INVESTIGATION · BUSINESS AND CORPORATE INVESTIGATION

Anti-Money Laundering Investigations

Money laundering disguises the criminal origin of funds so that they can be used freely. This article explains how laundering works, how banks and other businesses detect and report it, how suspicious activity is investigated, and what the evidence says about how well the system works.

ModQu research article · 2,930 words · 25 references (APA 7th edition)

Crime that produces money creates a problem for the criminal: the money must be used without revealing where it came from. A drug trafficker with bags of banknotes, a fraudster with funds in a stolen account or a corrupt official with bribes paid abroad all need to make illicit proceeds look legitimate. Money laundering is the process of doing so. Because laundering usually passes through banks, payment companies, lawyers, accountants, estate agents and other businesses, governments have made those businesses responsible for detecting it and reporting it. The result is a large system of monitoring, reporting and investigation that runs from the compliance teams of private firms to financial intelligence units and law enforcement agencies.

This article explains how money laundering works, the legal framework that governs the response, how suspicious activity is detected and investigated within firms, what happens after a report is made, and what research says about the effectiveness of the whole effort.

How money laundering works

The traditional description of money laundering divides it into three stages. **Placement** introduces criminal proceeds into the financial system, for example by depositing cash in bank accounts or using it to buy assets. **Layering** moves the funds through a series of transactions, accounts, companies and jurisdictions to obscure their origin. **Integration** returns the funds to the criminal in an apparently legitimate form, such as business profits, loan repayments or the proceeds of property sales (Madinger, 2011; Reuter & Truman, 2004).



Figure 1. The placement, layering and integration model. It is a simplification: proceeds of fraud or corruption are often already in the banking system, so placement may not be needed. Diagram by ModQu.

The model is a simplification. Many modern laundering schemes skip placement entirely, because the proceeds of fraud, tax evasion or corruption are already in bank accounts. Others combine stages, or launder money through trade by over- or under-invoicing goods so that value moves across borders hidden in commercial transactions. Levi and Reuter (2006) emphasise that laundering methods vary greatly with the type and scale of the underlying crime: a small-scale drug dealer may simply spend cash, while a large corruption scheme may use a network of companies, trusts and professional advisers in several countries.

Anonymous companies are a recurring feature of large schemes. In a field experiment, Findley et al. (2014) sent requests to thousands of company formation agents around the world asking to set up shell companies, with some requests designed to suggest a high risk of corruption or terrorism. Many agents were willing to form companies without obtaining the identity documents required by international standards, and agents in some countries with strict reputations performed worse than those in jurisdictions commonly described as tax havens.

Common methods investigators look for

Investigators learn to recognise recurring methods, often called typologies, which international bodies and financial intelligence units publish so that firms know what to look for (FATF, 2012/2023). Several appear again and again.

Structuring breaks large sums of cash into smaller deposits to stay below reporting thresholds. A pattern of deposits just under the threshold, made at different branches or on consecutive days, is a classic indicator.

Money mules are people who allow their bank accounts to be used to receive and pass on criminal funds, sometimes knowingly and sometimes after being deceived by fake job offers. Accounts that suddenly receive payments from many unrelated sources and forward them quickly are a common sign.

Cash-intensive businesses, such as restaurants, car washes and retail shops, can be used to mix criminal cash with genuine takings, so that the combined total appears to be business income. Investigators compare reported takings with what the business could plausibly generate.

Trade-based laundering moves value across borders by misstating the price, quantity or quality of goods in international trade. An importer that pays far more than market value for goods transfers the excess to the exporter under cover of a commercial transaction.

Real estate allows large sums to be invested in a single transaction, often through companies or trusts that hide the true owner. Purchases in cash or through layers of companies, at prices that do not make commercial sense, call for closer inquiry.

Virtual assets, including cryptocurrencies, can be moved quickly across borders. Their public transaction records allow funds to be traced in ways that cash cannot, but services that mix or obscure transactions, and exchanges with weak customer checks, create opportunities for laundering. International standards now apply anti-money laundering duties to virtual asset service providers.

The scale of the problem

Estimates of the amount of money laundered are uncertain. A figure of 2 to 5 per cent of global gross domestic product, first offered by the head of the International Monetary Fund in 1998 (Camdessus, 1998), is still widely quoted. A later study by the United Nations Office on Drugs and Crime (UNODC, 2011) estimated that criminal proceeds amounted to about 3.6 per cent of global output and that funds available for laundering were about 2.7 per cent. Researchers have criticised such figures as resting on weak data and questionable assumptions (Reuter & Truman, 2004; Unger, 2007). What is clear is that the sums involved are large, and that only a small fraction is ever detected and confiscated.

The legal framework

International standards

The Financial Action Task Force (FATF), an intergovernmental body established in 1989, sets the international standards for combating money laundering and terrorist financing. Its Recommendations require countries to criminalise money laundering, to require financial institutions and certain other businesses to identify their customers and report suspicious transactions, to establish a financial intelligence unit to receive and analyse those reports, and to be able to confiscate criminal proceeds (Financial Action Task Force [FATF], 2012/2023). Countries are assessed against the standards in peer reviews, and those with serious weaknesses can be publicly listed, which raises the cost of doing business with them. Sharman (2011) describes how this combination of standards, assessment and listing spread anti-money laundering rules to almost every country, including many with little domestic reason to adopt them.

National laws

National laws translate the standards into duties. In the United States, the Bank Secrecy Act (1970) requires financial institutions to keep records, to report large cash transactions and to file suspicious activity reports, and later rules require them to identify the beneficial owners of companies that open accounts (Financial Crimes Enforcement Network [FinCEN], 2016). In the United Kingdom, the Proceeds of Crime Act 2002 creates the main money laundering offences and the duty to report knowledge or suspicion of laundering, and the Money Laundering, Terrorist Financing and

Transfer of Funds (Information on the Payer) Regulations 2017 set out the detailed requirements for customer due diligence and internal controls. In the European Union, the rules derive from a series of directives, including the Fourth Anti-Money Laundering Directive (Directive (EU) 2015/849, 2015), which strengthened the risk-based approach and the identification of beneficial owners. In Canada, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (2000) imposes similar duties and established the national financial intelligence unit.

The risk-based approach

Modern rules require firms to take a risk-based approach: to assess the money laundering risks posed by their customers, products, delivery channels and geographic exposure, and to apply more scrutiny where risks are higher. This replaced an earlier approach based more heavily on fixed rules, such as reporting every cash transaction above a threshold. Unger and van Waarden (2009) compare the two approaches and note that a risk-based system relies heavily on the judgment of private firms, which may lead to large differences in practice and to defensive over-reporting.

Detection within firms

Know your customer

The foundation of anti-money laundering work is customer due diligence. Firms must identify their customers, verify their identity, understand the nature and purpose of the relationship and, for companies and trusts, identify the individuals who ultimately own or control them. Enhanced due diligence applies to higher-risk customers, including politically exposed persons, who hold or have held prominent public functions and therefore present a higher risk of corruption. The information gathered at the start of a relationship provides the baseline against which later activity is judged: a transaction is suspicious only in relation to what the firm knows about the customer.

Transaction monitoring

Banks and payment firms use automated systems to monitor transactions. Rule-based systems generate alerts when activity matches predefined patterns, such as cash deposits just below reporting thresholds, rapid movement of funds in and out of an account, or payments to high-risk jurisdictions. Increasingly, firms also use statistical and machine-learning models that learn typical behaviour for a customer or peer group and flag deviations (Chen et al., 2018).

Monitoring systems generate very large numbers of alerts, and the great majority turn out to have legitimate explanations. False positive rates are high because the systems are calibrated to miss as little as possible, and because regulators penalise firms more heavily for missing suspicious activity than for reviewing innocent activity. Each alert must nevertheless be reviewed by an analyst, which makes alert handling one of the largest costs of compliance.

Investigating an alert

Within a firm, an alert or an internal referral from staff starts an investigation, usually conducted by a financial crime team. The investigator reviews the customer's profile and history, the transactions in question and any related accounts, and searches internal and external sources for adverse information. The central question is whether the activity is consistent with what the firm knows about the customer and their legitimate business. If it is not, and no satisfactory explanation can be found, the investigator considers whether there are grounds for suspicion.

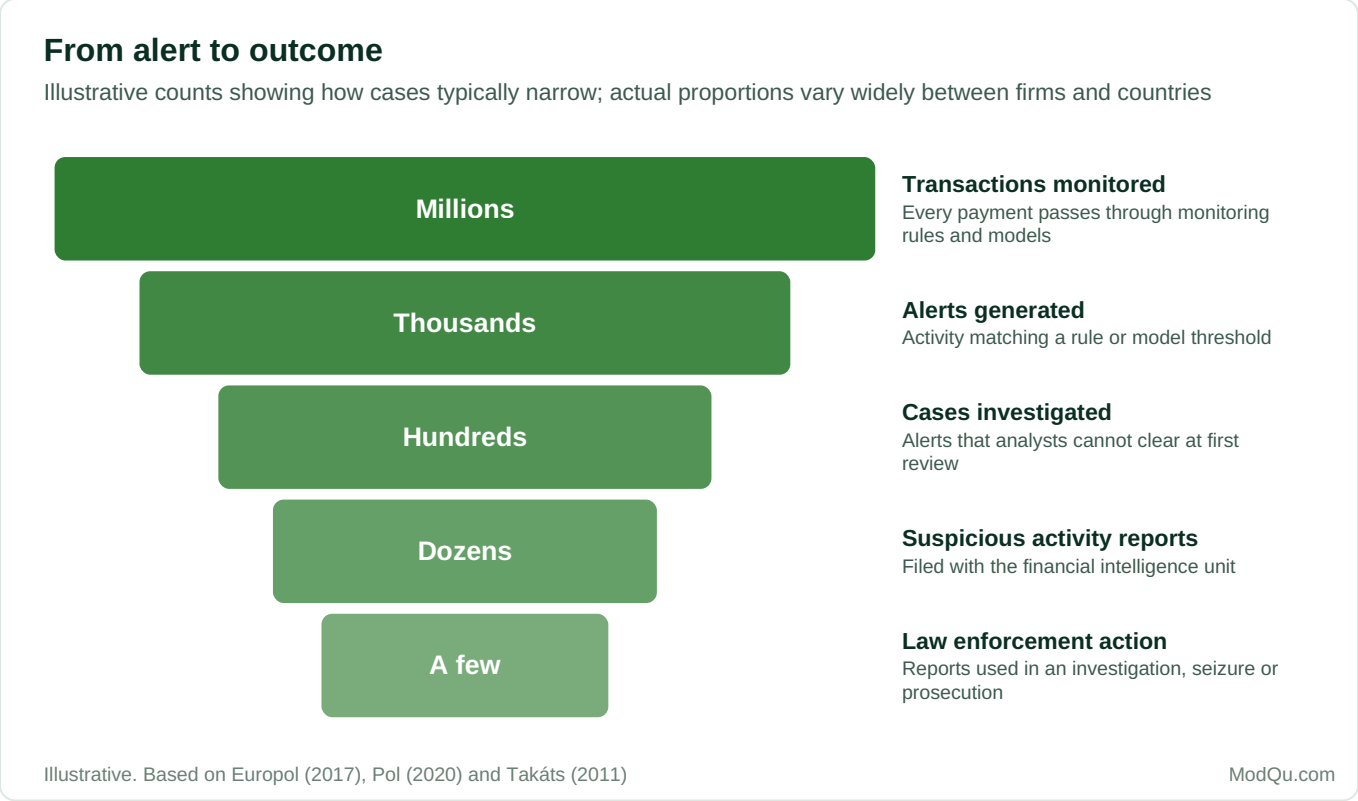


Figure 2. An illustrative view of attrition in the anti-money laundering system. Most alerts are cleared as legitimate, and only a small share of reports leads directly to law enforcement action. Diagram by ModQu.

A careful investigation records what was reviewed, what was found, what explanations were considered and why the conclusion was reached. Where the firm decides not to report, the record shows why the activity was judged not to be suspicious. Where it decides to report, the report should explain clearly what is suspicious and why, so that the financial intelligence unit can act on it.

The investigator must also avoid "tipping off". In the United Kingdom and many other jurisdictions, it is an offence to disclose to the customer, or anyone else, that a suspicious activity report has been made or that an investigation is under way, if doing so is likely to prejudice an investigation (Proceeds of Crime Act 2002). This shapes how firms handle customer contact: they may need to ask questions about the source of funds without revealing why.

What suspicion means

The threshold for reporting is suspicion, which is lower than belief or proof. A reporting employee does not need to know what crime produced the funds, or to be sure that a crime occurred at all; it is enough that the facts give rise to a suspicion that is more than fanciful. Because failure to report can be a criminal offence, and because firms face regulatory penalties for weak controls, there is a strong incentive to report whenever there is doubt. Takáts (2011) modelled this incentive and showed how heavy penalties for under-reporting can lead to "crying wolf": firms file so many low-quality reports that the information value of each report falls, and the financial intelligence unit struggles to find the reports that matter.

A short example

The following hypothetical case shows how an investigation inside a bank might proceed. A monitoring rule flags a small import company whose account has received many incoming payments from individuals in several countries over three months, each forwarded within a day to a company in another jurisdiction. The customer file describes the business as a supplier of kitchen equipment with modest turnover.

The analyst reviews the account history and finds that the pattern began suddenly and that the incoming payments bear no relation to the company's declared trade. Searches of public registries show that the receiving company was formed recently and shares a director with two other companies that have appeared in adverse media reports about investment fraud. The bank asks the customer, without revealing any suspicion, for invoices supporting a sample of the payments. The documents provided describe sales of equipment at prices far above market levels, and the shipping details cannot be matched to any recorded shipment.

The investigator concludes that the account appears to be receiving funds from victims of an investment fraud and passing them on, files a suspicious activity report setting out the facts and the reasons for suspicion, and recommends that the bank consider ending the relationship in a way that does not tip off the customer. The case file records each step, the explanations considered and why they were rejected.

After the report

Suspicious activity reports go to the national financial intelligence unit, which analyses them, combines them with other information and passes intelligence to law enforcement and other agencies. A report may contribute to an ongoing investigation, prompt a new one, support the freezing or seizure of assets, or simply be stored for future reference. The firm usually hears little about what happens next.

In many countries, only a small share of reports is used directly. A review by Europol (2017) of financial intelligence in European Union member states found that only about 10 per cent of suspicious transaction reports were further investigated after collection, and identified obstacles including differences in reporting formats, limited analytical capacity and poor feedback to reporting firms. This does not mean that the other reports have no value, since they may later help to identify networks or corroborate other evidence, but it shows how much information is collected relative to how much is used.

Failures and enforcement

High-profile failures show what happens when the system does not work. In 2012, HSBC agreed to forfeit more than 1.2 billion dollars and entered into a deferred prosecution agreement with the United States Department of Justice after admitting that weak controls had allowed hundreds of millions of dollars from Mexican drug trafficking to pass through its accounts, along with sanctions violations (U.S. Department of Justice, 2012). An investigation commissioned by Danske Bank found that its Estonian branch had handled around 200 billion euros of payments through accounts of non-resident customers over several years, a large share of which was suspicious, while controls failed and warnings were not acted upon (Bruun & Hjejle, 2018). In Canada, a public inquiry in British Columbia found that money laundering had affected the casino and real estate sectors and that regulators and law enforcement had failed to respond effectively for many years (Cullen, 2022).

These cases share common features: rapid growth in high-risk business, monitoring systems that were poorly calibrated or not used, alerts that were not investigated, warnings from staff that were ignored, and senior management that did not treat the risks seriously. For investigators, they show that the most important evidence of a laundering problem is often already inside the institution.

Does the system work?

Anti-money laundering rules impose large costs on businesses and customers, and researchers have questioned whether the benefits justify them. Pol (2020) argued that the policy has very low measured effectiveness, with the amount of criminal proceeds confiscated a tiny fraction of estimated laundering, while compliance costs are many times higher. Levi et al. (2018) argued that evaluation is hampered by a lack of good data on the scale of laundering, on the use of reports and on outcomes, and that the international assessment process has focused more on whether rules exist than on whether they work. Halliday et al. (2014) reached a similar conclusion about the international assessment system.

Other researchers point to benefits that are harder to measure: deterrence, the intelligence value of reports in investigations of serious crime, and the effect of due diligence in making it harder for criminals to use the financial system at all. The honest conclusion is that the effectiveness of the system is uncertain, and that better data on what happens to reports and alerts would allow it to be improved.

Lessons for investigators

Whether working in a bank, a regulator or a law enforcement agency, investigators of money laundering share some common practices:

1. **Know the baseline.** Suspicion depends on what is normal for the customer. Good customer information is the foundation of good investigation.
2. **Follow the money and the people.** Trace funds through accounts and companies, and identify the individuals who own and control them.
3. **Consider legitimate explanations.** Most unusual activity is innocent. Investigations should test explanations rather than assume guilt.

4. **Write clear reports.** A short, specific explanation of what is suspicious and why is far more useful to a financial intelligence unit than a long list of transactions.
5. **Look for networks.** Laundering rarely involves one account. Linking related customers, counterparties and companies often reveals the scheme.
6. **Escalate warning signs.** Many failures involved warnings that were raised internally and not acted on.

Conclusion

Anti-money laundering investigation is one of the largest investigative activities in the world, carried out mainly by private firms acting under legal duties. It combines customer knowledge, data analysis and judgment to identify activity that does not fit, and passes that information to authorities who can act on it. The system has real weaknesses: high false positive rates, large volumes of reports that are never used, and uncertain evidence of overall effectiveness. Its strengths lie in the investigative habits it requires: knowing who one is dealing with, testing activity against what is known, and recording reasoning clearly. Those habits, applied carefully, make it harder for criminals to enjoy the proceeds of crime.

References

Bank Secrecy Act, 31 U.S.C. § 5311 et seq. (1970).

Bruun & Hjejle. (2018). *Report on the non-resident portfolio at Danske Bank's Estonian branch*.

Camdessus, M. (1998, February 10). *Money laundering: The importance of international countermeasures* [Speech]. International Monetary Fund.

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems, 57*(2), 245–285. https://doi.org/10.1007/s10115-017-1144-z

Cullen, A. (2022). *Commission of Inquiry into Money Laundering in British Columbia: Final report*.

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. (2015). *Official Journal of the European Union, L 141*, 73–117.

Europol. (2017). *From suspicion to action: Converting financial intelligence into greater operational impact.* Publications Office of the European Union.

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

Financial Crimes Enforcement Network. (2016). Customer due diligence requirements for financial institutions. *Federal Register, 81*(91), 29398–29458.

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

Halliday, T., Levi, M., & Reuter, P. (2014). *Global surveillance of dirty money: Assessing assessments of regimes to control money-laundering and combat the financing of terrorism*. Center on Law and Globalization.

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

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

Madinger, J. (2011). *Money laundering: A guide for criminal investigators* (3rd ed.). CRC Press.

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692 (UK).

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 Act 2002, c. 29 (UK).

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.

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. (2007). *The scale and impacts of money laundering*. Edward Elgar.

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. https://doi.org/10.2202/1555-5879.1422

United Nations Office on Drugs and Crime. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*.

U.S. Department of Justice. (2012, December 11). *HSBC Holdings plc and HSBC Bank USA N.A. admit to anti-money laundering and sanctions violations, forfeit $1.256 billion in deferred prosecution agreement* [Press release].