in foreign currency).
5. The cash is deposited into the legal practitioner's trust account and later transferred to various bank accounts held in the name of the practitioner's business.
6. The legal practitioner transfers the funds to companies and bank accounts controlled by Suspect A's family and associates.
7. The funds are used to fund Suspect A's lifestyle and purchase high-value assets.

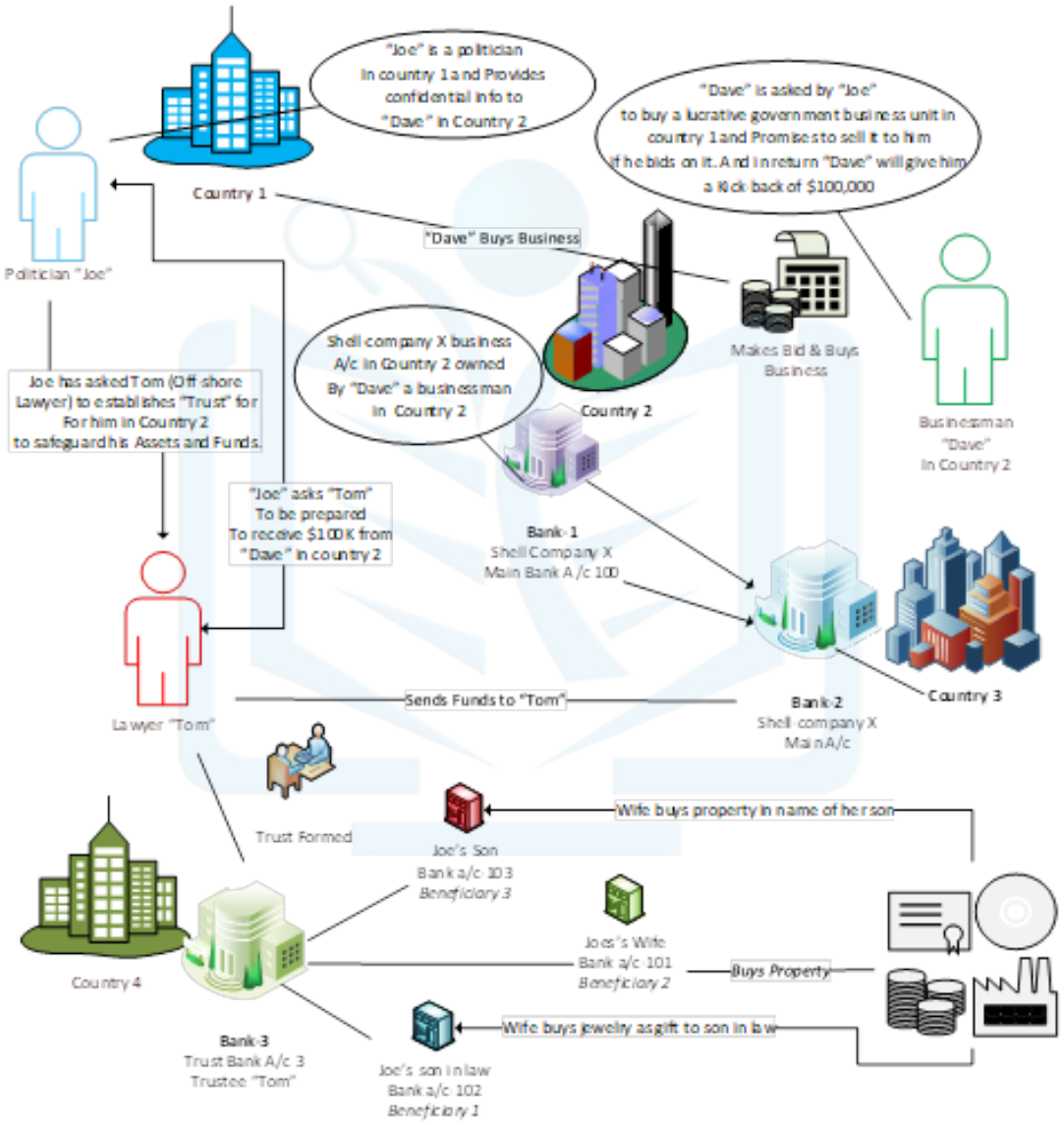

Figure 4. Method 3: Use of professional facilitators — lawyers, accountants, and offshore service providers — to launder bribery proceeds. Source: Original module diagram.

The FATF's 2025 typology reports explicitly flag customer due diligence (CDD) failures involving professional intermediaries — known as Professional Money Laundering Networks (PMLNs) — as one of the highest-risk areas globally. Financial institutions are urged to ensure their CDD and

Enhanced Due Diligence (EDD) frameworks can detect indirect exposure through professional enablers, not merely direct customer relationships (FATF, 2025).

4.4 Method 4 — Use of International Funds Transfers

Corrupt politically exposed persons (PEPs) use international funds transfers to move illicit funds outside their home jurisdiction. Bank accounts and legal entities in foreign jurisdictions are commonly used to launder corruption proceeds. International funds transfers through foreign jurisdictions distance corrupt PEPs from the criminal activity and illicit funds (AUSTRAC, 2021).

The following example involves an Australian company bribing foreign PEPs. Company A bribes officials of Country 1 in return for lucrative government contracts. To disguise the bribery payments, an elaborate routing scheme is created:

- Company A conceals bribery payments by moving funds through accounts of Companies B and C in secrecy havens. Company A controls both Companies B and C.
- Company B is incorporated in Country 2 and operates bank accounts in both Country 2 and Country 3.
- Company C is incorporated in Country 4, where it holds a bank account.
- Company XYZ in Country 1 acts as a front company and collection conduit for the government officials.
- Over time, Company A pays approximately AUD 5 million in bribes disguised as legitimate overseas expenses — e.g., transportation costs.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

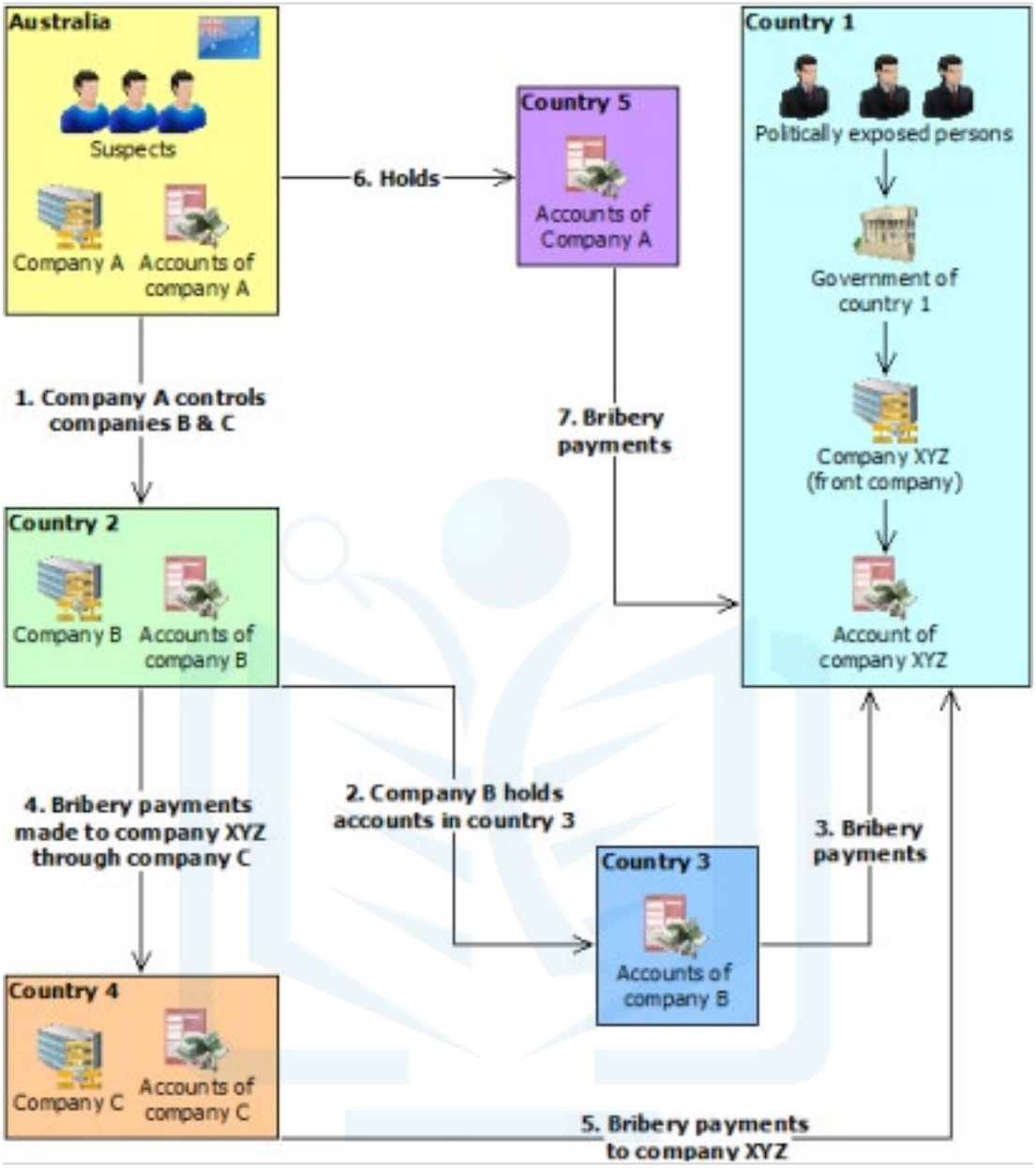

Figure 5. Method 4: International funds transfers routed through multiple corporate entities across five countries to disguise AUD 5 million in bribery payments. Source: AUSTRAC (2021); original module diagram.

Chapter 5: Emerging Money Laundering Typologies (2024–2025)

2025 Research Update
This chapter incorporates the latest findings from the FATF (2025), Chainalysis (2025), and FATF-published guidance through June 2025 on emerging laundering threats — areas not covered in the original module curriculum but now essential for CIRS professionals.

5.1 Cryptocurrency and Virtual Asset Laundering

Cryptocurrency and virtual assets have become a significant channel for money laundering, combining the cross-border speed and cost efficiency that makes them attractive for legitimate use with a pseudo-anonymous layer that criminals exploit. According to Chainalysis (2025), total illicit crypto activity reached USD 40.9 billion in 2024 — with the firm projecting the true figure will exceed USD 51 billion as more addresses are identified through ongoing blockchain analysis.

Key findings from the Chainalysis 2025 Crypto Crime Report include:

- Stablecoins — cryptocurrencies pegged to fiat currencies — made up 63% of all illicit transactions in 2024, rising to 84% of verified crypto fraud volumes in 2025. Their high liquidity and deep exchange integration make them the dominant vehicle for illicit value transfer (Chainalysis, 2025).
- North Korea-linked groups stole USD 1.34 billion in 2024 through sophisticated exchange hacks and protocol exploits, with proceeds laundered through a layering chain of private wallets, mixers, and cross-chain bridges (Chainalysis, 2025).
- Only 25% of FATF-assessed jurisdictions fully comply with virtual asset AML rules, creating significant regulatory arbitrage opportunities for criminal actors (FATF, 2024).

While public blockchains are inherently transparent and traceable, illicit actors exploit them for the same reasons legitimate users do: transactions are cross-border, virtually instant, and inexpensive. In crypto, one popular layering method involves sending funds through numerous intermediary personal wallets — known as hops — designed to obscure the connection between the illicit source and the eventual destination (Chainalysis, 2024).

Cryptocurrency laundering mirrors traditional placement, layering, and integration stages but occurs at significantly higher speed. Advanced blockchain analytics technology — offered by firms such as Chainalysis, Elliptic, and TRM Labs — provides opportunities for detection and disruption throughout this process. Elliptic's automated behavioral detection identifies laundering-specific patterns including peel chains (where funds are successively sent through multiple wallet addresses), mixing services, and structured transactions designed to fall below AML reporting thresholds (Elliptic, 2025).

5.2 Professional Money Laundering Networks (PMLNs)

FATF's 2024–2025 typologies reports have placed particular emphasis on Professional Money Laundering Networks (PMLNs) — organized groups that operate as third-party service providers for multiple criminal enterprises, offering end-to-end laundering solutions for a fee. Unlike traditional in-house laundering operations, PMLNs are characterized by their scale, cross-border reach, and integration of legitimate professional intermediaries (FATF, 2025).

PMLNs offer their clients a range of services including bulk cash handling, placement into financial institutions, layering through complex corporate structures, and integration through real estate and luxury asset purchases. The UK's National Crime Agency has reported significant growth in SAR volumes related to complex layering structures involving multiple legal entities — a pattern consistent with PMLN activity (FATF, 2025).

FinCEN data in the United States similarly shows elevated SAR volumes relating to professional money laundering and third-party payment processor abuse — both areas explicitly flagged in FATF's 2025 typologies guidance (FATF, 2025; INL, 2024).

5.3 Real Estate as a Laundering Vehicle

Real estate has long been favored for integrating laundered proceeds because property transactions involve large sums, are relatively complex, and are traditionally subject to lower AML scrutiny than financial products. The FATF's 2022 Risk-Based Approach Guidance for the Real Estate Sector identifies real estate as a major vulnerability, with criminals exploiting it through:

- Over- or undervaluing properties to justify loans or increase laundered amounts.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

- Structuring cash deposits: breaking down large cash payments to avoid detection thresholds.
- Rental income legitimization: using illicit funds to pay rents or finance renovations that increase property value.
- Use of shell companies and opaque ownership structures to mask the true owner's identity.
- Using legal professionals, real estate agents, or notaries to authenticate transactions and lend legitimacy to the acquisition process (FATF, 2022; Munge et al., 2024).

Property records remain one of the most effective starting points for financial investigators. Houses are among the easiest assets to find: most countries make real-property records publicly available, and even when properties are not in a corrupt official's name, the official and family members would have been seen there. Records on the acquisition of real property often lead to further investigative clues, including the names of shell companies and nominees that fronted for purchases, the bank accounts used, and the lawyers, architects, and real estate agents involved (Coronel, 2012).

A notable example is James Ibori, the former governor of Nigeria's Delta State, who was found to have used UK bank accounts and shell companies to acquire houses in London, a fleet of luxury vehicles including a Bentley and Maybach, and a USD 20 million private jet. Ibori was convicted of money laundering in a London court in 2012 (Coronel, 2012).

5.4 AI-Generated Synthetic Financial Identities

An emerging and particularly dangerous typology documented in 2024–2025 involves the use of artificial intelligence to generate synthetic financial identities and fabricated transactional records. These AI-generated records may then be used to build seemingly legitimate transactional histories or customer profiles, enabling criminals to 'clean' illicit funds with a digital paper trail that is algorithmically indistinguishable from genuine financial activity (Mallik et al., 2025).

This blurs the boundary between real and synthetic financial behavior, complicating efforts to delineate lawful from unlawful transactions. Compliance teams relying purely on rule-based detection are increasingly challenged by this typology, as synthetic identities can pass standard Know Your Customer (KYC) checks and generate plausible historical transaction patterns. The FATF's 2024 guidance on beneficial ownership and transparency recognizes the escalating challenge of AI-enabled identity fraud as a component of modern layering strategies (FATF, 2024; Mallik et al., 2025).

Chapter 6: Investigative Leak Intelligence — The ICIJ Offshore Leaks Database

The International Consortium of Investigative Journalists (ICIJ) has emerged as the most significant source of aggregated offshore financial intelligence available to researchers and journalists globally. The ICIJ Offshore Leaks Database currently contains information on more than 810,000 offshore entities — covering more than 80 years of activity up to 2020 — linking to people and companies in more than 200 countries and territories (ICIJ, 2022).

6.1 The Four Major Leak Investigations

The ICIJ database has been assembled through four transformative investigative leaks, each adding a new stratum of offshore financial intelligence:

Offshore Leaks (2013)

The first data added to the database, released in June 2013 in conjunction with Costa Rican newspaper La Nación. The data covers offshore entities incorporated through Portcullis Trustnet (now

Portcullis) and Commonwealth Trust Limited — two offshore service providers. This initial release established the template for data-driven offshore investigations (ICIJ, 2013).

Panama Papers (2016)

Data from Panama law firm Mossack Fonseca, whose inner workings were exposed in a landmark investigation published in April 2016 in conjunction with Süddeutsche Zeitung and more than 100 media partners. The Panama Papers revealed the offshore holdings of 12 current or former world leaders and 128 other politicians and public officials, triggering law enforcement investigations across dozens of jurisdictions. Mossack Fonseca's managing partners subsequently faced money laundering charges in Panamanian courts (ICIJ, 2016).

Bahamas Leaks (2016)

Added to the database on September 21, 2016, as part of the Bahamas Leaks investigation. This data was based on information from the official corporate registry of the Bahamas — including former EU official records among politicians named in the files (ICIJ, 2016).

Paradise Papers (2017–2018)

The Paradise Papers data in the database comes from offshore law firm Appleby and a trove of data from seven corporate registries. Appleby's structured data was added in November 2017, with corporate registry data from Aruba, Bahamas, Barbados, Nevis, Cook Islands, Malta, and Samoa incorporated through early 2018. The investigation revealed offshore dealings of prominent business figures and political donors (ICIJ, 2018).

Pandora Papers (2021) — The Largest Leak in ICIJ History

The Pandora Papers investigation, published in October 2021, represents the largest journalistic collaboration in history — involving more than 600 journalists from 150 news outlets and based on 11.9 million records from 14 offshore service providers. ICIJ added more than 25,000 new offshore entity records to the database between December 2021 and May 2022, bringing the total to over 810,000 entities (ICIJ, 2022).

Key Pandora Papers findings include identification of the secret deals and hidden assets of more than 330 politicians and high-level public officials in more than 90 countries and territories — including 35 current or former country leaders. ICIJ analysis identified more than 45 Russian oligarchs using offshore entities, and matched the Forbes billionaires list to find more than 130 billionaires with entities in secrecy jurisdictions (ICIJ, 2022).

Within hours of publication, authorities in Pakistan, Mexico, Spain, Brazil, Sri Lanka, Australia, and Panama promised to open inquiries into offshore holdings. The Pandora Papers prompted U.S. lawmakers to propose the most significant reform of anti-money laundering rules since 9/11, specifically targeting financial enablers — the lawyers, accountants, and corporate service providers who facilitate offshore secrecy (ICIJ, 2022).

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

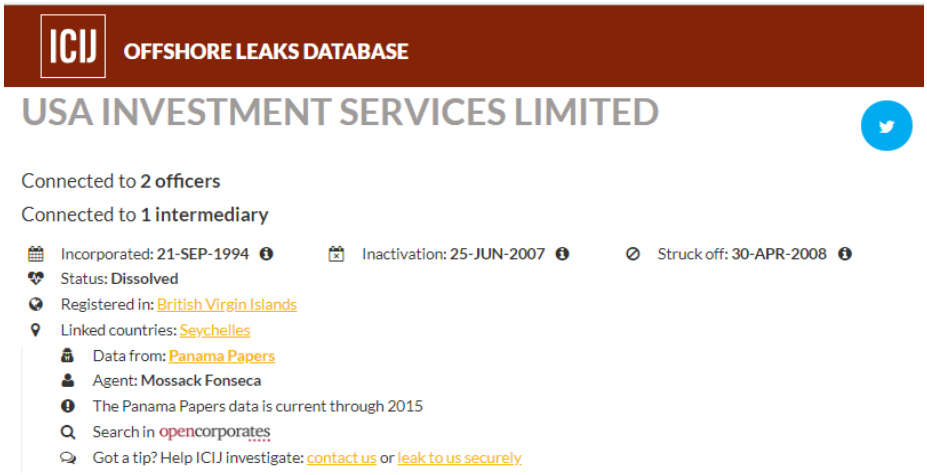

Figure 6a. The ICIJ Offshore Leaks Database entity record for USA Investment Services Limited — showing connections, agent (Mossack Fonseca), and Panama Papers sourcing. Source: ICIJ Offshore Leaks Database (offshoreleaks.icij.org).

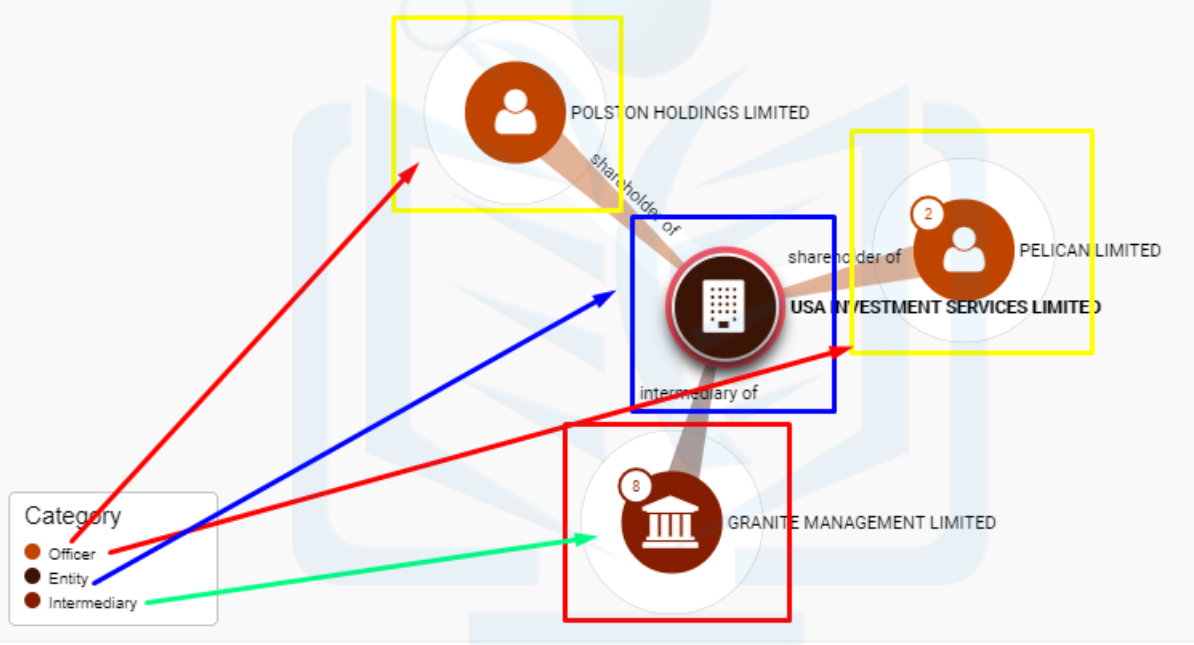

Figure 6b. ICIJ interactive network visualization showing the web of relationships between USA Investment Services Limited, its shareholders (Polston Holdings Limited, Pelican Limited), and its intermediary (Granite Management Limited). Source: ICIJ Offshore Leaks Database.

6.2 Case Study: The Nawaz Sharif Family

A high-profile case documented within the ICIJ Offshore Leaks Database involves three children of former and current Pakistan Prime Minister Nawaz Sharif — Mariam, Hasan, and Hussain — who were owners or had authorization rights for several companies identified in the Panama Papers.

Data collected by the ICIJ established the following:

- Daughter Mariam Safdar was the owner of British Virgin Islands-based firms Nielsen Enterprises Limited and Nescoll Limited, incorporated in 1994 and 1993 respectively. These companies owned London properties for family use.

- In June 2007, Hussain and Mariam signed documents in which Deutsche Bank Geneva lent up to USD 13.8 million to Nescoll, Nielsen, and another company, using their London properties as collateral.
- Hasan Nawaz Sharif was the sole director of Hangon Property Holdings Limited, incorporated in the British Virgin Islands in February 2007. The Liberia-based firm Cascon Holdings Establishment Limited was a shareholder of Hangon.
- Mossack Fonseca, aware that Mariam Safdar was Nawaz Sharif's daughter and thus a Politically Exposed Person (PEP), committed to checking her activities twice a year beginning July 2012. Mossack Fonseca later resigned as agent for Hangon after Hasan Nawaz Sharif was similarly identified as a PEP.

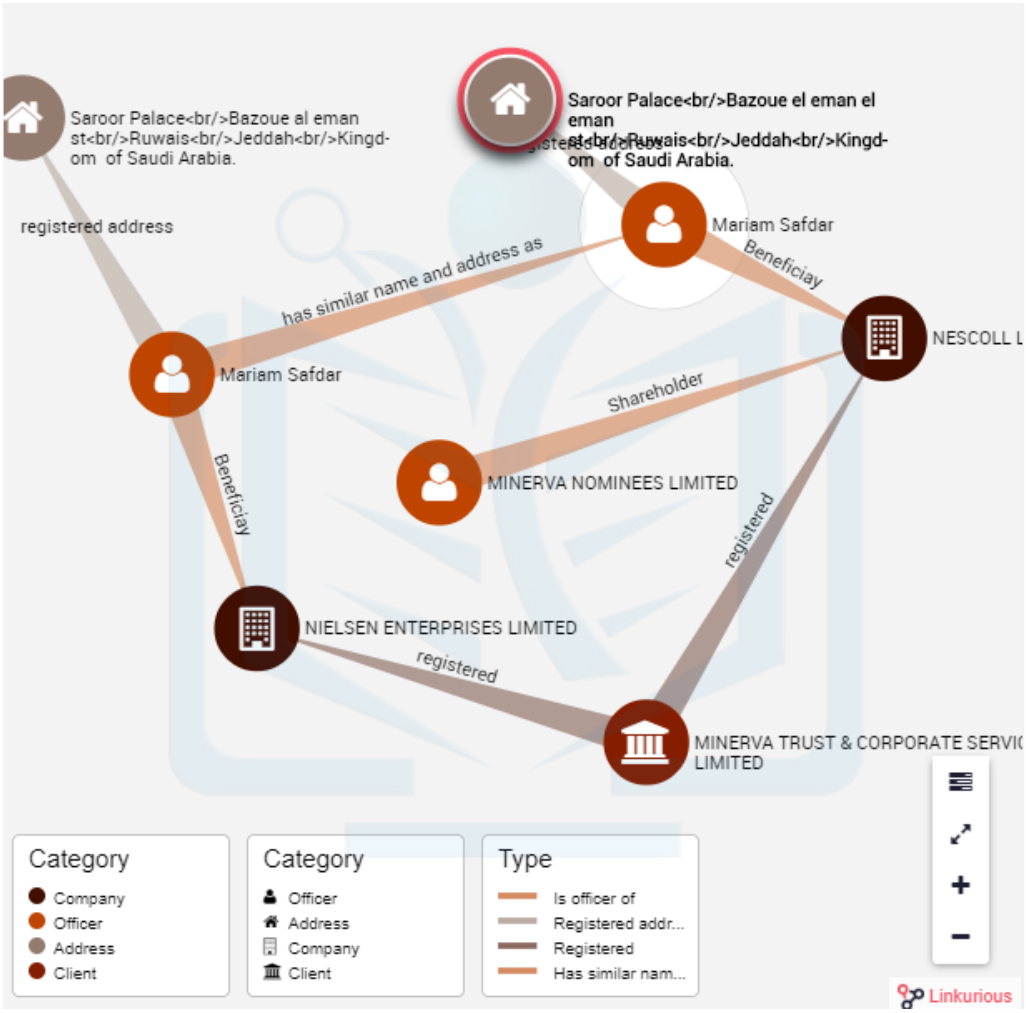

Figure 7. ICIJ network diagram illustrating the connections between Mariam Safdar, Nielsen Enterprises Limited, Nescoll Limited, Minerva Nominees Limited, and Minerva Trust & Corporate Services Limited — as revealed in the Panama Papers. Source: ICIJ Offshore Leaks Database / Linkurious visualization.

PART II: REGULATORY FRAMEWORK & ENFORCEMENT

Global Standards, U.S. Legislation, and Compliance Architecture

Chapter 7: Global Regulatory Architecture

7.1 FATF Standards and 2024–2025 Updates

The Financial Action Task Force (FATF) is the single most influential body shaping the global anti-money laundering (AML) and counter-terrorist financing (CFT) landscape. Its rolling program of mutual evaluations, guidance updates, and typologies reports defines the threshold of regulatory adequacy against which regulators, correspondent banks, and enforcement agencies measure institutional performance (FATF, 2025).

The FATF Recommendations — adopted in February 2012 and regularly updated — set out a comprehensive and consistent framework of measures which countries should implement to combat money laundering and terrorist financing. The most recent version was updated in June 2026. Key FATF typologies and guidance publications relevant to CIRS professionals include:

FATF Publication	Year / Theme
International Co-operation on ML Detection, Investigation, and Prosecution Handbook	June 2025
Comprehensive Update on Terrorist Financing Risks	June 2025
Detecting, Disrupting and Investigating Online Child Sexual Exploitation	Feb 2025
Beneficial Ownership and Transparency of Legal Arrangements	March 2024
Money Laundering National Risk Assessment Guidance	March 2024
Misuse of Citizenship and Residency by Investment Programmes	Nov 2023
Illicit Financial Flows from Cyber-enabled Fraud	Nov 2023
Risk-Based Approach Guidance for the Real Estate Sector	July 2022
Trade-Based Money Laundering: Trends and Developments	Dec 2020
Virtual Assets Red Flag Indicators	Sept 2020

Table 3. Selected FATF Methods and Trends Publications. Source: FATF (2025); Eurasian Group (2025).

A 2025 assessment of FATF's 4th Round Mutual Evaluations found that 69% of 194 participating jurisdictions had major or structural deficiencies in effectively investigating, prosecuting, and convicting terrorism financing cases. This underscores the persistent gap between formal regulatory architecture and practical enforcement effectiveness (White & Case LLP, 2025).

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

FATF identifies jurisdictions with weak AML/CFT measures through its 'black list' (High-Risk Jurisdictions Subject to a Call for Action) and 'grey list' (Jurisdictions Under Increased Monitoring), published three times per year. As of October 2025, FATF continued to update these designations, providing investigators with a current risk map of jurisdictions requiring heightened due diligence in cross-border transactions (FATF, 2025).

7.2 The U.S. Corporate Transparency Act (CTA) and BOI Reporting

The U.S. Corporate Transparency Act (CTA), enacted as part of the Anti-Money Laundering Act of 2020 (AMLA 2020), represented the most significant reform of U.S. anti-money laundering rules since the post-9/11 PATRIOT Act. The CTA's core mechanism — the Beneficial Ownership Information (BOI) reporting requirement — was designed to 'unmask shell companies and protect the U.S. financial system from abuse by money launderers, drug traffickers, sanctioned oligarchs, and other criminals,' according to FinCEN Acting Director Himamauli Das (FinCEN, 2024).

FinCEN launched the BOI E-Filing website (boiefiling.fincen.gov) on January 1, 2024. The system required many corporations, LLCs, and other entities to report the identities of their beneficial owners — the persons who ultimately own or control the company (FinCEN, 2024).

Critical 2025 Development: Domestic BOI Reporting Suspended
On March 21, 2025, FinCEN issued an interim final rule removing the requirement for U.S. companies and U.S. persons to report BOI to FinCEN under the Corporate Transparency Act. All entities created in the United States — including those previously known as 'domestic reporting companies' — are now exempt from BOI reporting requirements. The rule narrows the definition of 'reporting company' to mean only entities formed under foreign law that have registered to do business in a U.S. State or Tribal jurisdiction (FinCEN, 2025). Foreign reporting companies registered before March 26, 2025 must file BOI reports by April 25, 2025.

The FinCEN BOI database, when populated, would have been used in national security, intelligence, and law enforcement efforts to combat corruption through shell companies, money laundering, drug and human trafficking, tax evasion, terrorism, and other illicit activity (Epstein Becker Green, 2025). Despite the suspension of domestic reporting requirements, investigators still have access to BOI data filed before the rule change, and foreign entities remain subject to reporting.

FinCEN has made clear that it does not send correspondence requesting payment to file BOI and that any such correspondence should be treated as fraudulent — reflecting the emergence of scams abusing the CTA framework (FinCEN, 2025).

7.3 International AML Compliance Architecture

Beyond FATF and U.S. legislation, the global AML/CFT compliance architecture encompasses several interconnected regulatory and supervisory frameworks that CIRS professionals must understand:

- The Egmont Group — a global organization of national Financial Intelligence Units (FIUs) coordinating operational information exchange. The Egmont Group's 2024 research on non-profit organization abuse was cited in the FATF's 2025 Comprehensive Update on Terrorist Financing Risks.
- The Basel AML Index — published annually by the Basel Institute on Governance, ranking countries by their money laundering and terrorist financing risk levels. Used extensively in correspondent banking risk assessment.
- The Wolfsberg Group AML Principles — a consortium of 13 global banks that publishes guidance on managing financial crime risks, including standards for SAR filing, correspondent banking, and trade finance.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

- The European Union's Anti-Money Laundering Directives (AMLD) — a series of progressively stronger directives, with the 6th AMLD strengthening criminal liability for money laundering and expanding the list of predicate offenses.
- The U.S. Bank Secrecy Act (BSA) and its implementing regulations, administered by FinCEN, which require financial institutions to maintain AML compliance programs, file Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs), and implement Know Your Customer (KYC) procedures.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

PART III: TRAINING GUIDE

Investigative Research Methodology for CIRS™ Candidates

Chapter 8: Framework for Investigating Hidden Assets

Investigative research into international money laundering and hidden foreign assets requires a structured, systematic approach that combines legal knowledge, database access skills, and analytical methodology. This chapter provides the CIRS™ candidate with a practical framework for conducting such investigations.

8.1 Key Information Required for Hidden Asset Verification

Investigative research into hidden assets requires access to the following categories of information, which form the primary evidence chain in any offshore wealth investigation:

1. The names of the ultimate beneficial owner(s) — the real person(s) who own or control the entity.
2. Knowledge of the source of assets — where the funds originated and how they were initially generated.
3. The company or trust name and its declared objective — as registered vs. as actually operated.
4. Data from a competent authority — e.g., company registrars, FIUs, regulatory filings.
5. The entity registration jurisdictions — which countries and territories are involved.
6. The names of officers, directors, and shareholders who provide a front — nominees hiding the true beneficial owner.
7. Documentation of formation arrangements — trust deeds, shareholder agreements, power of attorney, etc.
8. Transaction records — where available, bank statements, wire transfer records, invoices.

8.2 Piercing the Corporate Veil — Investigative Techniques

A World Bank study in 2011 assembled a database of 150 cases of grand corruption over 30 years, finding that 112 of these cases involved transnational entities such as offshore companies and bank accounts. The World Bank's publication The Puppet Masters (Findley et al., 2014) details how sophisticated looters use multiple jurisdictions and layered companies to obscure the wealth trail — and provides a blueprint for investigators working to reverse-engineer those structures.

Step 1: Build the Family and Network Tree

The starting point for any corruption investigation is constructing a comprehensive family tree of the subject and then extending it to known associates, business partners, and political allies. Databases including electoral records, property registries, corporate filings, and social media profiles are used to identify nominees and family members who may hold assets on behalf of the subject (Coronel, 2012).

Step 2: Identify Real Property Holdings

Houses are among the easiest assets to find. Most countries make real property records publicly available. Even when properties are not in the subject's name, the subject and family members are often physically present at high-value properties, generating footprints in local records (utility accounts, neighborhood association records, property tax records, building permits). Property records frequently lead to the names of shell companies and nominees used for the purchase, and to the banks, lawyers, and real estate agents involved (Coronel, 2012).

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Step 3: Penetrate Corporate Structures

Excessive complexity in corporate structures is a red flag — it signals an intent to conceal something. A layered structure crossing multiple jurisdictions suggests deliberate obfuscation. Tools for penetrating corporate structures include:

- Online corporate registries — the Hong Kong ICRIS database is an example of excellence in public-access corporate registration data.
- Subscription databases — Dun & Bradstreet, Bureau van Dijk, LexisNexis, and Refinitiv World-Check provide proprietary corporate intelligence.
- OpenCorporates — has scraped data on hundreds of millions of companies from corporate registries worldwide, enabling searches by director name, company name, and jurisdiction.
- The ICIJ Offshore Leaks Database — for entities identified in the five major leak investigations.
- The Investigative Dashboard — maintained by nonprofit investigative reporting centers, with links to corporate registers worldwide.

Step 4: Work Human Sources

Many successful offshore investigations have tapped human sources to unravel transnational schemes. Service providers — lawyers, accountants, agents, registry companies — have been known to share information. Sometimes the front men (or women) confess for fear of legal liability, as occurred in the BAE Systems scandal, where a travel agency managing director brought documents to police rather than risk prosecution. Whistleblowers and undercover operations have also proved effective in exposing offshore service providers (Coronel, 2012).

8.3 Red Flags for Money Laundering — Investigator Checklist

Structural Red Flags	Transactional Red Flags
Nominee directors with no apparent business role	Transactions with no clear business purpose
Multiple layers of offshore entities in secrecy jurisdictions	Round-number transactions just below reporting thresholds (structuring)
Use of a flee clause in trust deeds	Rapid movement of funds through multiple accounts
PEPs listed as beneficial owners or family nominees	Payments disguised as legitimate business expenses
Mismatch between declared business activity and banking patterns	Use of multiple bank accounts in high-secrecy jurisdictions
Excessive legal privilege claimed over corporate documents	Cryptocurrency mixer or tumbler activity

Table 4. Money Laundering Red Flags for CIRS Investigators. Source: FATF (2025); AUSTRAC (2021); ICA (2022).

Chapter 9: Research Tools, Databases, and Resources

9.1 Using the ICIJ Offshore Leaks Database — Step-by-Step Guide

The ICIJ Offshore Leaks Database (offshoreleaks.icij.org) is the primary public intelligence resource for investigating offshore corporate structures. As of 2025, the database encompasses more than

810,000 entities from five major leak investigations. The following guidance, based on ICIJ's recommended methodology, provides a systematic approach to effective database use (ICIJ, 2022; Bellingcat, 2026):

Step 1: Download and Cross-Reference the Data

The full ICIJ Offshore Leaks database can be downloaded as ZIP files containing CSV data and is also available through a Reconciliation API compatible with tools such as OpenRefine. For systematic investigation, download the data and cross-reference it with other public datasets — the Forbes 500 list, lists of elected officials, or corporate registry exports — using OpenRefine or Excel's Fuzzy Lookup add-in. These tools compare character strings to identify similar but not identical names, matching variations such as 'John Doe,' 'John R. Doe,' and 'Doe, John' (ICIJ, 2022).

Step 2: Verify and Check for False Positives

Cross-referencing will generate false positives — individuals or companies with the same or similar names who are not the person sought. Return to the Offshore Leaks database and search specifically for the candidate name to find other companies associated with the same person and expand the network of connected entities by examining related nodes (ICIJ, 2022).

Step 3: Explore Network Relationships Using the Relationship Chart

The ICIJ database's network visualization tool (powered by Linkurious) allows investigators to visualize the web of relationships between entities — showing connections between officers, intermediaries, entities, and addresses. Entity nodes, officer nodes, and intermediary nodes are color-coded, with relationship types labeled. Expanding nodes reveals second and third-degree connections that may identify the ultimate beneficial owner behind multiple layers of nominees (ICIJ, 2022; Bellingcat, 2026).

Step 4: Filter by Jurisdiction and Dataset

The database allows filtering by investigation (Panama Papers, Pandora Papers, etc.), jurisdiction, and linked country. For investigations involving specific financial havens, filtering by British Virgin Islands, Cayman Islands, Panama, or Bahamas immediately narrows the universe of relevant entities. The Power Players section enables searches for notable names linked to world leaders, politicians, and their relatives across Panama Papers, Paradise Papers, and Pandora Papers simultaneously (ICIJ, 2022; Bellingcat, 2026).

9.2 Additional OSINT and Investigative Resources

Resource / Database	Purpose and Access
OpenCorporates (opencorporates.com)	Scraped data on hundreds of millions of companies from 130+ corporate registries worldwide. Free and API-accessible.
Investigative Dashboard (investigativedashboard.org)	Links to corporate registries worldwide, maintained by nonprofit investigative journalism centers.
OpenSanctions (opensanctions.org)	Combines ICIJ Offshore Leaks, sanctions lists, and PEP databases into a unified, queryable dataset.
Global Financial Integrity (gfintegrity.org)	Research on illicit financial flows globally; estimates and policy analysis.
Bureau van Dijk / Orbis	Proprietary database on companies worldwide including ownership structures and financial data.

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Resource / Database	Purpose and Access
Dun & Bradstreet	Commercial company intelligence including directors, shareholders, and financial risk data.
World Bank Puppets Masters Database	150 grand corruption cases with entity mapping and asset recovery documentation.
FATF Public Statements	Current FATF black and grey lists; jurisdictional risk assessments.
FinCEN BOI E-Filing Portal	Filed beneficial ownership reports for foreign reporting companies (boiefiling.fincen.gov).
Bellingcat Online Investigation Toolkit	OSINT tool guide including ICIJ database navigation tutorials and other investigative tools.

Table 5. Key Research Databases and OSINT Resources for CIRS Financial Investigators.

Chapter 10: Annexure — U.S. Fraud and Financial Crime Reporting Agencies

The following federal agencies should be contacted based on the specific type of fraud or financial crime encountered by the CIRS investigator or the researcher's client. Investigators should direct victims to the appropriate reporting channel, which will also establish an official record relevant to any subsequent civil or criminal proceeding.

Fraud / Crime Category	Reporting Agency and Resource
Common scams and fraud	Federal Trade Commission (FTC) — reportfraud.ftc.gov | ftccomplaintassistant.gov
Census fraud	U.S. Census Bureau — Regional Office (census.gov/about/regions.html)
Food stamp (SNAP) fraud	USDA Office of Inspector General (fns.usda.gov/fraud)
Financial fraud (credit, loans, mortgages)	Consumer Financial Protection Bureau (consumerfinance.gov/complaint)
Identity theft / data breaches	IdentityTheft.gov — includes recovery plan assistance
Immigration fraud	U.S. Immigration and Customs Enforcement (ice.gov/webform/hsi-tip-form)
International scams (e-commerce, travel)	Econsumer.gov — multi-country complaint portal
Internet fraud (phishing, malware, spoofing)	Internet Crime Complaint Center — IC3.gov
Investment fraud	Securities and Exchange Commission (investor.gov) / state securities regulator
IRS / government imposter scams	Treasury Inspector General for Tax Administration (TIGTA) — 1-800-366-4484
Mail fraud	U.S. Postal Inspection Service (postalinspectors.uspis.gov)
Medicaid fraud	State Medicaid program office; HHS Inspector General fraud directory

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Fraud / Crime Category	Reporting Agency and Resource
Medicare fraud	Department of Health and Human Services Inspector General
Misuse of federal funds	Government Accountability Office — FraudNet form (gao.gov)
Moving fraud (interstate)	Federal Motor Carrier Safety Administration (FMCSA)
Social Security fraud	Social Security Administration Inspector General (ssa.gov/fraudreport)
Telephone scams	Federal Communications Commission (FCC) — consumercomplaints.fcc.gov
Welfare (TANF) fraud	HHS Inspector General — 1-800-HHS-TIPS (1-800-447-8477)

Table 6. U.S. Federal Fraud and Financial Crime Reporting Agencies. Source: USA.gov; FinCEN (2025).

Chapter 11: Learning Objectives and Competency Assessment

Upon completing this module, CIRS™ candidates should be able to demonstrate the following competencies in the domain of financial crime investigation and international money laundering research:

CORE COMPETENCIES — CIRS Module 10, Unit 25

1. Define money laundering and articulate the three-stage placement–layering–integration model with real-world examples.
2. Explain how the Hawala system, trade-based money laundering, and physical cash smuggling enable the placement stage.
3. Describe the mechanics of shell companies, offshore trusts, and nominee arrangements in laundering schemes.
4. Analyze the four primary laundering methods (corporate vehicles, third parties, professional facilitators, and international transfers).
5. Identify global financial haven jurisdictions and explain their legal and regulatory characteristics.
6. Apply ICIJ Offshore Leaks Database search methodology, including cross-referencing, false-positive checking, and network visualization.
7. Explain the significance and investigative implications of the Panama, Paradise, Bahamas, and Pandora Papers leaks.
8. Assess the emerging role of cryptocurrency and virtual assets in modern money laundering schemes.
9. Apply the investigative framework for hidden asset detection, including corporate veil piercing and real property tracing.
10. Identify AML red flags and apply regulatory reporting knowledge (FATF, FinCEN, CTA/BOI).

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

References

All references are formatted in accordance with the Publication Manual of the American Psychological Association, 7th Edition (APA, 2020).

Australian Transaction Reports and Analysis Centre (AUSTRAC). (2021). Methodologies used by corrupt politically exposed persons (PEPs) to launder the proceeds of corruption. Australian Government. https://www.austrac.gov.au

Bellingcat. (2026, April). ICIJ Offshore Leaks Database. In Bellingcat's Online Investigation Toolkit. https://bellingcat.gitbook.io/toolkit/more/all-tools/icij-offshore-leaks-database

Chainalysis. (2024, July). Money laundering and cryptocurrency: Trends and new techniques for detection and investigation [Report preview]. https://www.chainalysis.com/blog/money-laundering-cryptocurrency/

Chainalysis. (2025). 2025 crypto crime report. https://www.chainalysis.com

Coronel, S. (2012). Following the money: How to track the proceeds of corruption. International Consortium of Investigative Journalists. https://www.icij.org

Elliptic. (2025, August). Levelling up crypto fraud and money laundering investigations with automatic behavioral detection. https://www.elliptic.co/blog

Epstein Becker Green. (2025, January). Corporate Transparency Act's January 1, 2025, deadline looms for reporting companies existing prior to 2024. https://www.ebglaw.com

Eurasian Group. (2025). FATF typology reports. https://eurasiangroup.org/en/fatf-typology-reports

Financial Action Task Force (FATF). (2013). The role of Hawala and other similar service providers in money laundering and terrorist financing. FATF/OECD. https://www.fatf-gafi.org

Financial Action Task Force (FATF). (2015). Money laundering through the physical transportation of cash. FATF/OECD. https://www.fatf-gafi.org

Financial Action Task Force (FATF). (2022). Risk-based approach guidance for the real estate sector. FATF/OECD. https://www.fatf-gafi.org

Financial Action Task Force (FATF). (2024). Money laundering national risk assessment guidance. FATF/OECD. https://www.fatf-gafi.org

Financial Action Task Force (FATF). (2024). Targeted update on virtual assets. FATF/OECD. https://www.fatf-gafi.org

Financial Action Task Force (FATF). (2025). Comprehensive update on terrorist financing risks. FATF/OECD. https://www.fatf-gafi.org

Financial Action Task Force (FATF). (2025). FATF recommendations [Last updated June 2026]. FATF/OECD. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

Financial Action Task Force (FATF). (2025). International co-operation on money laundering detection, investigation, and prosecution handbook. FATF/OECD. https://www.fatf-gafi.org

Financial Crimes Enforcement Network (FinCEN). (2024). U.S. beneficial ownership information registry now accepting reports. U.S. Department of the Treasury. https://www.fincen.gov

Financial Crimes Enforcement Network (FinCEN). (2025, March). FinCEN removes beneficial ownership reporting requirements for U.S. companies and U.S. persons, sets new deadlines for foreign companies. U.S. Department of the Treasury. https://www.fincen.gov/news/news-releases

Findley, M., Nielson, D., & Sharman, J. (2014). Global shell games: Experiments in transnational relations, crime, and terrorism. Cambridge University Press.

FluxForce. (2025). Cryptocurrency laundering volumes: 2024 statistics. https://www.fluxforce.ai/statistics/crypto-laundering-volumes

Hellvig, A., & Blanaru, I. (2023). Money laundering typologies and detection in the digital era. Journal of Financial Crime, 30(4), 1123–1141.

International Compliance Association (ICA). (2022). Anti-money laundering: The basics. ICA. https://www.int-comp.org

International Consortium of Investigative Journalists (ICIJ). (2013). ICIJ releases Offshore Leaks database revealing names behind secret companies and trusts. https://www.icij.org

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

International Consortium of Investigative Journalists (ICIJ). (2016). Panama Papers investigation. https://panamapapers.icij.org

International Consortium of Investigative Journalists (ICIJ). (2018). ICIJ releases Paradise Papers data — Appleby. https://www.icij.org/investigations/paradise-papers

International Consortium of Investigative Journalists (ICIJ). (2021, October). Pandora Papers: An offshore data tsunami. https://www.icij.org/investigations/pandora-papers/about-pandora-papers-leak-dataset/

International Consortium of Investigative Journalists (ICIJ). (2021, December). ICIJ releases new Pandora Papers data from two offshore service providers. https://www.icij.org/investigations/pandora-papers

International Consortium of Investigative Journalists (ICIJ). (2022, May). ICIJ publishes final batch of Pandora Papers data on more than 9,000 offshore companies, trusts and foundations. https://www.icij.org/investigations/pandora-papers

International Consortium of Investigative Journalists (ICIJ). (2022). ICIJ Offshore Leaks database [Data set]. https://offshoreleaks.icij.org

Levi, M. (2022). Money laundering risks and the role of financial intelligence. Journal of Financial Crime, 29(1), 4–16.

Mallik, R., Patel, K., & Sen, A. (2025). AI-generated synthetic financial identities: A new threat to AML compliance. Journal of Financial Regulation and Compliance, 33(2), 188–210.

Munge, P., Onyango, D., & Mwangi, A. (2024). Real estate money laundering: Evolving methods and detection frameworks. Journal of Financial Crime, 31(3), 789–812.

TrustSphere AI. (2025, June). FATF 2025 typologies update: What financial institutions need to act on now. https://www.trustsphere.ai/post/fatf-2025-typologies-update

U.S. Department of State, Bureau for International Narcotics and Law Enforcement Affairs. (2024). International narcotics control strategy report: Volume II — Money laundering. U.S. State Department. https://www.state.gov

U4 Expert Answer. (2022). Overview of money laundering: Definition, stages, and methods. Chr. Michelsen Institute. https://www.u4.no

United Nations Office on Drugs and Crime (UNODC). (2023). Money-laundering and globalization. UNODC. https://www.unodc.org

Verafin. (2024). Financial crime report 2024. Verafin. https://verafin.com

White & Case LLP. (2025, September). The evolving threat of terrorist financing: Understanding and managing risk. https://www.whitecase.com/insight-alert

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

Index

Note: Page numbers are approximate and based on document structure. Use Ctrl+F (Find) in Word to locate specific terms.

A

Anti-Money Laundering (AML) 12, 25–28, 40–43
AUSTRAC (Australian Transaction Reports and Analysis Centre) 17, 19, 36

B

Bahamas Leaks (2016) 30–31
Bank Secrecy Act (BSA) 43
Basel AML Index 43
Bearer shares 15
Beneficial Ownership Information (BOI) 40–42
British Virgin Islands (BVI) 14, 15, 31, 32, 34

C

Cayman Islands 14, 15, 18
Chainalysis 2025 Crypto Crime Report 23–24
Corporate Transparency Act (CTA) 40–42
Cryptocurrency laundering 23–25
Customer Due Diligence (CDD) 21

D

Dark Web 24
Discretionary offshore trust 16
Dun & Bradstreet 34, 50

E

Egmont Group 43
Elliptic (blockchain analytics) 24
Enhanced Due Diligence (EDD) 21

F

FATF (Financial Action Task Force) 9, 21, 23–24, 38–39
FATF Black and Grey Lists 39
FATF Recommendations 38–39
FinCEN (Financial Crimes Enforcement Network) 40–42
Flee clause (trust) 16
Front companies / front businesses 14, 18, 20

G

Global Financial Integrity (GFI) 28, 50
Gatekeepers (professional facilitators) 20–21

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

H

Hawala system 12–13
Hundi (see Hawala) 13

I

ICIJ Offshore Leaks Database 28–35, 47–49
Identity theft (AI-generated synthetic identities) 26
Informal Value Transfer Systems (IVTS) 13
Integration stage (money laundering) 8
Irrevocable offshore trust 15

K

Know Your Customer (KYC) 26, 43

L

Layering stage (money laundering) 8
Legal practitioners as facilitators 20–21

M

Money laundering, definition 7
Mossack Fonseca 31, 34

N

Nawaz Sharif case study 33–35
Nominee directors 14
North Korea (crypto theft) 23

O

Offshore Leaks (2013) 30
Offshore trusts — types 15–16
OpenCorporates 34, 50
OpenSanctions 50

P

Panama Papers (2016) 31
Pandora Papers (2021) 32–33
Paradise Papers (2017–2018) 31
Peel chains (cryptocurrency) 24
Placement stage (money laundering) 7–8
Politically Exposed Persons (PEPs) 20, 22, 34, 37
Professional Money Laundering Networks (PMLNs) 9, 21, 25

R

Real estate laundering 25–26
Red flags (money laundering) 45
Revocable offshore trust 15

© 2025 Association of Internet Research Specialists (AOFIRS) | Mississauga, Ontario, Canada

S

Shell companies 13–15
Smurfing / structuring 9, 45
Stablecoins (illicit use) 23
Suspicious Activity Reports (SARs) 9, 25, 43

T

Trade-Based Money Laundering (TBML) 13
Three-stage model 7–8
Trust companies 16

U

United Nations Office on Drugs and Crime (UNODC) 7
U.S. Federal fraud reporting agencies 52–53

V

Virtual assets / virtual asset service providers (VASPs) 23–24, 38

W

Wolfsberg Group AML Principles 43
World Bank Puppet Masters database 34, 46

Association of Internet Research Specialists (AOFIRS)
Mississauga, Ontario, Canada | www.aofirs.org
CIRS™ is a trademark of the Association of Internet Research Specialists.
© 2019–2025 AOFIRS. All rights reserved. No part of this document may be reproduced without written permission.

Association of Internet Research Specialists

This combined Research Report and Training Guide provides a comprehensive examination of international money laundering schemes and the detection of hidden foreign assets. It is designed for Certified Internet Research Specialists (CIRS™) seeking advanced competency in financial crime intelligence — incorporating foundational methodology alongside the most current typologies, enforcement developments, and investigative tools available as of 2025.

Money laundering represents one of the most pervasive forms of financial crime globally, with the United Nations Office on Drugs and Crime (UNODC) estimating that 2–5% of global GDP — roughly USD 800 billion to USD 2 trillion — is laundered annually (UNODC, 2023). As criminal networks and corrupt political actors grow more sophisticated in their use of offshore jurisdictions, shell companies, trusts, and emerging digital asset platforms, the role of the internet research specialist in tracing illicit financial flows has never been more critical.

This report covers traditional three-stage money laundering theory; the Hawala system and informal value transfer networks; the mechanics of shell companies, offshore trusts, and financial havens; four primary laundering methodologies using corporate vehicles, third parties, professional facilitators, and international wire transfers; emerging 2024–2025 typologies including cryptocurrency laundering and Professional Money Laundering Networks (PMLNs); the ICIJ Offshore Leaks Database — now encompassing 810,000+ entities from Panama Papers, Paradise Papers, Bahamas Leaks, and Pandora Papers; the U.S. Corporate Transparency Act (CTA) and the latest FinCEN Beneficial Ownership Information (BOI) reporting developments; and a detailed investigative training framework for CIRS™ candidates.

A full APA reference list and subject index are provided at the close of the report.

International Money Laundering Schemes & Foreign Assets Detection

Submitted by:

Naveed Manzoor

USVA7777904052027

May 10, 2026

Association of Internet Research Specialist | AOFIRS