INTELLIGENCE · CONCEPTS AND HISTORY

The Integration of Financial Intelligence into Broader Threat Knowledge

Money leaves traces that criminals and terrorists find hard to hide. This article explains how financial intelligence is gathered through anti-money-laundering systems, how it is analysed, how it feeds into wider knowledge of threats, and why its effectiveness remains contested.

ModQu research article · 1,813 words · 18 references (APA 7th edition)

Almost every serious threat needs money. Drug trafficking networks must move and hide their profits; terrorist groups must pay for travel, weapons and recruitment; corrupt officials must disguise bribes; states seeking to evade sanctions must find banks willing to process their payments. Each of these activities leaves financial traces: accounts, transfers, invoices, company registrations. **Financial intelligence** is the knowledge produced by collecting and analysing those traces. Over the past three decades it has grown from a specialised tool against drug money into a central part of how governments understand and counter crime, terrorism and hostile states. This article explains how financial intelligence is produced, how it is integrated with other sources, and why debate continues about how well it works.

The anti-money-laundering system

Most financial intelligence comes from a system built to combat money laundering. Its foundations are international standards set by the Financial Action Task Force, an intergovernmental body created in 1989. Its Recommendations require countries to criminalise money laundering, to oblige banks and other businesses to identify their customers and report suspicious transactions, and to create a national **financial intelligence unit** to receive and analyse those reports (Financial Action Task Force, 2012).

Reuter and Truman (2004) describe the system as having two pillars. The **prevention** pillar places duties on private businesses: knowing their customers, keeping records and reporting suspicious or large transactions. The **enforcement** pillar uses that information to investigate, prosecute and confiscate. Levi and Reuter (2006) note that the system rests on an unusual bargain: private companies act as the eyes of the state, collecting intelligence on their own customers as a condition of doing business.

In Canada, these obligations are set out in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (2000), which requires banks, money services businesses, casinos, real estate agents, dealers in precious metals and others to report suspicious transactions, large cash transactions and large international transfers to the national financial intelligence unit. Most other countries have comparable laws.

Financial intelligence units

The International Monetary Fund and World Bank (2004) describe the financial intelligence unit as a central national agency that receives, analyses and disseminates financial information to combat money laundering and terrorist financing. Units take different forms: some are administrative agencies separate from the police, some sit within police services, and some are attached to prosecutors. All share the same basic function, shown in Figure 1: they collect reports from businesses, analyse them together with other information, and pass relevant findings to agencies that can act.

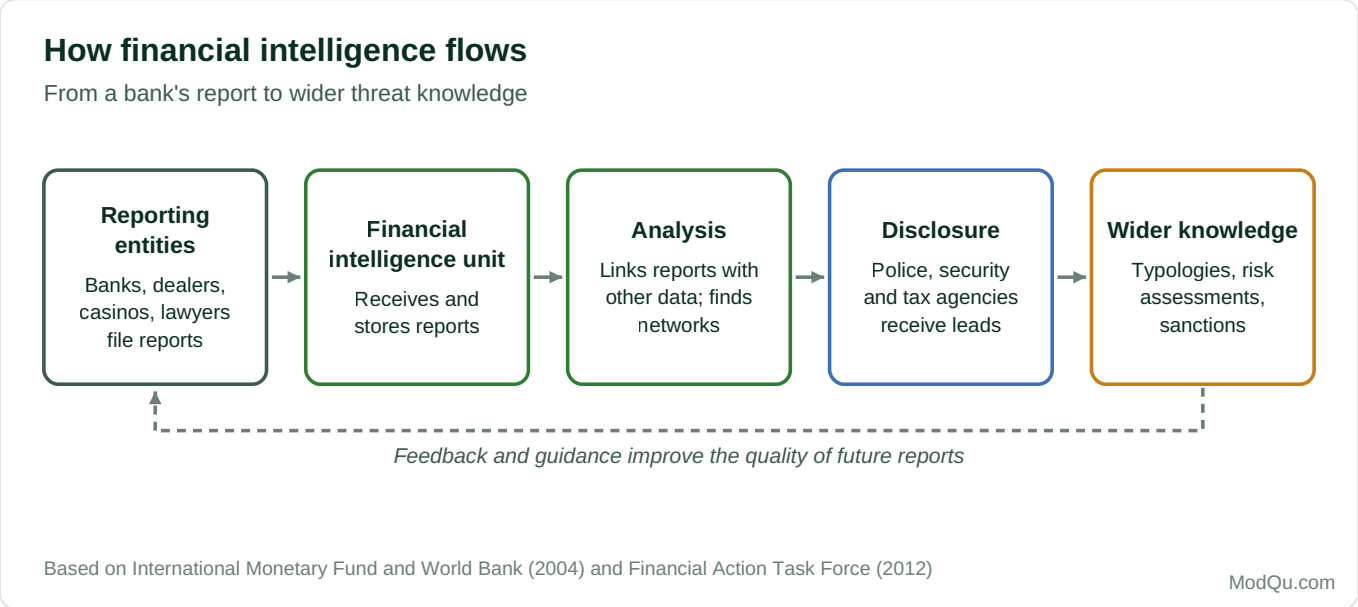


Figure 1. How financial intelligence flows. Reports from businesses become intelligence only after analysis and dissemination; feedback to reporters improves future reports. Based on International Monetary Fund and World Bank (2004) and Financial Action Task Force (2012); diagram by ModQu.

Financial intelligence units also cooperate internationally, exchanging information through secure networks, because money moves across borders far more easily than police investigations do.

How financial intelligence is analysed

A single suspicious transaction report rarely means much on its own. Its value comes from combination. Analysts link reports that share names, accounts, addresses or telephone numbers, and match them with police records, company registries, property records and customs data. Patterns that are invisible in one bank's records may emerge when reports from many institutions are combined.

Network analysis is central to this work. Sparrow (1991) argued that criminal organisations are best understood as networks, and that identifying the brokers who connect different parts of a network shows where disruption will have most effect. In financial investigations those brokers are often professional facilitators: accountants, lawyers or company formation agents who create the structures through which money moves.

Analysts also study **typologies**: recurring methods of laundering or financing, such as trade-based laundering through false invoices, the use of shell companies, or the structuring of cash deposits to stay below reporting thresholds. Typologies help businesses recognise suspicious activity and help analysts interpret what they find.

Financial intelligence serves different purposes at different levels. At the **tactical** level, it supports individual investigations, tracing assets and identifying associates. At the **operational** level, it reveals networks and the facilitators who serve them. At the **strategic** level, it informs national risk assessments, showing which sectors are most exposed, how methods are changing and where laws need strengthening.

Following the money of terrorism

The attacks of September 11, 2001, transformed the profile of financial intelligence. The 9/11 Commission found that the attacks cost relatively little, perhaps several hundred thousand dollars, and that the money moved through ordinary bank transfers and cash without raising suspicion (National Commission on Terrorist Attacks Upon the United States, 2004). The Commission concluded that stopping terrorist financing entirely was unrealistic, but that tracing it could reveal networks and connections that other intelligence missed.

Biersteker and Eckert (2008) review the international effort that followed: asset freezes, new reporting obligations and closer scrutiny of charities and informal money transfer systems. They and Levi (2010) caution that the amounts involved in terrorism are often too small to stand out, so the main value of financial intelligence lies less in prevention than in understanding: identifying who is connected to whom, how groups are funded and how they adapt.

Financial intelligence as statecraft

Financial intelligence is also used against states. Zarate (2013), who helped lead the United States Treasury's efforts after 2001, describes how detailed knowledge of the global banking system allowed governments to cut targeted individuals, companies and banks off from international finance. Because most international payments pass through a small number of major banks and currencies, intelligence about who is using them, and for what, became a powerful instrument of foreign policy. The same knowledge supports sanctions against states pursuing nuclear weapons or engaged in aggression, and the monitoring of efforts to evade them.

Lowenthal (2022) notes that this has drawn finance ministries into the intelligence community, and that financial intelligence now forms part of the all-source picture of many national security threats.

Integration with other sources

Financial intelligence is most useful when combined with other sources. A human source may name a suspect; financial records can confirm whom the suspect pays and who pays the suspect. Communications intercepts may reveal a plan; financial data can show whether money has moved to carry it out. Conversely, an unusual pattern of payments may prompt other collection to find out what lies behind it.

Integration also works in the other direction. Investigative journalism and leaked data have repeatedly revealed financial structures that official systems missed. Obermayer and Obermaier (2016) describe how a leak of millions of documents from a law firm specialising in offshore companies, the Panama Papers, exposed how politicians, criminals and wealthy individuals used shell companies to hide assets, prompting investigations in many countries. Such disclosures feed back into official knowledge, informing risk assessments and reforms of company ownership rules.

Financial intelligence inside businesses

Financial intelligence is not produced only by governments. Banks, payment companies and other regulated businesses run their own intelligence functions, because they must decide which customers to accept, which transactions to question and which relationships to end. Their compliance teams screen customers against sanctions lists, monitor transactions with automated rules and models, and investigate alerts before deciding whether to file a report. In doing so they build detailed knowledge of the risks in their own customer base. Unger and van Waarden (2009) note that the shift to risk-based regulation made this judgement central: institutions are expected to understand their own exposure rather than simply apply fixed thresholds.

In recent years several countries have created partnerships in which government agencies share information about specific threats with selected banks, so that the banks can search their own records and return more focused reports. Such arrangements aim to replace the one-way flow of defensive reporting with a two-way exchange of intelligence. They also raise questions about privacy and about how much state power should be exercised through private firms, questions that Levi and Reuter (2006) identified as inherent in the system's design.

Does it work?

For all its growth, the anti-money-laundering system faces persistent questions about its effectiveness.

The volume problem. Businesses file millions of reports a year, and most are never examined in depth. Takáts (2011) modelled what was called "crying wolf": because banks are penalised for failing to report but not for over-reporting, they file defensively, flooding financial intelligence units with low-value reports and diluting the useful ones. Unger and van Waarden (2009) compared rule-based systems, which require reports above fixed thresholds, with risk-based systems, which rely on banks' judgement, and found that both can produce large volumes of data that overwhelm analysts.

Weak enforcement of the rules. Findley et al. (2014) tested compliance by requesting anonymous shell companies from thousands of company service providers around the world. Many were willing to form companies without proper identification, and providers in some wealthy countries performed worse than those in jurisdictions usually labelled as tax havens. Sharman (2011) argues that international standards have spread widely on paper, but that implementation often lags behind formal adoption.

Little evidence of impact. Pol (2020) estimates that the system recovers only a tiny fraction of criminal proceeds while imposing very large compliance costs, and calls it one of the least effective policy experiments of its kind. Levi et al. (2018) argue that the system cannot be properly evaluated because the data needed, such as the outcomes of financial intelligence disclosures, are rarely collected or published.

These critiques do not mean financial intelligence lacks value. Investigators consistently report that financial records are among the most reliable evidence available, because transactions leave records that are hard to falsify after the fact. The problem lies in the gap between the enormous collection effort and the much smaller capacity to analyse and act on what is collected, a gap familiar from many other intelligence disciplines.

Lessons for integration

Several lessons follow for anyone seeking to integrate financial intelligence into broader knowledge of threats:

1. **Prioritise quality over volume.** Clear guidance and feedback to reporting businesses improve the usefulness of what they file.
2. **Invest in analysis.** Collection without analytic capacity produces data, not intelligence.
3. **Combine sources.** Financial data are most powerful when linked with other records and intelligence.
4. **Focus on facilitators and networks.** Disrupting the professionals and structures that move money affects many criminal groups at once.
5. **Measure results.** Recording what happens to financial intelligence disclosures is the only way to know whether the system works.

Conclusion

Financial intelligence turns the traces of money into knowledge about crime, terrorism and hostile states. It depends on a vast system in which private businesses report on their customers and specialised units analyse what they receive. Integrated with other sources, it can reveal networks, confirm suspicions and inform national strategy. Its weaknesses, excessive volume, uneven compliance and little evidence of impact, are reminders that collection is only the first step: the value of financial intelligence depends on the analysis and action that follow.

References

Biersteker, T. J., & Eckert, S. E. (Eds.). (2008). *Countering the financing of terrorism*. Routledge.

Financial Action Task Force. (2012). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations* (updated 2023). FATF.

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

International Monetary Fund, & World Bank. (2004). *Financial intelligence units: An overview*. International Monetary Fund.

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice*, *34*(1), 289–375. https://doi.org/10.1086/501508

Levi, M. (2010). Combating the financing of terrorism: A history and assessment of the control of 'threat finance.' *British Journal of Criminology, 50*(4), 650–669. https://doi.org/10.1093/bjc/azq025

Levi, M., Reuter, P., & Halliday, T. (2018). Can the AML system be evaluated without better data? *Crime, Law and Social Change, 69*(2), 307–328. https://doi.org/10.1007/s10611-017-9757-4

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report*. W. W. Norton.

Obermayer, B., & Obermaier, F. (2016). *The Panama Papers: Breaking the story of how the rich and powerful hide their money*. Oneworld.

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design and Practice, 3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, S.C. 2000, c. 17 (Canada).

Reuter, P., & Truman, E. M. (2004). *Chasing dirty money: The fight against money laundering*. Institute for International Economics.

Sharman, J. C. (2011). *The money laundry: Regulating criminal finance in the global economy*. Cornell University Press.

Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13*(3), 251–274. https://doi.org/10.1016/0378-8733(91)90008-H

Takáts, E. (2011). A theory of "crying wolf": The economics of money laundering enforcement. *Journal of Law, Economics, and Organization, 27*(1), 32–78. https://doi.org/10.1093/jleo/ewp018

Unger, B., & van Waarden, F. (2009). How to dodge drowning in data? Rule- and risk-based anti money laundering policies compared. *Review of Law & Economics, 5*(2), 953–985.

Zarate, J. C. (2013). *Treasury's war: The unleashing of a new era of financial warfare*. PublicAffairs.