



Managementsummary

Research into the Nature and Extent of Damage Caused by Online Fraud Against Businesses

Authors

Tessel Blom

Menno Driesse

Luuk Brouwers

Iris van Vugt

Managementsummary

Research into the Nature and Extent of Damage Caused by Online Fraud Against Businesses

Authors

Tessel Blom

Menno Driesse

Luuk Brouwers

Iris van Vugt

Assignment given by

Wetenschappelijk Onderzoek- en Datacentrum

Publicationnumber

2024.184-11032

Cite as

Blom, T., Driesse, M., Brouwers, L., & van Vugt, I., (2026). *Onderzoek naar de aard en omvang van schade door online fraude bij bedrijven*. WODC: Den Haag.

Date

15 April 2026

Cover photo

Adrien via Unsplash

Managementsummary

Background to the study

In recent years, online fraud has become an increasingly important and topical issue for the Dutch business community. Technological developments, including the further digitalisation of business processes and communications, have provided fraudsters with more opportunities to deceive companies online. At the same time, **there is a lack of up-to-date and reliable knowledge about the nature and extent of online fraud affecting businesses, as well as the direct financial damage incurred as a result.**

Existing literature and studies mainly offer background information or focus on private individuals, cybercrime in a broad sense, or specific types of fraud, but do not provide a coherent picture of online fraud affecting businesses in the Netherlands. However, such knowledge is essential for developing targeted policy measures and for better supporting companies that fall victim to online fraud.

Objectives and research questions

The objective of this study was to gain insight into the nature and extent of damage caused by online fraud affecting businesses in the Netherlands. This involved not only examining the outcomes themselves, but also assessing the extent to which data sources are available and which methods can be used to estimate online fraud affecting businesses on the basis of these sources. Subsequently, an attempt was made to actually map this out in practice. Explicit attention was also paid to the limitations and possibilities of this exercise, the assumptions made, uncertainties involved, and opportunities for improving future estimates.

Research approach

The study comprised a preliminary phase and a main research phase. The preliminary study involved a literature review and interviews with stakeholders and experts in the field of online fraud. Among other things, the preliminary study resulted in a taxonomy of online fraud affecting businesses, which can also be used in the future to classify and register types of fraud in a consistent manner (see Figure 1).

What is the gain for the offender?	What is the modus operandi?	Specification of the modus operandi
1. Payment fraud (<i>proceeds consist of a payment</i>)	1.1 Failure to deliver promised goods or services	1.1.a Purchase fraud
		1.1.b Acquisition fraud
		1.1.c Investment fraud
		1.1.d Recovery fraud
	1.2 Assuming a false identity	1.2.a CEO fraud
		1.2.b Helpdesk fraud
		1.2.c Identity fraud (employee)
	1.3 Manipulation of information	1.3.a Domain name fraud
		1.3.b Invoice fraud
1.3.c Payment request fraud		
2. Product or service fraud (<i>proceeds consists of products or services</i>)	2.1 Failure to make payment	2.1.a Sales fraud

Figure 1: Taxonomy of online fraud to companies.

In addition, an **inventory was made of the available data sources**, mapping both the possibilities and limitations of each source, as well as constraints in current implementation practice. For the study, four sources were identified that can currently provide insight into the nature and extent of online fraud affecting businesses. However, **these data sources have clear limitations that have a major impact on the reliability of estimates**. These data sources are:

1. *Police records*. Police records can be an important source of information on online fraud, as they constitute a large national reporting point for victims. However, **current police registration practices are insufficient for mapping victimisation of online fraud affecting businesses**. Reports and formal complaints are often incomplete, and it is frequently unclear whether the victim is a business or a private individual. In addition, no consistent definitions are used for different types of fraud, and information on financial losses is often missing.
2. *Fraudehelpdesk Zakelijk*. Fraudehelpdesk Zakelijk is an online reporting point for businesses in cases of fraud. **Data from Fraudehelpdesk Zakelijk contain extensive and consistent information on fraud incidents and types of fraud**. However, no information is collected on the characteristics of the reporting

businesses, meaning that this data source cannot provide further insight into the types of businesses that become victims.

3. *Survey among an entrepreneur panel.* We conducted a survey among a representative panel of 600 entrepreneurs from Ipsos I&O. In this survey, we successfully applied the developed taxonomy for online fraud. Using extrapolation, we subsequently produced an estimate of the extent of online fraud affecting businesses. However, **victimisation surveys often involve victim bias**, which may lead to overestimation, and **the number of victims in the sample was too small** to allow for more in-depth insights into the nature of online fraud and the different types of fraud affecting businesses.
4. *Survey among the business population.* Through VNO-NCW, MKB-Nederland and affiliated trade associations, we distributed a survey broadly among entrepreneurs. Once again, **we found that entrepreneurs are generally reluctant to complete surveys**. Despite multiple reminders, response rates remained very low, meaning that this data source could not be used further in this study.

Finally, a research approach was established in which we attempt to estimate the extent of online fraud by extrapolating the survey results and by applying the multiplier method. In the multiplier method, we use the reporting rates derived from the survey to estimate the dark figure underlying police records and data from Fraudehelpdesk Zakelijk. This makes it possible to estimate the total extent of online fraud affecting businesses. Where possible, these three estimates are subsequently triangulated to arrive at a more robust overall estimate.

The nature and extent of online fraud affecting businesses

The method described above results in estimates of the extent of online fraud that differ substantially across data sources. Estimates based on administrative data (Fraudehelpdesk Zakelijk and police records), combined with the reporting rates observed in the survey (multiplier method), are many times lower than the estimate based on extrapolation of the survey results, and the 95% confidence intervals are also very wide (Table 1). As a result, we are unable to produce a reliable estimate of the extent of online fraud affecting businesses.

Table 1. Overview of estimates of victims and fraud incidents across different data sources. Police records do not contain (reliable) information on the financial damage caused by fraud incidents..

Data source	Estimate (95% confidence interval)
Survey among entrepreneur panel	52.849 - 124.573 victims 80.532 - 189.825 incidents with direct financial loss
Fraudehelpdesk Zakelijk	1.680 - 11.667 incidents with direct financial loss
Police records	4.061 - 9.748 incidents

The estimated extent of direct financial damage caused by online fraud also differs substantially between the results derived from the survey (extrapolation) and those based on reports to Fraudehelpdesk Zakelijk (multiplier method based on the reporting rate from the survey). **The direct financial damage estimated on the basis of the survey ranges between €90 million and €211 million (95% confidence interval).**

Estimates based on reports to Fraudehelpdesk Zakelijk are lower.

Table 2. Overview of estimates of the extent of financial damage across different data sources. Police records do not contain (reliable) information on the financial damage caused by fraud incidents.

Data source	Estimate (95% confidence interval)
Survey among entrepreneur panel	€90 million - €211 million direct financial loss
Fraudehelpdesk Zakelijk	€14 million - €95 million direct financial loss

Most recorded and reported incidents of online fraud affecting businesses involve purchase and sales fraud. Incidents of invoice fraud, CEO fraud, identity fraud and helpdesk fraud are relatively more often reported to the police, whereas acquisition fraud is more frequently reported to Fraudehelpdesk Zakelijk. Purchase and sales fraud mainly occurs via webshops, while the other types of fraud typically take place by telephone or email.

Recommendations

To improve insight into online fraud affecting businesses, it is important that **more data are collected in the future and that the available data are of higher quality.** To achieve this, we make the following recommendations:

- **Police registration practices should be structurally improved.** The police serve as an important national reporting point where victims come forward. To gain insight into this victimisation, it is essential that police records at a minimum indicate whether the reporter is a business or a private individual, and

what direct financial damage resulted from the fraud incident. Making certain fields mandatory in the registration process when recording a report or formal complaint—such as type of fraud, type of victim, and financial damage—would be an important first step.

- Estimating the dark figure requires combining multiple data sources. **It is therefore important that different organisations adopt a shared taxonomy for online fraud**, as proposed in this report. Using the same definitions and delineations enables data to be compared and aligned across sources. Given its central position in the landscape, it could be considered to assign responsibility for this to Fraudehelpdesk.¹
- To gain insight into types of victims, Fraudehelpdesk Zakelijk could **consider collecting information on reporting businesses, such as sector and company size**. With better insight into victim profiles, policy interventions for the prevention and combating of online fraud affecting businesses can be developed in a more targeted manner.
- Entrepreneurs are a notoriously difficult group to reach through surveys. It is therefore advisable **to bundle efforts and align victimisation surveys with ongoing monitoring initiatives**. A promising monitor for mapping the extent of online fraud affecting businesses is the CBS Monitor on Business Crime (*Monitor Criminaliteit Bedrijfsleven*), which is expected to be conducted in 2026.

¹ This is in line with one of the development directions formulated for the Fraudehelpdesk in the organisation's 2023 evaluation (Pro Facto, 2023).