

Case



Agenda

1. How we start our cases
2. Initial Findings and Focus
3. Investigation steps
4. Results
5. Problems/challenges
6. Use of CS:GO Skins in Money Laundering

If we there's time and interest



How we start out cases

5 steps



Background & Reporting

Reports typically submitted by financial institutions, attorneys, or auditors.

Triggered by suspicions of tax fraud and/or money laundering.



NSK's Role

National Unit for Special Crime (NSK) consolidates multiple reports.

Combined into a single intelligence report per legal entity.

Report is forwarded to our unit as a formal case file.



Case Evaluation Process

Machine learning-based scoring model used by the Danish Tax Agency.

Assesses likelihood of fraud based on report characteristics.

High-risk cases are prioritized on an internal selection list.



Case Assignment & Confidentiality

Caseworkers draw cases from the prioritized list.

Legal constraints prohibit disclosure of money laundering suspicions to subjects.

Initial phase involves discreet information gathering on the legal entity.



Initiating the Investigation

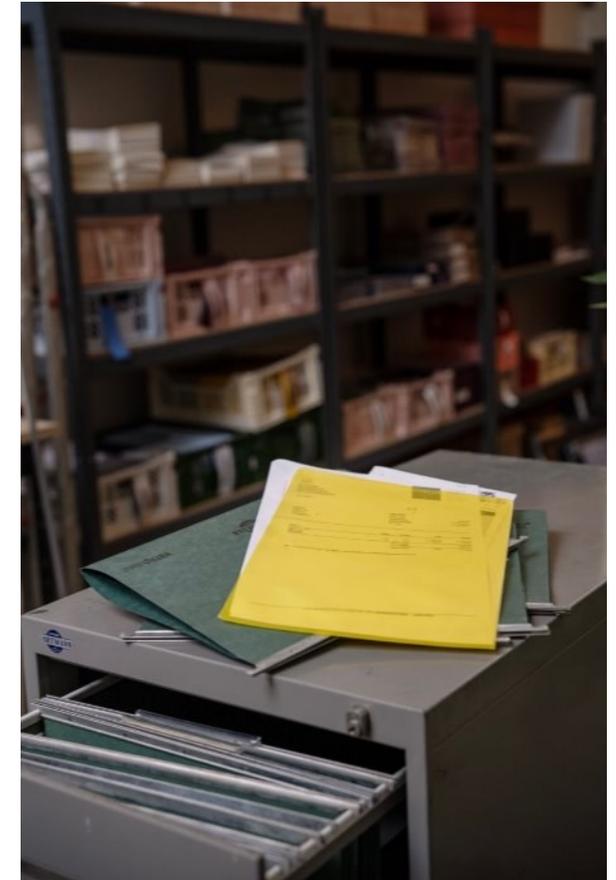
Collected data forms the basis for formally opening a case.

Full investigation process begins thereafter.

Initial Findings and focus

The case stems from a network of fraudulent invoicing entities

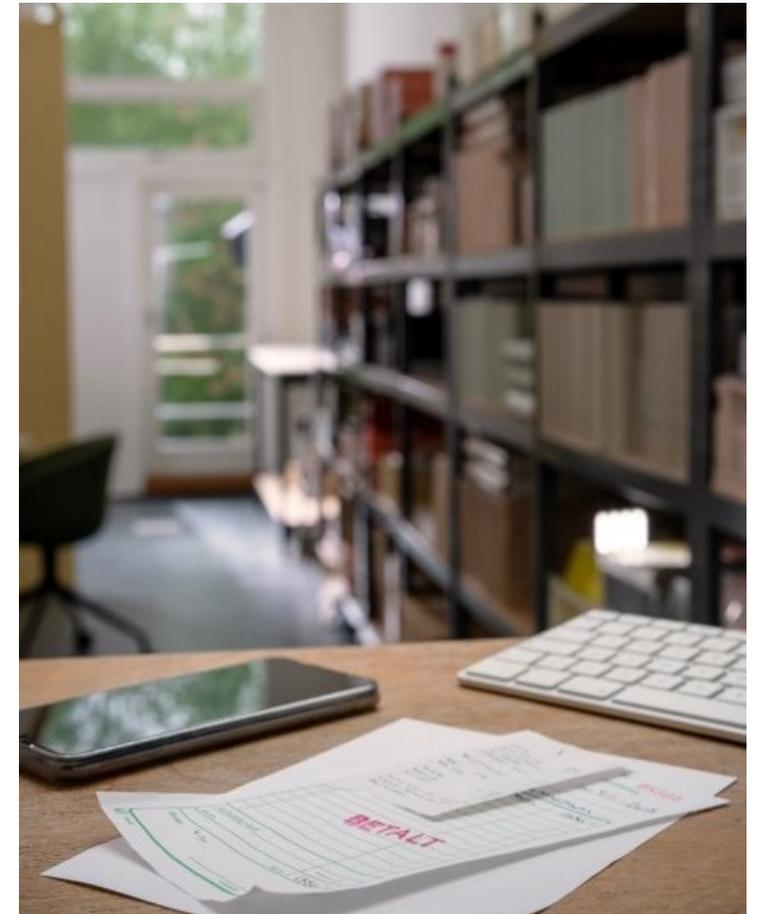
- Subcontractor to an invoice factory identified within a broader criminal network.
- Company purchases “external labor” despite being registered solely as a property management business.
- Part of a corporate group with a single owner and no registered employees.
- Investigation initiated into:
 - The company itself
 - Affiliated companies
 - The principal shareholder and owner



Investigation steps

What options do we have in terms of investigation?

- Investigations initiated on three companies:
 - The parent company
 - Two subsidiaries
 - As well as the principal shareholder
- The primary actor is one of the subsidiaries, which invoices onward for fictitious labor purchases.
- The company temporarily uses the parent company's bank account.
 - Discovered through invoices issued by the subsidiary
- Funds transferred out of the company typically leave the country.
 - Either through transfers to foreign bank accounts or to cryptocurrency exchanges
- Ongoing investigation includes:
 - Documentation submitted by the company itself
 - Material obtained through audits of related business partners
 - Tracing the destination of foreign transfers



Results

Findings from this case and the subsequent actions it triggered

- Tax and VAT adjustments applied to both the parent company and the subsidiary.
- The principal shareholder is taxed on dividends for the foreign transfers.
 - Based on the suspicion that he receives funds back from the fictitious purchases.
 - After a small "fee" is deducted by intermediaries/facilitators.
- Additional cases initiated against individuals receiving cryptocurrency from the company.
 - These individuals previously had links to known fictitious companies.



Problems/challenges

Obstacles faced throughout the course of the investigation

- Following the flow of funds – these companies/individuals know which channels to exploit.
- Use of Counter-Strike skins – funds or cryptocurrencies that ultimately end up on platforms such as **CSGOEmpire** or **Rollbit**.



Use of CS:GO Skins in Money Laundering

How does it tie in with the use of cryptocurrencies



The methods are attractive due to the pseudonymity of skin transactions and the global, unregulated nature of many related platforms.

Thank you!

Any questions?