NORTH DATA

Risk Signals

Money Laundering

Cross-Border Risk Signals

The Identity Split

- Laundering networks might register a person with slight variations across different registries to avoid automated detection.
- E.g., a Russian or Middle Eastern UBO might be registered as Vladimir PETROV (with a Cyprus passport) in the German registry, but as Wladimir PETROW (with a UK address) in the British registry.
- North Data surfaces related name variants through fuzzy matching, but researchers still need to evaluate whether a discrepancy is a harmless variance or a deliberate identity split.

The “Mirror Company” Typology

- A cluster of companies with nearly identical names across different countries, controlled by the same UBO.
- It can create administrative noise during manual cross-border lookups, as the identical names make it highly challenging for investigators to quickly pinpoint which exact jurisdiction holds the actual assets or liabilities.

The Baltic/Fintech Crypto-Gateway

- Some laundering schemes documented have used Eastern European or Baltic corporate vehicles as gateways to crypto or offshore banking.
- A company network includes Estonian or Lithuanian entities, especially where they appear as payment, fintech, IT, licensing, or service companies with limited visible staff or assets. This can be a risk signal when the Baltic entity receives significant revenue or related-party flows that appear disproportionate to its visible operations, or when it sits between higher-risk foreign counterparties and EU operating companies.

The VAT Carousel Fraud (MTIC – Missing Trader Intra-Community)

- VAT carousel fraud, or MTIC fraud, is one of Europe's most damaging organised financial crime schemes. It exploits VAT-free intra-EU trade: goods are bought cross-border without VAT, sold domestically with VAT, and the trader disappears without remitting the VAT. In carousel schemes, chains of companies and repeated cross-border transactions are used to generate fraudulent VAT refund claims, with proceeds often laundered or linked to wider organised crime.
- North Data Financials: A company's profile may show explosive, almost exponential growth in turnover within one to two years, while tangible assets (such as warehouses or equipment) and the number of employees remain close to zero.
- North Data Network: A trading company that routes the same goods through a tight circle of three to four related logistics or wholesale firms in different EU countries, issuing repeated invoices within that closed group, matches the circular transaction chains described in VAT carousel fraud typologies.

Financial Risk Signals

High "Other Operating Expenses"

- Dominance of vague cross-border service fees (for consulting, marketing,

IP rights, etc.) in the “Other operating expenses” line can signal funds being shifted out of the entity via ghost services and fictitious invoicing.

Unrealistically High or Low Financial Figures

- Operational Disproportion: Massive discrepancies between a company's reported turnover and its physical infrastructure, tangible asset base, or human resources.
- Abnormal Revenue Spikes: Extreme, sudden growth in revenue or inexplicably high profit margins that deviate completely from historical performance and industry benchmarks.
- Balance sheet anomalies: Significant, unexplained inflation of specific line items (for example “other operating income” or large advance payments) that does not reconcile with physical inventory or underlying business activity.

Persistent, Uncommercial Loss-Making

- A company has been operating at a massive loss for five to ten consecutive years, resulting in deeply negative equity, yet it never files for insolvency and continues to stay active.
- Sustained multi-year losses with deeply negative equity and no insolvency filing warrant scrutiny, especially where there is no visible external commercial financing or strategic rationale.
- One possible explanation is that the company is being used as an expense-generation vehicle – to absorb illicit funds through operational costs or to offset taxes elsewhere in a related group. But: Other commercial reasons should also be considered.

Cash-Heavy Balance Sheets in Non-Cash Industries

- High amounts of “Cash on hand” or liquid bank assets on the balance sheet of companies operating in traditionally digital B2B sectors (e.g., software development, international commodity brokering).
- When combined with other risk signals, this can be consistent with the

company being used as a “cash-in” or “cash-out” node. But: It can also reflect legitimate treasury or fundraising activity.

Audit & Transparency Risk Signals

Drastic Changes in Fiscal Year

- Abruptly changing a company's financial year-end (e.g. from December to May) can serve as an audit evasion tactic designed to artificially delay mandatory disclosure deadlines and disrupt the financial paper trail.
- This tactic can be used to delay the legal deadline for filing audited financial statements, giving launderers more time to move funds and dissolve the company before anyone takes a closer look.

The “Micro-Entity” Shield

- Criminal networks may fragment activity across several small companies to keep each entity below reporting, audit, or disclosure thresholds. In the UK and Germany, micro-entity regimes allow very small companies to file highly abbreviated public accounts, often with little or no public profit-and-loss detail and no mandatory audit.
- This can make it difficult for outside investigators to assess true turnover, margins, related-party flows, or the commercial rationale for transactions, especially when several connected micro-entities appear to share directors, addresses, counterparties, or business activity.

Qualified or Adverse Audit Opinions

- If the company is large enough to require an audit, click through to the full filing. Look for phrases like “We were unable to obtain sufficient appropriate audit evidence regarding the valuation of foreign trade receivables...”
- This is a significant red flag: the auditor could not verify key international

trade receivables, which warrants further investigation into the underlying transactions.

Offshore Fund / Proxy Ownership Risk

- The ownership chain leads to a complex investment fund, nominee manager, trustee, or corporate service provider in an offshore or low-transparency jurisdiction. Public data may show the chain stopping at this intermediary layer, making it difficult to identify the natural person who ultimately controls or benefits from the company.
- This is a red flag when combined with additional indicators, such as links to PEPs, sanctioned individuals, state-connected investors, nominee directors, opaque fund structures, unusual financing, or jurisdictions with restricted beneficial-ownership access.

Network Risk Signals

Complex corporate networks and opaque ownership structures

- Multi-Tiered Graph Analysis: Use the network view to trace extended, layered ownership chains that span multiple international borders and may make the ultimate beneficial owner harder to identify.
- Unnatural Node Intersections: Identifying overlapping directors, shared virtual service addresses, or common shell parent entities that link seemingly independent international corporations.
- Structural Timeline Disruptions: Monitoring abrupt historical shifts in corporate parentage, shareholder allocations, or country of origin within the network, particularly right before major financial transactions.

The “Corporate Hijack” (Sudden Parent-Company Swap)

- An established, reputable European company with decades of clean history is suddenly bought out by a freshly incorporated shell company from another

jurisdiction (e.g. a 20-year-old German GmbH suddenly owned by a 2-month-old UK Ltd).
- This pattern warrants closer scrutiny. Possible explanations range from legitimate SPV-led acquisitions to misuse of an established company's reputation or the injection of illicit funds into a clean asset.

Asymmetric Jurisdiction Stacking

- A visible holding company is incorporated in a high-reputation jurisdiction, while subsidiaries, sister companies, shareholders, or service providers are concentrated in jurisdictions with limited public beneficial-ownership access, strong nominee-service industries, or historically higher secrecy risks.
- This can create a legitimacy wrapper around an otherwise opaque structure. The risk is higher where the offshore or low-transparency entities have no obvious operational role, share directors or registered agents, hold key assets or IP, receive group payments, or interrupt the public ownership trail.

Unusually frequent changes of managing directors or shareholders

- Disruption of Operational Continuity: Systematic cycling of legal representatives or equity owners every few months can fragment the historical paper trail and make it harder for compliance systems to establish a baseline.
- Possible Nominee Rotation: Rapid swaps of individual directors may shorten the exposure time of any single proxy director and limit the scope for prolonged regulatory scrutiny or deep background checks.

Recurring liquidations and newly formed companies by the same individuals

- The Phoenix Typology: A repeating pattern where an individual repeatedly incorporates a new company immediately after their previous, identically structured entity is forced into compulsory liquidation or strike-off.
- Trace Eradication & Reset: Using short-lived companies to push through high-

risk transactions, shut them down before audits or investigations begin, and restart the same activity under a fresh legal entity.

Address Risk Signals

Operational & Geographic Mismatch

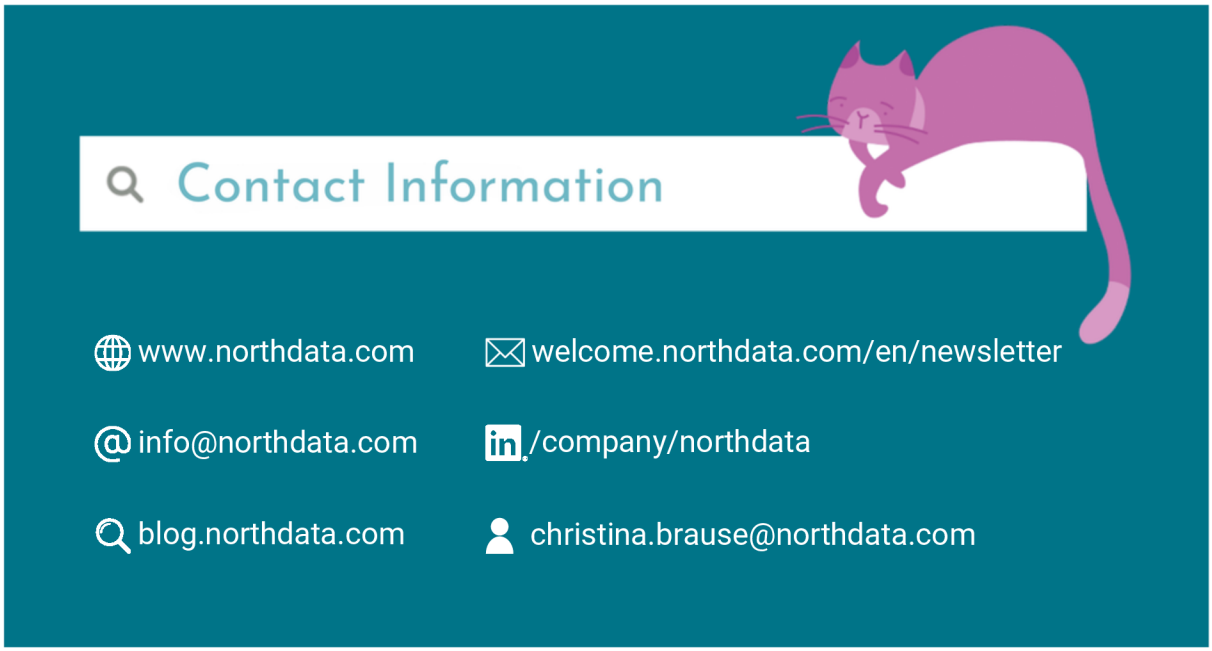
- A company's physical address must logically align with its reported financial and business activity.
- The "Living Room" Multinational: The company's North Data profile shows €20 million in revenue from importing heavy industrial machinery or wholesale solar panels from China. However, when you drop the registered address into Google Maps Satellite/Street View, it is a suburban semi- detached house, a tiny apartment in a residential block, or a rural farm.
- The Logistics Ghost: If a company claims to be a high-volume logistics, shipping, or warehousing business, its address must map to an industrial park, a port, or a warehouse facility. A logistics company operating out of a 4th-floor downtown office with no physical loading zones is a Trade-Based Money Laundering (TBML) risk sign.

Mass-Registration Hubs (The "Mailbox Factory")

- Shell-company operators often avoid physical offices and instead use virtual addresses provided by Corporate Service Providers. But: Many legitimate small businesses also use these services, so the address alone is not conclusive.
- Clicking on a company's registered office address in North Data reveals that dozens, hundreds, or even thousands of other active companies are registered at that exact same suite, apartment, or mailbox number.
- Advanced OSINT Pivot: Analyse the other companies at that address
  - Do they share the same directors?
  - Do they operate in completely unrelated industries but file financial statements on the exact same day?

Strategic Address Relocation (The "Jurisdiction Hop")

- High-Frequency Relocation: Successive changes to the registered office every six to twelve months (particularly across different cities or judicial districts) visible as a dense cluster on the North Data history timeline.
- Possible Audit Evasion via File Transfers: Moving to a new municipality just before an audit can trigger a bureaucratic transfer of the tax file.

The “Care Of” (c/o) and PO Box Shield

- Legitimate operational businesses want their mail, clients, and suppliers to reach them directly. Laundering entities want to create distance.
- The address in the registry is heavily padded with “c/o” (Care Of), “Suite X”, “Floor Y”, or “PO Box” designations, without any actual physical presence.