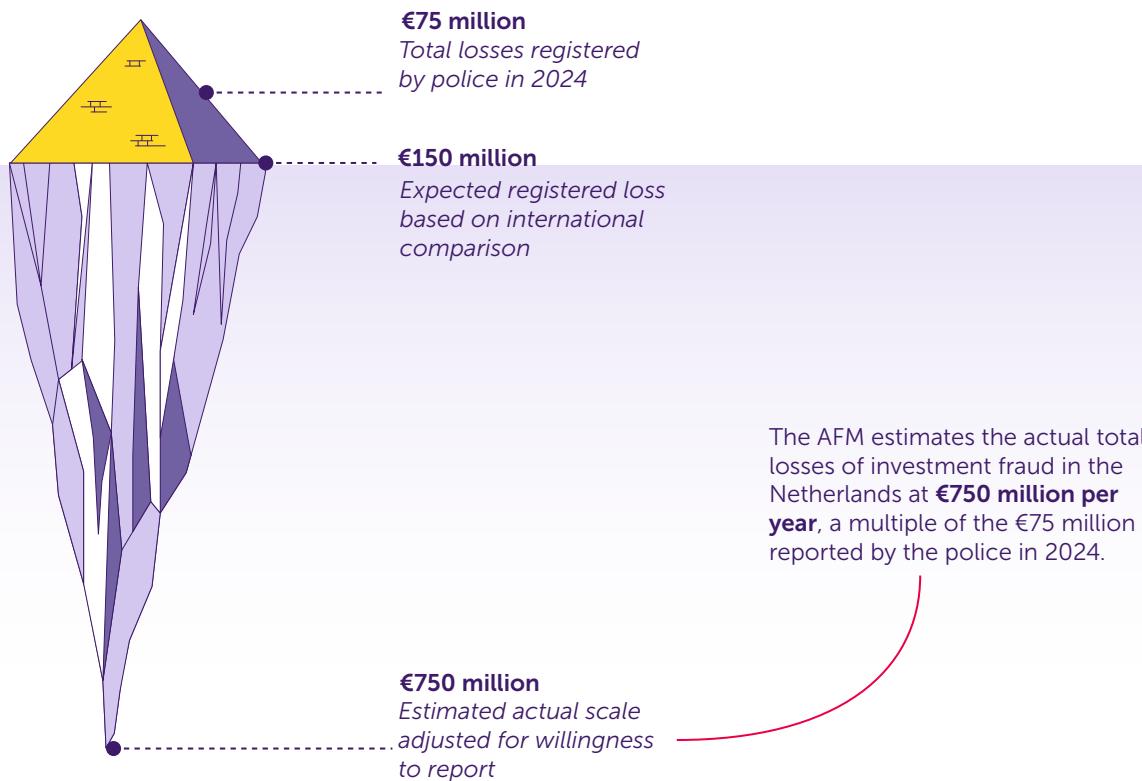


From pyramid to iceberg: the hidden scale of investment fraud in the Netherlands

In short Investment fraud is an urgent and growing threat to consumers and to confidence in financial markets. The true scale of investment fraud is structurally underestimated. Taking into account fragmented registration and victims' low willingness to report, the AFM estimates the actual losses of investment fraud in the Netherlands at €750 million annually, a multiple of the €75 million reported by police in 2024. This report provides insight into the nature, scale and response to investment fraud.

The AFM advocates for centralized and standardized registration of investment fraud, to gain better insight into its growing impact and welcomes discussion with stakeholders to strengthen the efforts to combat investment fraud.



Contents

1. Investment fraud is a growing threat	4
2. The nature of investment fraud	6
2.1 Definition	6
2.2 The consequences of investment fraud	6
2.3 The evolution of investment fraud	6
2.4 Types of investment fraud	9
2.4.1 Boiler room fraud	9
2.4.2 Ponzi fraud	9
2.4.3 Pyramid scheme	9
2.4.4 Recovery room fraud	10
2.4.5 Pump-and-dump	10
2.4.6 Fraud with complex products	10
2.5 Specific approach: relationship investment fraud	11
2.6 Perpetrators	11
2.7 Victims	11
2.8 Facilitators	12
3. The scale of investment fraud	14
3.1 The dark number of investment fraud	14
3.2 The top of the pyramid: reported investment fraud in the Netherlands	15
3.2.1 Dutch Authority for the Financial Markets	17
3.2.2 Fraud Helpdesk	18
3.2.3 Police and FIOD	18
3.2.4 FIU-the Netherlands	18
3.3 Recorded investment fraud internationally	19
3.3.1 United States	20
3.3.2 United Kingdom	20
3.3.3 France	20
3.3.4 Germany	21
3.3.5 Italy	21
3.4 A full view of the pyramid: estimation of the scale of registered damage from investment fraud in the Netherlands	21
3.5 The iceberg below the pyramid: estimation of the hidden scale of investment fraud in the Netherlands	23
4. The current approach to investment fraud in the Netherlands	24
4.1 Approach	24
4.1.1 Boiler room fraud	24
4.1.2 Ponzi fraud	25
4.1.3 Pyramid scheme	25
4.1.4 Recovery room fraud	26
4.1.5 Pump-and-dump	26
4.1.6 Fraud with complex products	26
4.2 Tackling investment fraud within financial supervision	27
4.3 Investment fraud within criminal law	27
4.4 Prevention and education	27
4.5 International approach	28

Contents

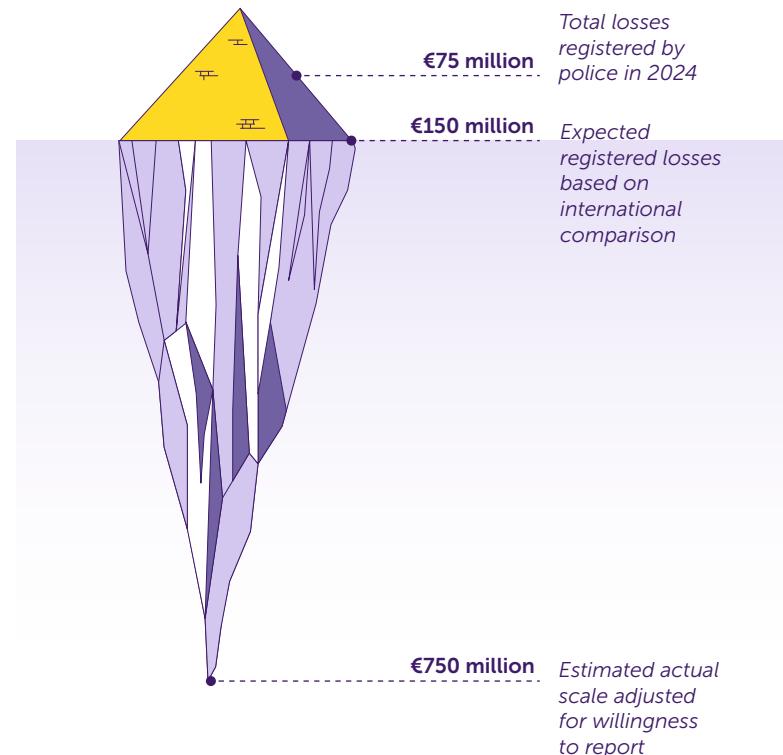
5. Appendices	29
5.1 Methodology and justification.....	29
5.1.1 Aim and approach.....	29
5.1.2 International benchmark comparison.....	29
5.1.3 Extrapolation based on amount of losses per capita	34
5.1.4 Extrapolation based on GDP	35
5.1.5 Limitations.....	36

1. Investment fraud is a growing threat

Investment fraud is an urgent and growing threat to consumers and confidence in the financial markets. Criminals mislead victims with fake or dubious investment offers, often through digital channels, with the aim of extracting money from them. The consequences of investment fraud are far-reaching: victims not only suffer major financial losses but also experience severe psychological stress. The proceeds disappear into criminal assets and strengthen illegal structures. This leads to a loss of investment capital in the real economy. In the Netherlands, investment fraud therefore causes significant financial damage. Only the top of the pyramid is visible through registered cases, but beneath the surface hides a large iceberg of losses. Moreover, there has been an upward trend in cases of investment fraud for several years. Internationally, the situation is equally alarming. Its scale and increasing professionalisation make this a form of criminal behaviour that requires an approach of equal scale.

Most of the losses remain hidden due to the lack of central and standardized registration and a low willingness to report among victims. The police reported €75 million in losses from investment fraud in 2024: this is only the top of the pyramid. International comparisons provide a full view of the pyramid: the recorded damage amounts to approximately €150 million.

The AFM estimates the actual losses from investment fraud at €750 million per year. Assuming a reporting rate of only 17%, as indicated by Statistics Netherlands (CBS) for online fraud, we also see the hidden scale of the invisible iceberg: estimated actual losses of €750 million. Factors such as growing digitalisation and the cross-border nature of investment fraud offer opportunities for fraudsters and are expected to inflate this amount further in the future – a worrying image. The lack of central registration and the low willingness to report mean that the insight into the problem is fragmented, further impeding an effective approach.



Combating investment fraud is a responsibility shared with stakeholders and a core priority¹ of the AFM. The AFM works with stakeholders, such as the police, the Fiscal Intelligence and Investigation Service (**FIOD**), the Fraud Helpdesk, the Financial Intelligence Unit-Netherlands (**FIU-Netherlands**), the Dutch Banking Association (**NVB**) and a Dutch crypto-asset service provider (**CASP**), to improve insight into the extent and different types of investment fraud. This insight is crucial for determining the appropriate approach.

The AFM invites stakeholders to take joint action to achieve structural improvements in the information position regarding investment fraud.

Improving the reporting and registration process is an important precondition for more coordinated, decisive and effective action between stakeholders. The AFM hopes this report will encourage a joint effort to combat investment fraud. In order to work together effectively, the AFM welcomes a discussion with stakeholders.

¹ [Agenda](#)

2. The nature of investment fraud

2.1 Definition

Investment fraud is nothing new; it has existed for as long as people have been looking for financial returns. Examples of investment fraud include the South Sea Bubble in the 18th century, the original Ponzi scheme in the 20th century and the large-scale scams perpetrated by Bernie Madoff. *The motive* is money. *The opportunity* lies in the investor's search for yield, which goes hand in hand with a uncritical attitude, involving an irrational belief that a particular asset (GameStop), development (dot.com) or manager (Madoff) will deliver extraordinary returns. *The method* is a form of deception that is bolstered by limited transparency about the investment or the way in which it is invested.

The AFM defines investment fraud as follows:

Investment fraud is a form of financial fraud in which investors are misled by the provision of false information, deceitful promises about returns or (non-existent) investment products, with the aim of financial gain.

2.2 The consequences of investment fraud

Investment fraud often causes serious financial losses for victims, who lose their savings, pension rights or other assets. In addition to the financial impact, it also leads to psychological damage. Victims experience feelings of shame, guilt and distrust, which lowers their willingness to report and hinders them in seeking help. This emotional burden can affect the well-being of victims and their direct environment and impact their trust in financial institutions and the financial market.

The proceeds of investment fraud do not flow into legitimate investments but are used to build up criminal assets. Perpetrators use these resources to strengthen their position within organised networks, develop new forms of fraud or finance other illegal activities. This increases the effectiveness of criminal organisations and makes enforcement and investigation more complex, especially when the money is channelled through international structures.

Victims' money is not actually invested, causing it to disappear from the legitimate financial circuit. This leads to a loss of investment capital in the real economy, which undermines consumer and investor confidence in financial markets and institutions. When fraud occurs structurally and on a large scale, it can disrupt market functioning and weaken support for investing in general.

2.3 The evolution of investment fraud

Digitalisation has not only changed the nature of investment fraud but also increased its scale, speed and complexity. Investment fraud has shifted to the online domain to a significant extent. This shift has expanded the reach of scammers: through social media, email and online advertising, they can target potential victims from anywhere in the world at low cost. Fraudsters present themselves online with professional-looking websites or use websites cloned from reputable companies to appear credible. The growing use of AI – such as deepfake videos or audio and the use of AI agents – will also drive the further digitalisation of investment fraud and the emergence of new operating methods.

Digitalisation has created new tools for investment fraud, the most important of which is the rise of trading in crypto-assets.² The promise of high returns and the technological innovation of crypto-assets attracts investors, while the complexity and limited knowledge among investors provide an information advantage for fraudsters. Crypto-assets have not only become popular 'bait' but also offer fraudsters a relatively anonymous and difficult-to-trace payment method to channel embezzled funds.

Within the chain of online investment fraud, specialisations have emerged, which are offered as crimes-as-a-service (CaaS). As a result, fraudsters no longer need to control all aspects of the fraud themselves; they can use specialised services offered as CaaS. This means that criminal networks or individual providers perform separate fraud services, such as building convincing fake websites, generating false advertisements, delivering stolen personal data or facilitating anonymous crypto payments. This development lowers the threshold for new fraudsters while also improving the efficiency and professionalisation of fraud practices.³

The internationalisation of financial markets has given investment fraud an increasingly cross-border character. Financial markets and services are becoming more international. This trend is mirrored in the rise of cross-border criminal activity. Investment fraudsters often operate from abroad without a licence or target several countries at the same time. For example, Dutch investors are regularly approached by telephone from call centres located abroad (such as Eastern Europe or Southeast Asia) or come into contact with fraudsters through international websites or social media. This development increases the need for cross-border exchange of data and coordinated supervision, as national measures have limited effectiveness in international and online investment fraud.

Online recruitment as a driver of investment fraud:

Online contact through internet platforms is a crucial driver of investment fraud. Digital channels offer fraudsters economies of scale: they can reach a large number of potential victims with minimal effort. The contact between the consumer and the online fraudster often starts through one or a combination of the following routes:

- Internet search engines and fraudulent advertising:**

Consumers who search online for ways to invest their money are tricked into clicking on fraudulent offers through search results or paid advertisements. These ads often refer to professional-looking websites with convincing promises of high returns.

- Social media platforms:**

Consumers fall victim to investment fraud through malicious advertisements on social media, promotion by influencers or malicious 'investment opportunities' through chat contact.

- Dating apps:**

Following a match on a dating platform, consumers are tempted to invest with or through a fraudulent party after intensive contact.

These methods – also known as 'social engineering' – are psychologically sophisticated and play on emotions such as trust, hope and greed.⁴ These online targeting techniques enable fraudsters to operate efficiently and constantly adapt their practices to new digital trends.

2 Europol (2025), The changing DNA of serious and organised crime; AFM Signalenmonitor 2023

3 Europol (2023), Online fraud schemes: a web of deceit

4 Drew & Cross (2016), Fraud and its PREY: Conceptualising Social Engineering Tactics and its Impact on Financial Literacy Outcomes

OVERVIEW Types of investment fraud

	Modus operandi	Offer	Promise	Communication	Victims
Boiler room fraud 	Fraudsters aggressively approach victims from call centers ('boiler rooms'). 	Fake stocks, fraudulent bonds, non-existent crypto-assets	High returns, exclusive opportunities	Phone, email, websites, social media and messaging apps	Investors
Ponzi fraud 	Fraudsters operate through professional-looking investment platforms. Returns are paid from money from new investors, rather than from actual investment profits.	Investments	High and guaranteed returns	Phone, email, websites, social media and messaging apps	Investors
Pyramid scheme 	Fraudsters lure investors through websites and fake reviews. Investors are financially rewarded for recruiting new investors.	Investments	High and guaranteed returns	Phone, email, websites, social media and messaging apps	Investors
Recovery room fraud 	Fraudsters pose as lawyers, regulators, or specialized firms. 	Assistance recovering prior lost investments	The lost money is recovered	Phone, email, websites, social media and messaging apps	Victims of previous investment fraud
Pump-and-dump fraud 	Fraudsters drive the price of stocks or crypto-assets to an artificially high level and then sell them off in high volumes.	A stock or crypto-asset will surge in price	Explosive price surges	Social media, influencers, bots, messaging apps, internet forums	Investors
Fraud with complex products 	Fraudsters offer (assistance with) investments in highly complex financial instruments. They pressure victims to deposit increasing sums of money and to trade frequently. 	Help in becoming a better trader	Lucrative investments	Fake advertisements with celebrities, phone, email, websites, social media and messaging apps	Investors

 This type of fraud often involves 'pig butchering', an approach in which victims are manipulated over longer stretches of time and financially 'fattened up', before finally being fully defrauded.

- Trust in the fraudster's professionalism and credibility;
- Susceptible to 'social proof';
- Frequently seeking higher returns and the opportunity to get rich quick.

2.4 Types of investment fraud

Nowadays, investment fraud often starts online. The first step is to approach consumers through fake advertisements with high returns, on social media, chat groups or so-called lead lists. Subsequently, persistent (often very) intensive contact (by telephone or chat) starts up between the fraudster and the victim. The victim is persuaded initially to invest a relatively small amount, such as €250. The fraudster then maintains intensive contact and persuades the victim to deposit increasingly larger sums.

Investment fraud occurs in different forms, which are fairly stable over time. However, the methods used within these forms are liable to change under the influence of far-reaching digitalisation and internationalisation, but also because fraudsters respond quickly to new trends and developments.

2.4.1 Boiler room fraud

Boiler room fraud is a form of investment fraud where fraudsters typically work from call centres (so-called boiler rooms) to aggressively approach potential investors and persuade them to invest in worthless or non-existent financial products. Boiler rooms often use fake stocks, fraudulent bonds or non-existent crypto-assets. The fraudsters present themselves as reputable investment advisers and use convincing sales techniques. In this way, they put pressure on victims, often with promises of high returns and exclusive opportunities displayed on dashboards with fake data. In the end, the victims lose most, if not all, of the invested capital and the perpetrators disappear. Boiler rooms usually operate from non-existent entities and often change names and websites. In addition, their physical location is often unclear and they defraud victims in different countries. This concealment of identity, the fleeting nature of boiler rooms and the international component make detection very difficult.

2.4.2 Ponzi fraud

Ponzi fraud is a form of investment fraud where returns are paid to previous investors with the deposits of new participants, rather than with actual profits from investments. This creates an illusion of profitability (sometimes by misleading victims through fake returns displayed on dashboards), when in reality there are limited to no legitimate revenue streams. Ponzi schemes are usually carried out through professional-looking investment platforms and personal networks. Modern Ponzi schemes operate online, through websites and social media, where scammers offer investments with promises of high, guaranteed returns. As long as enough new investors join, the fraudster can continue to make pay-outs and build trust. This can go on for extended periods of time, but eventually the system collapses when the inflow of new capital dries up or when too many investors want to withdraw their money at the same time. The term 'Ponzi scheme' derives from Charles Ponzi, who became infamous in the 1920s for a fraudulent stamp trading scheme. One of the most infamous modern cases is that of Bernie Madoff, who ran a large-scale Ponzi scheme for years, causing losses estimated at \$65 billion and seriously undermining confidence in financial institutions worldwide.

2.4.3 Pyramid scheme

A pyramid scheme is a form of investment fraud where participants invest money and are rewarded for recruiting new participants. The structure resembles a pyramid: the initial investors receive pay-outs from the deposits of newly recruited members, while most participants at the bottom eventually lose their money. Sometimes part of the money is actually invested, but not enough to pay out a return to all participants. As with Ponzi schemes, it can take a long time before a pyramid scheme is discovered, because investors are paid 'returns' as long as new participants join, so the fraud is not immediately visible.

Pyramid schemes are conducted in a variety of ways, both online and through in-person approaches. Nowadays, they are mainly run through social media and messaging apps, where scammers lure investors with success stories and exclusive investment groups. Email campaigns and online advertisements are also used to entice people with promises of high returns. Fake reviews and professional-looking

websites are often used to convey legitimacy. In addition, telephone recruitment is used, where fraudsters use aggressive sales techniques to put pressure on victims, similar to boiler room fraud.

2.4.4 Recovery room fraud

In recovery room fraud, victims of previous investment fraud are approached again by fraudsters who pretend to be lawyers, regulators (such as the AFM or ESMA) or specialised companies that can recover lost investments. The fraudsters claim that they can recover the lost money in return for payment of legal fees, administration fees or taxes. The fraudsters often have detailed information on previous losses, as victims end up on lead lists, which are then traded on the internet. Public complaints about fraud are also consulted. Armed with this information, the fraudsters can create a credible story and thus build confidence among their victims. In reality, the transferred funds disappear, causing victims to lose their money yet again and leaving them empty-handed.

2.4.5 Pump-and-dump

Pump-and-dump fraud is a manipulative trading strategy where scammers push the price of, for example, a stock or crypto-asset to an artificially high level before selling it all. Examples of the techniques used include misleading information, false rumours and organised buying promotions. This often happens through social media, influencers, bots, messaging apps and online forums, where it is easy to spread false analysis, fake news and hyped messages, and where fraudsters lure investors with promises of explosive price appreciation. Consumers are thus tempted to purchase the share or crypto-assets in question (pump). When many people do this, the value increases. Once the price has risen sufficiently, the fraudsters sell the positions that they took before the pump (dump), making a profit while the price then collapses and leaving other investors with large losses. Pump-and-dump fraud is particularly common in small, less liquid stocks and crypto-assets, where a relatively small group of traders can influence the price of a financial product.

2.4.6 Fraud with complex products

Some fraudsters offer investments in risky complex financial instruments such as contracts for difference (CFDs) or similar forex-related instruments, without disclosing the risks. These are basically legal products that can be used to invest, but rogue parties mislead their customers about the risks and the exact workings of the product. Victims are often lured with fake advertisements featuring well-known people who ostensibly promote a lucrative investment. After depositing a small amount of money, the victim is assigned an account manager or agent who will supposedly help the victim become a successful trader. The account manager pressures the victim into depositing more money and trading as much as possible. In doing so, they recommend trading with high leverage and the use of high-risk investment strategies. The account manager does not mention that the characteristic of a CFD is that it is settled between two parties. The victim is not aware that the platform that the account manager represents is the opposing party. Parties often seem to deliberately recruit victims outside their own jurisdiction, possibly so that the regulator is less likely to intervene.

A recent variation of this scam is fraud with so-called funded trading programmes, where the participants run a high risk of loss. These programmes promise that after successfully passing a paid testing phase, participants will have access to trading capital from the platform. In reality, many of these programmes are designed in such a way that participants almost always fail the test, which means that they have to pay again to resume the process. Some platforms also offer instant funding: participants get direct access to trading capital by paying a high entry fee (e.g. \$1,500). If an investor loses too much – which happens quickly due to the enormous leverage with which they trade – their account is immediately closed and they must pay again to continue trading. The revenue model of funded trading providers is therefore based not on sharing profits but on collecting new registration fees. Some platforms additionally manipulate the trading environment or apply unrealistic rules to prevent participants from succeeding. In addition, profit pay-outs are often subject to unreasonable conditions, such as a minimum number of transactions or a restriction whereby only a limited part of the investment can be withdrawn in a certain period. This leads to victims losing significant amounts of money without

ever actually accessing real trading capital or without having a fair chance of recouping the registration fees.

2.5 Specific approach: relationship investment fraud

Relationship investment fraud, also known as 'pig butchering', is an approach that is used in the various types of investment fraud mentioned above. This involves manipulating victims over a longer period of time and financially 'fattening' them up before they are completely scammed (butchered). The fraudsters often approach their targets through social media, dating apps or random text messages, spending a lot of time building trust. They pose as successful traders or old acquaintances and gradually introduce an attractive investment opportunity, usually in crypto-assets or forex. Victims are persuaded to invest small amounts of money, after which they initially see fake profits (on a fake dashboard, for example), which encourages them to deposit larger amounts. Eventually, once the victim has invested a significant amount, the scammers cut off access and disappear with the money. This type of approach involves a lot of shame, precisely because the victim thought they had entered into a relationship of trust with someone. This method of fraud has developed in recent years in particular due to the rise of crypto markets, and has spread rapidly through the digital world, with organised gangs, often from Southeast Asia, attracting victims in droves around the world with estimated losses of €64 billion since 2020.⁵

2.6 Perpetrators

Due to the digitalisation and internationalisation of the financial markets, investment fraud is increasingly being carried out by organised cybercriminals, scammers without a professional financial background and international criminal networks. Fraudulent investment offers are now widely distributed on social media and fake trading platforms. Criminal groups without a financial background can use deepfake videos, fake ads and social engineering to deceive victims,

5 Griffin & Mei (2024), How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering

6 Reuters (2025), What are Southeast Asia's scam centres, and why are they being dismantled?

7 Rechtspraak.nl

without the need for traditional financial institutions or platforms. In addition, we see that fraudsters often operate from countries with less strict regulations and target victims worldwide. There is also evidence of forced labour in criminal call centres (mainly in Southeast Asia) that focus on investment fraud, often in the form of relationship investment fraud and crypto fraud.⁶ These developments make detecting and combating investment fraud very complex.

Committing investment fraud requires not only technical capabilities, but also specific knowledge and psychological skills. In investment fraud, creating trust is crucial: victims invest because they believe in the sincerity of the fraudsters or their companies. Fraudsters often use a personal approach to build this trust with the victim. To strengthen credibility, psychological tactics are used, such as showing previous 'successful' investors, actually paying out returns to the investors (as in a Ponzi scheme), displaying authority such as using titles or partnerships with reputable companies or displaying the fraudsters' apparent wealth.

The low likelihood of being caught makes investment fraud particularly attractive to perpetrators. Investment fraud is relatively unlikely to be detected because it is often committed through digital platforms. In addition, perpetrators often operate in international groups. They are therefore difficult to trace and building criminal cases is challenging. In addition, perpetrators deliberately look for ways to circumvent bank detection, for example by encouraging victims to create their own crypto wallet, by using accounts in the name of money mules or by using credit cards for transactions. As an indication, in Dutch case law, the term 'investment fraud' has only appeared in a court decision 220 times since 2002,⁷ compared to, for example, 863 judgments relating to bankruptcy fraud.⁷

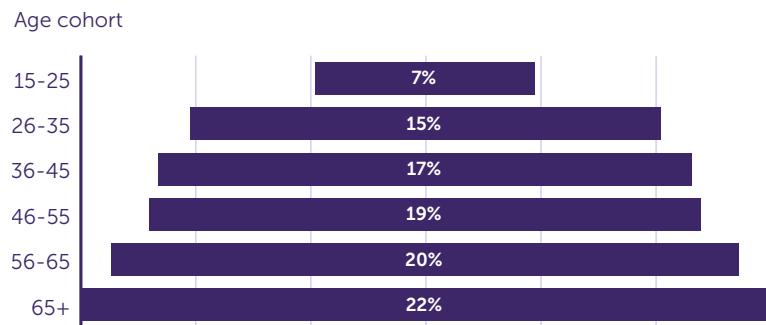
2.7 Victims

Victims of investment fraud are diverse, but they often share certain characteristics and psychological traits that make them susceptible to scams. One of the most important factors is trust in the fraudster's professionalism and credibility, especially if they present themselves as

a successful businessman or financial expert. In addition, social proof plays a significant role: if others appear to be investing and making a profit, potential victims lower their guard and are more likely to become involved.

Victims are often looking for high returns or financial security. These may be older people who want to supplement their pension, working people who are looking for a higher return than the savings rate offers or young investors who are tempted by high returns and the opportunity to get rich quickly. What is striking when looking at victims of investment fraud who have reported to the police or the Fraud Helpdesk is that the age cohorts are relatively evenly distributed (see Figure 1). Although the willingness to report and the number of people investing may vary by age group, this generally suggests that investment fraud can affect anyone, regardless of their investment experience or digital skills. However, the extent of the average losses will differ between the different age cohorts.

Figure 1: Distribution of ages of victims of investment fraud who have reported it



(Source: police and Fraud Helpdesk)

The high level of online financial services creates a large pool of potential victims for online fraudsters. Almost all Dutch people over the age of 12 (96%) use the internet on a daily basis, with 92.2% using internet or mobile banking.⁸ This broad digital presence increases

the likelihood that people will come into contact with fraudulent investments, which are often spread through online channels.

Victims of investment fraud are not necessarily financially gullible.

On the contrary, many victims have some investment experience but overestimate their own knowledge and underestimate the risks. Even well-trained professionals can fall for investment fraud if the scam is packaged in a plausible narrative, backed by ostensibly official documents, reliable intermediaries and legitimate-looking companies. Emotions such as greed, fear of missing out on an opportunity and trust in success stories make them vulnerable to fraudsters. This explains why investment fraud is often successful in times of economic uncertainty or emerging financial trends, such as crypto-assets or sustainable investments. Additionally, we see that psychological mechanisms take precedence over rational thinking once someone has invested money. Victims do not want to question their previous decisions and will, in fact, often reinvest in an attempt to recoup their losses. Moreover, the recent strong rise in recovery room fraud shows that repeated victimisation is becoming increasingly common in investment fraud.⁹ This partly explains why the losses from investment fraud are often substantial.

2.8 Facilitators

Facilitators are persons or entities who, consciously, unconsciously or under duress, make undermining crime possible. In many cases, interference in legitimate business through facilitators is intended to continue to facilitate criminal activities or to keep them out of sight. Investment fraud today almost always starts online. People are approached through social media, fake advertisements on social media or fraudulent websites. These 'digital facilitators', such as social media platforms, dating apps, finfluencers, ad affiliates and forums on crypto investing, play a very important role – possibly unknowingly – in enabling the recruitment of victims. Other digital applications, such as remote access tools, hosting companies, call centres and telecom providers which enable anonymity, and the dark web are also important. The latter could include CaaS (crime-as-a-service), where fraudsters

8 Statistics Netherlands figures on internet access and internet activities 2024

9 FSMA - Investment fraud and illegal offers – Dashboard 2nd half of 2024

buy the tools and skills of cybercriminals, as it were. Finally, investment fraudsters often use facilitators such as money mules and so-called 'cash couriers', i.e. often young people who are recruited by criminals, for example on social media, to have their bank account or debit card misused or to move physical money, for a fee.

3. The scale of investment fraud

Investment fraud is a serious and growing social problem, the true scale of which is structurally underestimated. Based on estimates, we see possible losses of €150 to €750 million per year. Despite increasing reports and amounts of losses being notified to authorities such as the AFM, the Fraud Helpdesk, the Public Prosecution Service, the Fiscal Intelligence and Investigation Service (FIOD) and the police, much of the fraud remains hidden due to low willingness among victims to report the crime. International estimates suggest that up to 90% of victims of investment fraud do not report, meaning that official figures reflect only a fraction of the problem. In the Netherlands – unlike in the United States, for example – there is no central registration of investment fraud cases. The discrepancy between the amount of losses reported by bodies such as the Fraud Helpdesk and the police and the losses revealed in individual criminal investigations also indicates that previously published figures underestimate the actual reported damage.

To determine the real impact, this chapter analyses the scale of investment fraud in three steps. Figures from the AFM, the Fraud Helpdesk, police, FIOD and FIU-Netherlands show a sharp increase in both the number of cases and the average loss amount between 2020 and 2024. Because these figures are compiled in different ways and there is no standardized registration, the figures cannot simply be combined. This underlines the fragmented nature of the registration landscape in the Netherlands. This national situation is then compared to international figures, which show that investment fraud is also increasing rapidly in other countries and is often accompanied by advanced digital techniques such as AI and blockchain technology. Based on extrapolation of these foreign figures with regard to reported damage, the scale of the losses in the Netherlands can be estimated. This estimate gives an indication of the expected reported damage in the Netherlands. Finally, we apply a correction to this indication based on willingness to report.

¹⁰ Police (2024), Online Fraud Landscape. Translation by AFM; not an official translation.

¹¹ It is important to note that victims of bank helpdesk fraud can sometimes be compensated for their loss, for which reporting is a requirement.

¹² Statistics Netherlands, Safety Monitor 2023.

¹³ Estimates range between 11% and 16.5%.

¹⁴ Deliema et al. (2017) Exploring the roles played by trust and technology in the online investment fraud victimisation process, FINRA (2013) Financial Fraud and Fraud Susceptibility in the United States.

3.1 The dark number of investment fraud

The full extent of investment fraud is difficult to measure, because part of the fraud is not registered and therefore remains unknown. This is known as the dark number. This has several causes, including the use of divergent and sometimes inconsistent definitions of investment fraud. The low willingness to report among victims also plays an important role. Victims of investment fraud often experience feelings of shame, guilt or lack of confidence in the usefulness of reporting to the authorities. As a result, the previously published figures on investment fraud are likely to underestimate the actual cases (and losses) of investment fraud.

The police's 'Online Fraud Landscape 2024'¹⁰ shows that the willingness to report varies greatly depending on the type of online fraud. Only 20% of victims of purchase fraud report it, whereas for bank helpdesk fraud the figure rises to 82%.¹¹ Statistics Netherlands data shows that 17% of victims of online fraud report it; there are no reporting percentages available specifically for investment fraud.¹² Although no exact percentage is known for investment fraud, it is plausible that willingness to report is also low in this case. This is not only due to feelings of personal responsibility and shame, but also because victims are not always aware that they have been victims of investment fraud. Instead, they think that their loss was the result of a normal unprofitable investment.

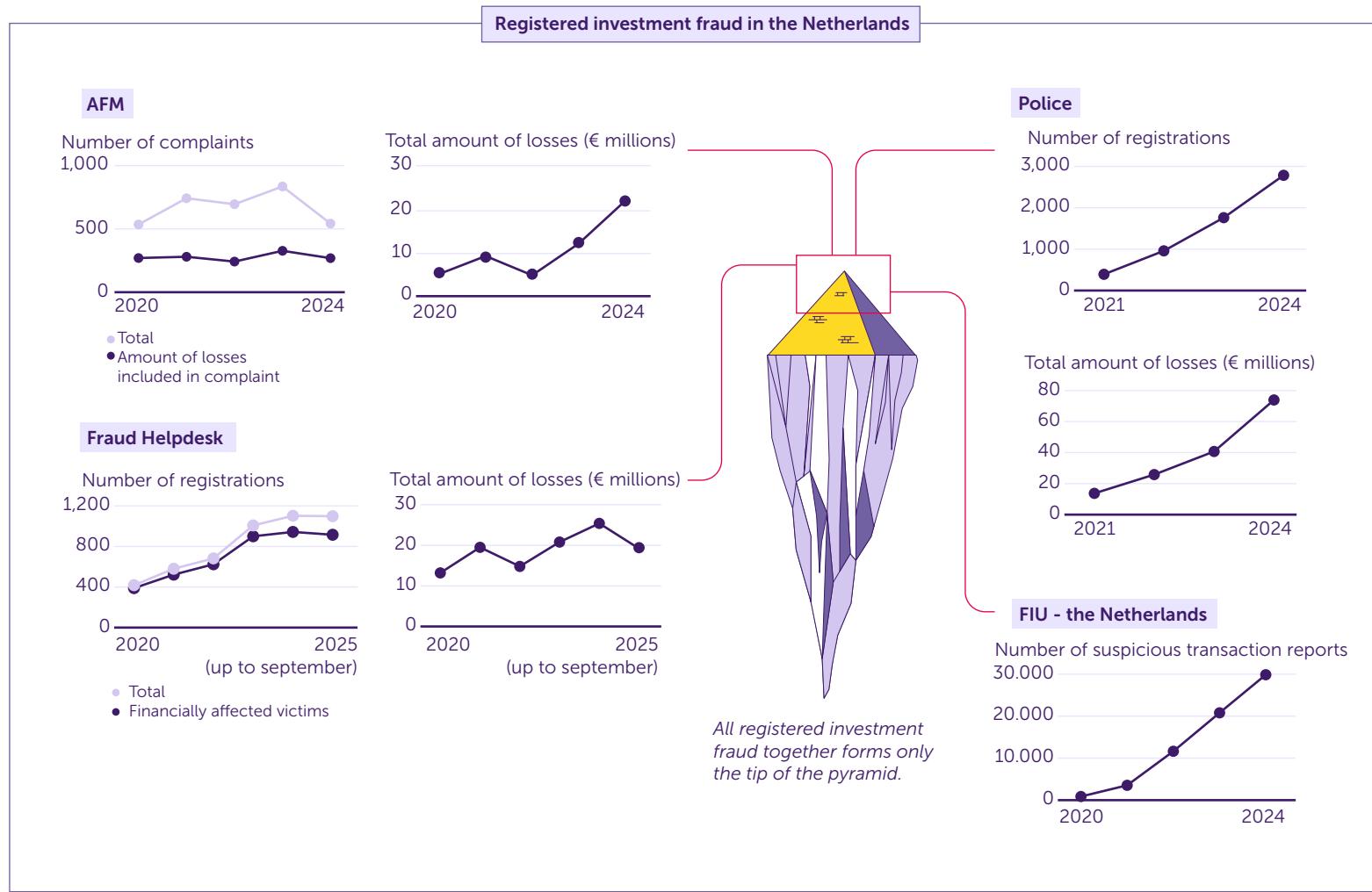
International sources also confirm the picture that only a small percentage¹³ of investment fraud victims report it.¹⁴ This suggests that our understanding of the scale of this type of crime is very limited worldwide.

3.2 The top of the pyramid: reported investment fraud in the Netherlands

In the Netherlands, there is no central reporting desk for investment fraud, which means there is only a fragmented view of the number of registered cases. Victims can report to the AFM, the police, the Public Prosecution Service, the FIOD, the Fraud Helpdesk or their bank. It is also common for victims to report to multiple agencies for a single incident, which results in duplicates in the registration.

Nevertheless, data from the AFM, the Fraud Helpdesk and the police show a clear increase in both the number of complaints and the amount of losses. The number of records made by the police increased by more than 600% between 2021 and 2024, from 392 to 2,785, while the reported amount of total losses rose to €75 million in 2024. The AFM and the Fraud Helpdesk also report a sharp increase, with average losses per incident almost quadrupling in a few years. FIU-Netherlands data confirms this trend with strong growth in the number of reported unusual transactions (often with a crypto component). Victims of investment fraud also often report to the financial institution or CASP where the transactions took place. The AFM has made enquiries of the NVB and a Dutch CASP about their insights into investment fraud. Both the NVB and the CASP indicate, based on a rough estimate, that the losses suffered by customers who have fallen victim to investment fraud is substantial (millions of euros per year) and show an upward trend over the past few years.

Figure 2: Registered complaints and amounts of losses due to investment fraud



3.2.1 Dutch Authority for the Financial Markets

The AFM has seen a sharp increase in the losses reported over the past four years. In recent years, the AFM has received between 500 and 800 reports of investment fraud. These include, for example, reports from consumers, but also valuable reports from banks that detect irregularities in their transaction monitoring at an early stage. An analysis of the reports received by the AFM in the period from 2020 to 2024¹⁵ shows that the total amount of losses per year in this period grew from approximately €5 million in 2020 to more than €22 million in 2024, amounting to more than €55 million over the entire period. The total amount of annual losses reported to the AFM increased by 300% during this period. It should be noted that only a fraction of the reports mention the amount lost. It is also worth noting that the reports are characterised by outliers of up to €3.6 million in losses per report.

The reports investigated by the AFM show a much higher amount of losses. Based on the reports received, the AFM may decide to start an investigation into possible violations of the regulations it supervises. If the investigation reveals indications of serious violations and criminal

offences, the AFM can file a report with the Public Prosecution Service to initiate a criminal investigation. Because these reports are the result of carefully conducted investigations, a better understanding of both the number of victims and the total extent of the fraud has emerged in these cases. This makes it possible to determine the average amount of losses per victim more accurately.

In total, the reports filed by the AFM between 2020 and 2024 involved losses of over €96 million, spread across 1,993 victims. The average amount of losses per victim is therefore approximately €48,300. The impact was particularly significant in 2023, with losses totalling over €82 million and more than 1,500 victims.

The percentage of reporting to the AFM was also found to be low, sitting at 5%. In the investigations that led to a report, consumers reported possible investment fraud to the AFM a total of 106 times. Compared to the total number of victims in these cases (1,993), meaning that approximately 5% of victims reported to the AFM.¹⁶

Table 1: Reports of investment fraud AFM 2020-2024

Year	Total reports	Reports with amount of losses	Total losses	Maximum losses for single report
2020	535	270	€5,188,164	€393,391
2021	742	280	€9,388,062	€1,800,000
2022	695	242	€4,893,294	€500,000
2023	835	327	€13,324,678	€3,632,788
2024	542	269	€22,296,875	€2,655,544
Total	3,349	1,388	€55,091,073	

15 For reliability, all reports that may have been related to investment fraud but contain less than 100 words are not included in the analysis.

16 This percentage gives an indication of the proportion of victims who report to the AFM on the basis of a limited number of observations (nine reports). A report can also be made by a consumer who has not become a victim. Furthermore, it happens that more victims report to the AFM after it has become known that the AFM is investigating.

Table 2: Overview of reports of investment fraud by the AFM to the Public Prosecution Service 2020-2024

Year	Total losses	Number of victims	Number of reports to the AFM	Average loss amount
2020	No reports	N/A	N/A	N/A
2021	€2.527.368	71	47 (66%)	€35.596
2022	€331.000	31	2 (6%)	€10.677
2023	€82.322.195	1.581	42 (3%)	€52.070
2024	€11.105.970	310	15 (5%)	€35.826
Total	€96.286.533	1.993	106 (5%)	€48.312

3.2.2 Fraud Helpdesk

The losses reported to the Fraud Helpdesk rose sharply during the examined period, to €25 million in 2024. The Fraud Helpdesk received more than 1,100 reports of suspected investment fraud in 2024. Of these, 943 victims actually reported financial losses. The total reported amount of damage in 2024 was €25.4 million. Since 2020, both the number of victims and the total amount of losses reported to the Fraud Helpdesk have increased sharply.

3.2.3 Police and FIOD

Official (statistical) figures on investment fraud by the police and the FIOD are unavailable, because investment fraud is often registered under broader categories such as scams or fraud. Nevertheless, several sources indicate an increase in the number of reports and the total losses from investment fraud. For example, the police's 'Online Fraud Landscape' shows that total losses of €31 million from investment fraud were reported to the police in 2023.¹⁷ This report also refers to various investigations by the FIOD in 2023 with a combined loss amount of €86 million. This is in line with the AFM's figures in 3.2.1, which show that the reports filed by the AFM with the Public

Prosecution Service and the FIOD in 2023 involved a loss amount of more than €82 million. These reports were drawn up after an extensive investigation by the AFM. An additional analysis at the request of the AFM of the cases of investment fraud recorded by the police in the period between 2021 and 2024 confirms the upward trend in both the number of reports and the amount of losses. The additional analysis adjusts the amount of damage from €31 million in 2023 to almost €41 million and shows an increase of about 80% to €75 million for 2024. The number of records also shows a significant increase of around 60%.

3.2.4 FIU-the Netherlands

FIU-the Netherlands is the central reporting point where various institutions¹⁸ report unusual transactions. At the request of the AFM, FIU-the Netherlands has created an overview of the phenomenon of investment fraud by means of strategic analysis based on the data available at FIU-the Netherlands.¹⁹

17 Police (2024), Online Fraud Landscape. Translation by AFM; not an official translation.

18 The Wwft designates various groups as [institutions with a reporting obligation](#) that act as "gatekeepers" of the financial system. These can include [art dealers](#), [banks](#), [notaries](#), [payment service providers](#) and [casinos](#). These institutions must monitor their activities for transactions that may be related to money laundering, underlying crimes or terrorist financing. FIU-the Netherlands receives these reports of unusual transactions (FIU-Netherlands website).

19 At the request of the AFM, FIU-the Netherlands searched its database and, based on keywords determined in consultation with the AFM, selected transactions that appeared to be related to investment fraud.

The strategic analysis shows a clear increase in the number of reported transactions that may be related to investment fraud (Figure 2).²⁰ Although this increase can partly be explained by increased attention and improved detection at institutions subject to a reporting obligation, the size of the reports indicates a growing problem. Between 2020 and 2024, a total of 66,717 unique transactions were reported, 19% of which were explicitly linked to boiler room fraud by the reporting entity. In addition, 19% of all reports contain a crypto component.²¹ Of the reported payment transactions, 73% were actually executed, with a combined transaction amount of €608 million. More than half of the payment transactions were below €1,000. Since 2021²², the number of reports has risen sharply, with an increase of more than 700% to almost 30,000 reports in 2024.

3.3 Recorded investment fraud internationally

Investment fraud is pre-eminently a cross-border form of crime and is increasing sharply in all the countries studied. For this reason, this section compares recorded investment fraud in five other countries²³. Investment fraud is increasing sharply in all the countries studied, both in size and complexity. In the United States, the damage rose to more than €4.8 billion in 2024; similarly sharp increases were visible in the United Kingdom and France. Germany and Italy also report growing losses. Notable trends include the use of AI, crypto-related fraud, romance scams and recovery room fraud. Although the number of reports remains relatively limited, investment fraud accounts for the largest share of financial losses among fraud types in several countries.

20 It is important to emphasise that this analysis is based solely on reports received by FIU-the Netherlands. The analysis therefore gives an indication, but not a complete picture, of investment fraud. The FIU-the Netherlands analysis may contain reports that do not actually concern investment fraud, may include duplications or may concern transactions without a Dutch component. As a result, it is not possible to draw firm conclusions about the total extent of investment fraud in the Netherlands based on these figures.

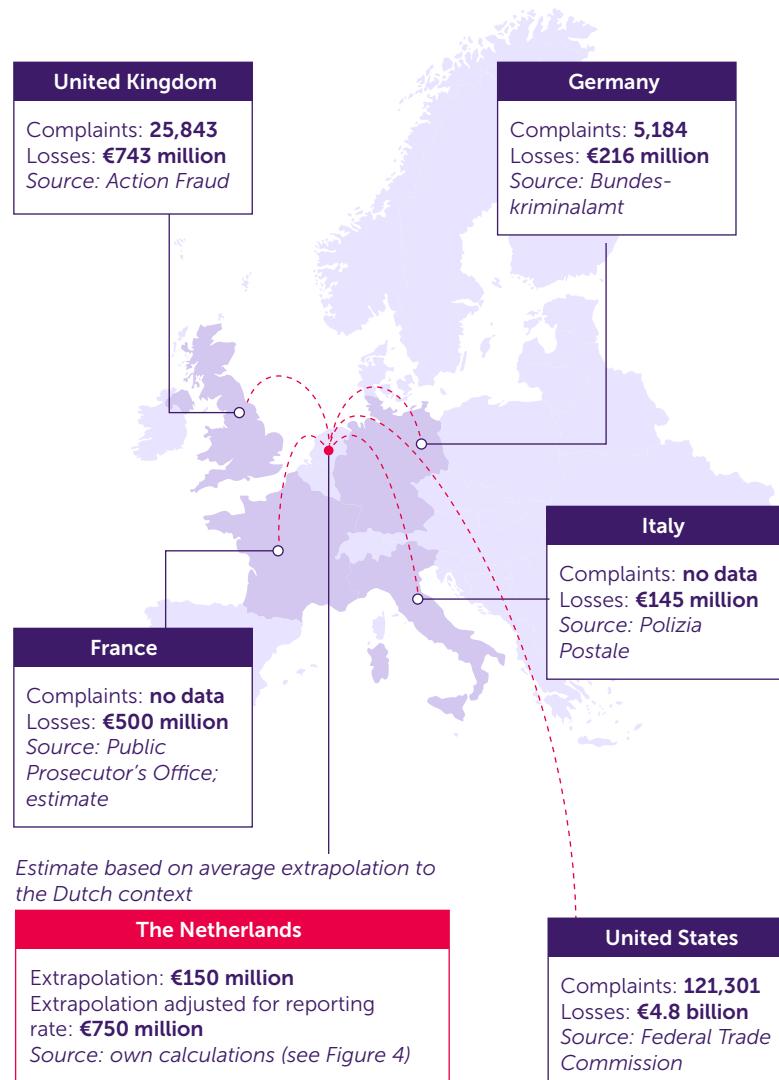
21 This is particularly evident in boiler room fraud (in 45% of cases) and pump-and-dump reports.

22 The increase from 2020 onwards gives a distorted picture, because FIU-the Netherlands no longer has transactions from before 1 August 2020 due to statutory data cleansing.

23 The methodology is explained in more detail in the appendix. When several authorities report figures on investment fraud in a country, the most conservative number is used in the comparison, unless the figures differ significantly, as in the case of France.

Figure 3: Losses due to investment fraud per country

Registered losses due to investment fraud per country



3.3.1 United States

In the United States, financial losses due to investment fraud rose to €4.8 billion in 2024. According to figures from the Federal Trade Commission (FTC), consumers lost more than €3.2 billion in 2022. This figure increased further by 21% to €3.9 billion in 2023. In 2024, the damage increased again by 24% to a total loss of €4.8 billion, with an average reported loss of €41,000.²⁴ In particular, the FTC identifies relationship investment fraud as a strongly emerging form. This makes extensive use of AI (deepfakes) and crypto-assets. In the same year, the FBI reported a damage amount of €5.6 billion.²⁵ Investment fraud is the category of internet-related crime with the highest damage, while only 7% of the number of reports concern investment fraud.

3.3.2 United Kingdom

In the United Kingdom, €743 million worth of damage from investment fraud was reported to Action Fraud in 2024. This was an increase of 13% compared to 2023, despite a 7% decrease in the number of reports²⁶. According to the Crime Survey for England and Wales (CSEW), there were an estimated 3.9 million fraud-related incidents in 2024, a 19% increase from the previous year²⁷. In 2024, the National Economic Crime Centre recorded 4.1 million fraud incidents, accounting for 43% of all recorded crime. Within this category, the number of romance scams and cases of investment fraud increased.²⁸ The British industry body UK Finance reported that UK banks saw more than €126 million

in damage from investment fraud in 2024 – a 34% increase from the previous year, despite a 24% drop in cases.²⁹ Investment fraud therefore forms a relatively small part of the incidents but is responsible for the largest share of the financial losses.

3.3.3 France

In France, a sharp increase in investment fraud has recently been observed. The Public Prosecutor's Office in Paris estimates the total scale of the losses from financial fraud in France in 2024 at €500 million per year.³⁰ At the request of the AFM, the French regulator AMF indicates that in 2021, consumers reported a total of €54 million in damage from investment fraud to the AMF. By 2024, this reached €68 million. In a representative survey of French investors conducted by the AMF, 1.2% of French adults (approximately 693,600 people) reported³¹ having been victims of investment fraud in 2021.³² By the end of 2024, that percentage had risen to 3.2% of French adults (approximately 1.7 million people³³). This means that between 2022–2024, an estimated 1.1 million new victims suffered losses.³⁴ The AMF reports an average loss of €29,000 per fraud victim (including investment fraud).³⁵

24 [New FTC Data Show a Big Jump in Reported Losses to Fraud to \\$12.5 Billion in 2024 | Federal Trade Commission; FTC - Consumer Sentinel Network](#).

25 [FBI – Internet Crime Report 2024](#).

26 [City of London Police: over £649m lost to investment fraud in 2024, with cryptocurrency fraud on the rise](#). This concerns the amount of damage related to all forms of investment fraud. Not all of these forms fall under the supervision of the Financial Conduct Authority.

27 [https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2024](#) Crime in England and Wales - Office for National Statistics.

28 [National Economic Crime Centre - Annual report 2024-2025](#).

29 [UK Finance Annual Fraud report 2025](#).

30 [The authorities are taking action to combat the massive phenomenon of financial scams catching out an increasing number of individuals | AMF](#).

31 AFM estimate.

32 [amf-report-invesment-scams-december-2024_2.pdf](#).

33 AFM estimate.

34 This AFM survey does not explicitly record whether respondents have been victims of investment fraud in the past year or at any time in the past. As a result, the increase from 1.2% to 3.2% over the entire 2022–2024 period cannot simply be interpreted as an absolute increase in new victims. These percentages therefore represent a cumulative increase and not necessarily an annual increase.

35 [The authorities are taking action to combat the massive phenomenon of financial scams catching out an increasing number of individuals | AMF](#).

Since the second half of 2023, crypto-related scams have surged in France, often through fraudulent trading platforms and misleading social media advertisements. Fake forex platforms and so-called trading robots also remain popular. Another striking trend is that recovery room fraud is becoming more common. The modus operandi of fraudsters is becoming increasingly sophisticated, including through the use of AI and social engineering. For example, fake videos and fake press releases are used in which celebrities "testify" about their alleged success with investments in crypto-assets.³⁶

3.3.4 Germany

The figures from the German Federal Police Office (Bundeskriminalamt - BKA) show an upward trend in damage from investment fraud to €216 million in 2024. The Bundeslagebild reports for 2023 and 2024 show a clear increase.³⁷ The number of investment fraud cases increased from 2,609 cases in 2023 to 5,184 in 2024, an increase of almost 100%, while the damage increased from €196 million to €216 million. This growth is partly due to extensive investigations, such as a case in Baden-Württemberg into services for concealing money flows from fraudulent online trading platforms.

The modus operandi therefore has a clear digital component in Germany. The main manifestations are cybertrading through online platforms and romance scams. Furthermore, victims are often approached again through recovery room fraud, in which so-called lawyers offer help in recovering previously incurred losses for a fee. The BKA states that the criminal network surrounding investment fraud is professionally organised with call centres, platform providers, affiliate marketing and international money laundering networks.

3.3.5 Italy

In its annual report for 2024, the Italian cyber police Polizia Postale calls investment fraud one of the fastest growing forms of cyber-crime, amounting to €145 million in 2024.³⁸ The Polizia Postale also reports a clear increase in registered damage from investment fraud. Consob, the Italian regulator, recognises this trend. According to

figures provided by Consob to the AFM, losses grew from €110 million in 2023 to €145 million in 2024, an increase of 32%.

Consob also points to a growing presence of fraudulent investment platforms, in which crypto-assets increasingly play a role. Fraudsters successfully target a broad group of investors (not just more vulnerable groups, such as the elderly), which indicates sophisticated organisation and methods.

3.4 A full view of the pyramid: estimation of the scale of registered damage from investment fraud in the Netherlands

As the previously published figures probably only show part of the extent of the registered damage, it is important to estimate the expected registered scale of investment fraud in the Netherlands in various ways. To do this, the AFM uses two approaches based on an international benchmark comparison. Using this benchmark, we make an extrapolation based on the number of inhabitants and a second extrapolation based on gross domestic product (GDP). Both methods give an indication but must be viewed with due regard to uncertainty.

Figure 4 provides an overview of the registered damage due to investment fraud in the five countries as described in Section 3.3. For each country, the amount of losses that is calculated for the extrapolation to the Netherlands is shown. The amount of losses is then shown when we extrapolate the figures from that country to the Dutch situation. We do this based on two criteria: the number of inhabitants aged 18 and over and gross domestic product. It follows that the recorded amounts of damage vary greatly between countries, with the United States and the United Kingdom showing the highest absolute losses. The average extrapolation for the Netherlands is approximately €148.8 million based on population and approximately €151.8 million based on GDP. These approaches indicate that the expected registered size of investment fraud in the Netherlands is approximately €150 million.

³⁶ The authorities are taking action to combat the massive phenomenon of financial scams catching out an increasing number of individuals | AMF.

³⁷ BKA - Federal Situation Report on Economic Crime 2023 & BKA - Federal Situation Report on Economic Crime 2024

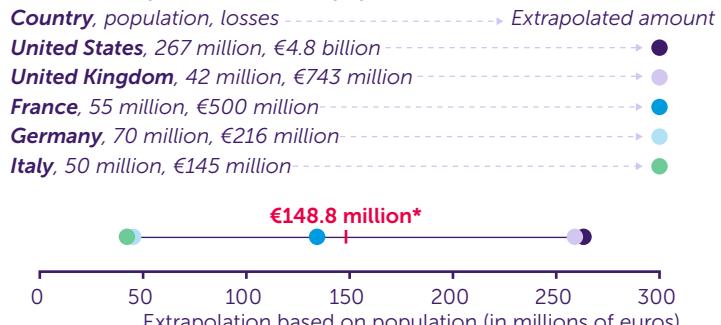
³⁸ Postal and Cyber Security Police – 2024 annual report.

A comparison of Dutch and international reports must take the necessary caveats into consideration. For example, the degree of comparability is influenced by the variation in the presence of a central registration point for investment fraud. In countries such as the United States and the United Kingdom, central registration exists, while in the Netherlands, France, Germany and Italy, it does not. This can lead to differences in the number of registered cases, regardless of the actual scale of investment fraud. In any case, it is striking that countries with such a central registration point clearly report higher losses. In addition, there are factors specific to the Dutch context, such as the pension system and the high level of home ownership, which may lead to a lower level of investment fraud in the international context. For example, the Dutch pension system manages a relatively large proportion of the assets of professional investors, who are much less vulnerable to investment fraud. A third factor that may play a role is the willingness to report. Despite the uncertainty surrounding this – dark numbers – there are currently no indications that the willingness to report differs greatly for the countries included in the comparison. This is therefore a structural limitation that plays a role in every country included in the comparison. In general, the share of investment fraud as a percentage of GDP falls within a similar range in most countries.

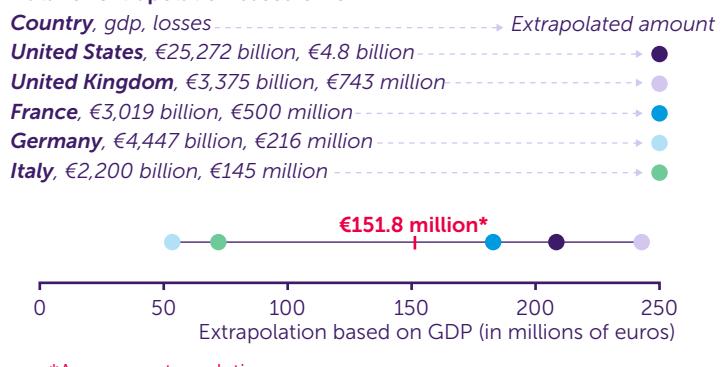
Figure 4: Losses due to investment fraud per country

The expected reported scale of investment fraud in the Netherlands is approximately €150 million. Below and in paragraphs 5.1.2 en 5.1.3 is an explanation of how the AFM arrived at this amount by extrapolating data from other countries to the Dutch context.

Data for extrapolation based on population size:



Data for extrapolation based on GDP:



3.5 The iceberg below the pyramid: estimation of the hidden scale of investment fraud in the Netherlands

Based on the international extrapolation from Section 3.4 (€150 million), adjusted with the reporting percentage, the actual scale of the losses caused by investment fraud in the Netherlands is estimated at approximately €750 million per year. This is because the willingness to report investment fraud is low, meaning that the registered losses only reflect a fraction of the actual scale. The expected reported damage must therefore be regarded as a lower limit and thus be adjusted to take account of the willingness to report. There are no Dutch figures available on the willingness to report investment fraud, specifically. Based on cases in which the AFM has filed a report with the Public Prosecution Service in recent years, the reporting percentage is approximately 5%. More generally, data from Statistics Netherlands shows that 17% of victims of online fraud report it. International sources (see Section 3.1) show a reporting rate between 11% and 16.5%. In summary, it follows that the reporting rate of investment fraud is probably somewhere between 5% and 17%. The reporting rate from the reports filed by the AFM is based on a limited number of cases. To limit the risk of overestimation, using the percentage based on Statistics Netherlands data seems more appropriate. This means that the expected reported damage must be multiplied by at least a factor of five in order to arrive at a realistic estimate of the actual scale of investment fraud.

4. The current approach to investment fraud in the Netherlands

Who tackles investment fraud and how they do so depends greatly on the type of fraud and the techniques involved. After all, investment fraud is a collective term for different kinds of fraudulent behaviour and does not have its own section of criminal law. Partly as a result of this, various parties are involved in tackling investment fraud. At the national level, public and private partners collaborate through the Integrated

Approach to Online Fraud. Under the coordination of the Ministry of Justice and Security, these partners work on targeted interventions to combat online fraud more swiftly, decisively and effectively. The approach to investment fraud is schematically shown below for each type.

4.1 Approach

4.1.1 Boiler room fraud

Actor	Description
Gatekeepers	<ul style="list-style-type: none">Outgoing payments relating to deposits from consumers that gatekeepers consider unusual must be reported to the FIU as an unusual transaction.Incoming payments involving a Dutch bank account used by the boiler room – often from a money mule – can be reported to the FIU.
Supervision and enforcement	<ul style="list-style-type: none">The provision of investment services (including fictitious services) with regard to financial instruments or crypto-assets falls under the supervision of the AFM.Aggressive or misleading commercial practices are subject to supervision by the AFM, in the case of financial products, or ACM.IOSCO maintains a global overview of warnings about boiler rooms (I-Scan).
Investigation and prosecution	<ul style="list-style-type: none">The provision of investment services without a licence is an economic offence.The provision of fictitious investment services is a type of fraud.Online boiler room fraud may be accompanied by cyber- or cyber-enabled crime.

4.1.2 Ponzi fraud

Actor	Description
Gatekeepers	<ul style="list-style-type: none"> Outgoing payments relating to deposits from consumers that gatekeepers consider unusual must be reported to the FIU as an unusual transaction. Incoming payments relating to deposits from consumers that gatekeepers consider unusual must be reported to the FIU as such. Gatekeepers must report outgoing payments relating to the distribution of returns from the deposits of new investors to the FIU as an unusual transaction. Gatekeepers must report outgoing payments that conflict with the offer to the FIU as unusual transactions.
Supervision and enforcement	<ul style="list-style-type: none"> The issuance of securities such as bonds is (in principle) subject to a prospectus and falls under the supervision of the AFM. The management of an investment fund falls under the supervision of the AFM.
Investigation and prosecution	<ul style="list-style-type: none"> Violation of the prospectus obligation is an economic offence. Managing an investment fund without a licence is an economic offence. Self-enrichment by the provider constitutes embezzlement. Inducing investors to invest under false pretences is fraud.

4.1.3 Pyramid scheme

Actor	Description
Gatekeepers	<ul style="list-style-type: none"> Outgoing payments relating to deposits from consumers that gatekeepers consider unusual must be reported to the FIU as an unusual transaction. The same applies to incoming payments relating to deposits from consumers that gatekeepers consider unusual. Gatekeepers must report outgoing payments regarding fees for bringing in new customers to the FIU as an unusual transaction.
Supervision and enforcement	<ul style="list-style-type: none"> When a pyramid scheme has characteristics of a game of chance, it falls under a prohibition supervised by the Netherlands Gambling Authority (KSA). The sale of financial and other products by means of a pyramid scheme is a misleading commercial practice and is subject to supervision of the AFM, in the case of financial products, or ACM.
Investigation and prosecution	<ul style="list-style-type: none"> Offering a pyramid scheme with characteristics of a game of chance is an economic offence. Self-enrichment by the provider constitutes embezzlement. Inducing investors to invest under false pretences is fraud.

4.1.4 Recovery room fraud

Actor	Description
Gatekeepers	<ul style="list-style-type: none"> Outgoing payments from consumers to recovery room fraud operators that gatekeepers consider unusual must be reported to the FIU as unusual.
Supervision and enforcement	<ul style="list-style-type: none"> Recovery room fraud does not fall within the legal mandate of a regulator, as it does not involve financial services. It is not an economic offence but a common offence (fraud).
Investigation and prosecution	<ul style="list-style-type: none"> Inducing investors under false pretences to pay to supposedly help recover their previous loss constitutes fraud.

4.1.5 Pump-and-dump

Actor	Description
Gatekeepers	<ul style="list-style-type: none"> Financial institutions report unusual price movements or trading transactions with regard to financial instruments to the AFM. Crypto-asset service providers are obliged to report suspicious transactions and/or orders to the AFM. Unusual price movements or trading transactions in relation to crypto-assets are reported to the FIU.
Supervision and enforcement	<ul style="list-style-type: none"> Pump-and-dump is a form of market manipulation that falls within the AFM's supervisory remit, insofar as it concerns financial instruments that are traded on a Dutch platform or Dutch persons who carry out the pump-and-dump. The AFM also has an enforcement mandate in the event of pump-and-dump with crypto-assets.
Investigation and prosecution	<ul style="list-style-type: none"> Market manipulation is an economic offence.

4.1.6 Fraud with complex products

Actor	Description
Gatekeepers	<ul style="list-style-type: none"> Outgoing payments relating to deposits made by consumers that businesses consider unusual must be reported to the FIU as an unusual transaction.
Supervision and enforcement	<ul style="list-style-type: none"> The provision of investment services in relation to financial instruments or crypto-assets is subject to supervision by the AFM. Aggressive or misleading commercial practices with regard to financial instruments are subject to supervision by the AFM.
Investigation and prosecution	<ul style="list-style-type: none"> Inducing investors to invest under false pretences constitutes fraud.

4.2 Tackling investment fraud within financial supervision

In the field of financial supervision, various laws protect investors and tackle illegal providers, and cooperation with partners is actively sought in order to join forces. The Financial Supervision Act requires parties that offer investment services or products to have an AFM licence and the Consumer Protection Enforcement Act prohibits the use of misleading or aggressive commercial practices when providing services. Fraudsters who operate without a licence – such as boiler rooms – violate this legislation and the AFM can, on this basis, issue public warnings or impose administrative fines, for example. The AFM therefore regularly publishes warnings stating the names of fraudulent investment platforms and intermediaries. In order to increase its effectiveness, the AFM works with stakeholders, including Dutch banks, to publish boiler room websites on the warning list more quickly and to have them taken offline. The AFM is a partner of the Financial Expertise Centre (FEC) where knowledge and experience on financial economic crime is exchanged.

4.3 Investment fraud within criminal law

In criminal law, investment fraud often falls under the heading of fraud or embezzlement or concerns the prosecution of economic offences resulting from violations of supervisory legislation. Although the word ‘fraud’ does not have its own legal definition and functions as a collective term, investment fraud and similar scams are classified as a form of horizontal fraud. These are forms of fraud in which the injured party is not a government agency; the latter situation is known as vertical fraud. The detection of investment fraud in the Netherlands is the responsibility of the police and the FIOD. Traditionally, the approach to horizontal fraud has been focused on the police.³⁹ Every police unit has fraud teams that investigate reports of fraud and internet fraud. The

FIOD specialises in financial crime and is part of the Tax and Customs Administration. Because of the strong financial component, the FIOD is also active in combating specific themes within horizontal fraud such as investment fraud, where there is also a violation of financial supervisory legislation and the cases concerned have effect and impact because of the large scale or impact on society.⁴⁰

Fraud is a growing area of attention within the criminal law approach.

Figures from the Public Prosecution Service show that the number of fraud cases it recorded increased significantly between 2021 and 2022 compared to previous years.⁴¹ Whereas in 2018-2019 the Public Prosecution Service received around 3,000 to 4,000 fraud files annually, in 2021 there were almost 6,000. This increase indicates that investigative services are also able to detect and arrest more online investment fraudsters. For example, several investigations by the FIOD into investment fraud were completed in 2023. In August 2023, the FIOD arrested three suspects in an international fraud case in which Dutch investors had been duped.⁴² In addition, in April 2023, the FIOD arrested two people and searched a home for large-scale investment fraud after a report by the AFM; this involved a then 26-year-old main suspect who allegedly defrauded dozens of people.⁴³ The FIOD conducts such complex investigations under the authority of the Functional Public Prosecutor’s Office of the Public Prosecution Service, due to the required financial expertise.

4.4 Prevention and education

Prevention and education are integral to tackling investment fraud.

Prevention focuses both on making potential victims more resilient and on disrupting the modus operandi of fraudsters before they can strike. From 2020 to 2025, various initiatives and campaigns were launched to warn the public and block fraud attempts in time. An important aspect of prevention is public awareness. Various organisations – the AFM,

39 [Public Prosecution Service – Fraud Monitor 2021 and 2022](#).

40 [FIOD Annual Report 2024](#): Public Prosecution Service – Fraud Monitor 2021 and 2022.

41 [Fraudemonitor 2021-2022](#).

42 <https://www.fiod.nl/drie-verdachten-aangehouden-in-onderzoek-naar-omvangrijke-beleggingsfraude/>.

43 <https://www.fiod.nl/aanhouding-vanwege-grootschalige-beleggingsfraude/>.

the Fraud Helpdesk, the Police and the Ministry of Justice & Security – have actively warned about investment fraud through mainstream and social media, news releases and information campaigns. In 2021, for example, the AFM launched campaigns targeting fake advertisements featuring well-known Dutch people⁴⁴ and finfluencers⁴⁵ to prevent them from unknowingly participating in deception. In addition, the AFM launched www.checkjeaanbieder.nl in 2024 <http://www.checkjeaanbieder.nl/>, where consumers can find information about warnings, fraudsters' practices and red flags. The Fraud Helpdesk plays a central role in prevention and victim support, and Dutch banks are also actively committed to protecting their customers from investment fraud through prevention campaigns and warning notifications. We see this as a positive development. The problem of investment fraud can only be combated jointly.

4.5 International approach

At the international level, too, work is being carried out in a joint approach to online investment fraud. The international supervisory organisation IOSCO⁴⁶ plays an important role in this, for example by contacting social media platforms to encourage them to play a greater role in the fight against fraud and through the I-SCAN digital warning platform. This platform makes it possible to share public warnings from regulators worldwide and allows them to exchange information among themselves, which strengthens the investigation into cross-border investment fraud.

Europol considers online investment fraud to be one of the biggest crime threats in the EU today and plays a central role in the cooperation between investigative services. As a centre of expertise, Europol provides operational support and coordinates joint actions. Europol considers online investment fraud to be one of the biggest crime threats in the

44 <https://www.afm.nl/nl-nl/sector/actueel/2021/oktober/campagne-tegen-beleggingsfraudeurs>.

45 <https://www.afm.nl/nl-nl/sector/actueel/2021/december/verkenning-finfluencers>.

46 IOSCO is the body that connects financial regulators in the securities market worldwide: more than 95% of the regulators are affiliated, from more than 130 jurisdictions.

47 Europol (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, Luxembourg.

48 Europol (2025), European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg.

49 <https://www.consilium.europa.eu/en/press/press-releases/2025/06/13/council-defines-eu-crime-fighting-priorities-for-next-years/> and EUR-Lex - 52025DC0148 - EN - EUR-Lex.

50 FCA Annual Report – 2024.

EU today. Recent threat analyses, such as the Internet Crime Threat Assessment (IOCTA) 2024⁴⁷ and the Serious and Organised Crime Threat Assessment (SOCTA) 2025⁴⁸, identify investment fraud as one of the most urgent and extensive forms of online crime. The analyses show that thousands of people are affected and that the proceeds for criminals are very large. Crypto plays a key role in this, both as a lure for investments and as a means of payment within fraudulent structures. Furthermore, the reports highlight that criminals are deploying increasingly sophisticated techniques, including AI-generated ads and fraudulent apps distributed through legitimate app stores. They also use so-called remote administrative tools (RATs) to gain access to victims' devices.

Using AI helps fraudsters create compelling and up-to-date stories that respond to societal trends, making fraud more difficult to spot.

Europol warns that the scale and complexity of online fraud is expected to increase further. This development has a financial as well as a psychological impact on victims. Party in view of these developments, the European Commission has prioritized 'online fraud schemes' and has announced an 'Action Plan on Online Fraud'.⁴⁹

A good example of an effective approach to online investment fraud is the approach taken by the Financial Conduct Authority (FCA). In many cases, consumers come into contact with investment fraudsters through malicious websites or fake advertisements. The FCA tackles online investment fraud right from the source by taking illegal websites offline – more than 1,600 in 2024 – banning rogue financial promotions and, in collaboration with big tech platforms, having malicious apps removed from the app store.⁵⁰

5. Appendices

5.1 Methodology and justification

5.1.1 Aim and approach

Determining the true scale of investment fraud in the Netherlands requires an approach that goes beyond analysing registered reports. Due to the presumed low willingness to report and the lack of central registration in the Netherlands, a multiple methodology approach has been adopted that consists of:

1. Analysis of reports and amount of losses registered by various Dutch authorities, see Section 3.2;
2. International benchmark comparison with countries that are comparable to the Netherlands in terms of their economic context, see Section 3.3 and a further explanation in Section 5.1.2;
3. Extrapolation to the Dutch situation based on population and GDP, see Section 3.4 and a further explanation in Sections 5.1.3 and 5.1.4.

5.1.2 International benchmark comparison

For a meaningful comparison with other countries, it is important to assess the extent to which the Dutch context with regard to investment fraud can be compared to that of other countries. We assume that the actual extent of investment fraud depends on a number of specific characteristics related to the behaviour and wealth of consumers or 'demand side' on the one hand, and the financial infrastructure and macroeconomic environment or 'supply side' on the other. Consumers' behaviour and wealth include risk appetite, the degree of digital skills, consumer confidence, the size of free savings and the level of income.

How these factors influence the scale of investment fraud is shown in Table 3. This table provides an overview of factors that influence the extent of investment fraud, divided into supply and demand sides. The second column (+ or -) shows whether a factor has a positive, i.e. increasing (+), or negative, i.e. decreasing (-), effect on the extent of investment fraud. The third column describes how this factor manifests itself in the Dutch context.

Table 3: Demand and supply side of investment fraud

Factors	General effect on the scale of investment fraud + -	Factor within the Dutch context (increasing/decreasing)
Demand side	Risk appetite	Decreasing. Investors are generally relatively risk-averse. ⁵¹
	Consumer confidence	Decreasing. Confidence is negative, which means that willingness to buy is relatively low. ⁵² This leads to a higher savings rate and possibly less demand for risky investments.
	Digital skills	Increasing. Consumers have a relatively high level of digital skills. ⁵³ At the same time, they often overestimate their digital skills. ⁵⁴
	Size of free savings	Increasing. Consumers have a relatively large amount of savings (an average of €73,000 per household) and the Netherlands has a relatively high savings rate. ⁵⁵
	Income	Decreasing. Disposable household income is below the OECD average. ⁵⁶
Supply side	Interest rates	Increasing. The interest rate in the Netherlands follows the ECB. Interest rates have recently been historically low.
	Online trading offer	Increasing. The Netherlands has a number of local providers that offer online investing. Due to its high level of digital skills and a good digital infrastructure, the Netherlands is an attractive market for online providers based elsewhere in the EU.
	Popularity of crypto-assets	Increasing. Around 13% of households invest in crypto-assets, of which 4% invest exclusively in crypto. Research by the AFM among investors shows that 22% of investors also invest in crypto. ⁵⁷
	Financial regulation and effective system of gatekeepers	Increasing. The FATF describes the Dutch approach to money laundering as a robust system. ⁵⁸

51 [AFM Consumer Monitor Investing 2024](#); An exception to this was the sharp increase in popularity for independent investing during the Covid pandemic. These novice investors had a preference for risky investment products.

52 [Statistics Netherlands - Consumer confidence](#) and see Figure 5.

53 [Statistics Netherlands \(2023\) - The Dutch increasingly digitally skilled; The Netherlands 2025 Country Report on the Digital Decade | Shaping Europe's digital future](#)

54 [Centerdata \(2023\) - Digital skills of the Dutch?](#)

55 [DNB \(2025\) - Dutch households save record amount: what's behind it? DNB - Household Savings Dashboard; NOS - We sparen flink door and Figure 6](#)

56 The OECD dashboard and Statistics Netherlands data differ on this point. Statistics Netherlands data points to disposable income above the OECD average ([Prosperity of private households: key figures | Statistics Netherlands](#)). The OECD dashboard therefore offers a lower limit here. Also see Figure 7.

57 <https://www.kantar.com/nl/kantar-nieuws/dutch-wealth-control-2024>; AFM Consumer Monitor Investing 2025.

58 <https://www.rijksoverheid.nl/actueel/nieuws/2022/08/24/fatf-beoordeelt-nederland-positief-in-evaluatie-aanpak-witwassen>

The purpose of this analysis is to assess the extent to which the Netherlands can be compared to other countries. By examining the direction of each factor, we can estimate whether specific countries are sufficiently similar to the Dutch context to include

them in the benchmark comparison. Table 4 provides an overview of the comparability of these countries. It follows that these countries are sufficiently similar to the Netherlands to arrive at a reliable estimate.

Table 4: Comparability of benchmark countries

Factors vs Netherlands		United States	United Kingdom	France	Germany	Italy
Demand side	Risk appetite ⁵⁹	Higher	Higher	Equal	Equal	Lower
	Consumer confidence ⁶⁰	Equal	Equal	Equal	Equal	Higher
	Digital skills ⁶¹	Lower ⁶²	Equal ⁶³	Lower ⁶⁴	Lower	Much lower ⁶⁵
	Size of free savings ⁶⁶	Lower	Lower	Equal	Equal	Lower
	Income ⁶⁷	Higher	Equal	Equal	Equal	Lower
Supply side	Interest rates ⁶⁸	Higher	Higher	Equal	Equal	Equal
	Online trading offer	Equal	Equal	Equal	Equal	Equal
	Popularity of crypto-assets	Higher ⁶⁹	Higher ⁷⁰	Equal ⁷¹	Equal ⁷²	Equal ⁷³
	Financial regulation and effective system of gatekeepers ⁷⁴	Equal	Equal	Equal	Equal	Equal

59 Financial Times - Britons have lowest appetite for stock market investing in the G7; Brooks & Williams (2022) – People are people: A comparative analysis of risk attitudes across Europe.

60 Figure 5

61 Dutch people in European leading group of digital skills | Statistics Netherlands.

62 National Skills Coalition (2020) - The New Landscape of Digital Literacy.

63 Dutch people in European leading group of digital skills | Statistics Netherlands.

64 France 2025 Country Report on the Digital Decade | Shaping Europe's digital future.

65 Dutch people in European leading group of digital skills | Statistics Netherlands.

66 Figure 6

67 Figure 7

68 Figure 8

69 PEW Research Center (2024): Majority of Americans aren't confident in the safety and reliability of cryptocurrency.

70 Financial Conduct Authority: Cryptoassets consumer research 2024.

71 European Central Bank (ECB) – Consumer survey 2024.

72 European Central Bank (ECB) – Consumer survey 2024.

73 European Central Bank (ECB) – Consumer survey 2024.

74 FATF - Consolidated assessment ratings.

United States: The United States differs from the Netherlands in several ways. The higher risk appetite, higher income and greater popularity of crypto-assets indicate a higher relative size of investment fraud. However, the more limited digital skills, lower savings (precisely due to more investment) and higher interest rates indicate a lower relative size of investment fraud. In view of this balance, the United States is sufficiently equal to the Netherlands to be used as a benchmark.

United Kingdom: The United Kingdom is similar to the Netherlands in many ways. Investors' risk appetite and the popularity of crypto-assets are higher in the UK. As a result, the expected extent of investment fraud is higher than in the Netherlands. On the other hand, there are lower savings and higher interest rates, which has an inverse effect on the expected extent of investment fraud.

France: France is similar to the Netherlands for most factors. The level of digital skills in France is lower than in the Netherlands. This indicates a lower expected level of investment fraud. Since this is the only deviating factor, France is comparable to the Netherlands.

Germany: Germany is similar in many ways and is therefore generally comparable to the Netherlands. For example, both countries have a high savings capacity and a similar average gross income.⁷⁵ Digital skills in Germany are lower.⁷⁶ The popularity of crypto-assets is about the same as in the Netherlands.

Italy: In terms of risk appetite and average income, Italy is the only country in the benchmark that scores lower than the Netherlands. The significantly lower level of digital skills is striking. Other factors are about the same as in the Netherlands. It is therefore likely that the expected size of investment fraud will be lower than in the Netherlands. The inclusion of Italy in the benchmark comparison is therefore not expected to result in an overestimation of the size in the Netherlands.

⁷⁵ Average gross monthly earnings - German Federal Statistical Office.

⁷⁶ Germany | Digital Skills and Jobs Platform.

Figure 5: Consumer confidence 2020 to April 2025 (source: Households' economic well-being: the OECD dashboard)

Consumer confidence

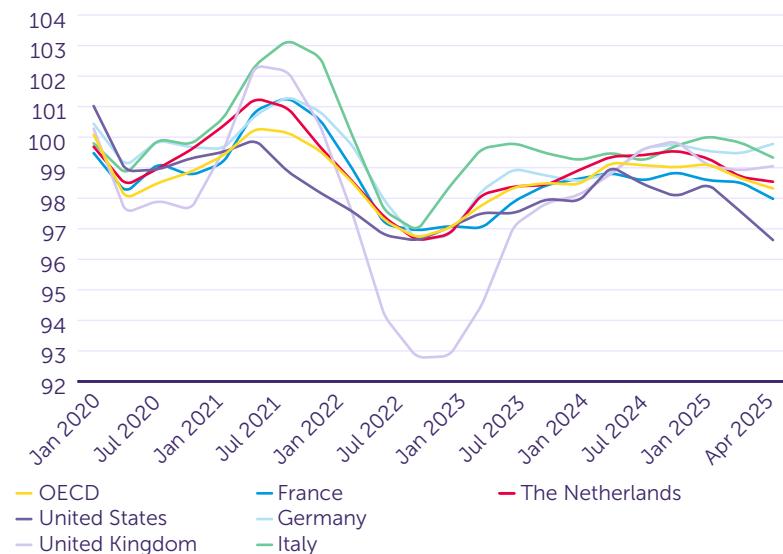


Figure 6: Savings rate 2020 to April 2025 (source: Household savings rate, the OECD dashboard)

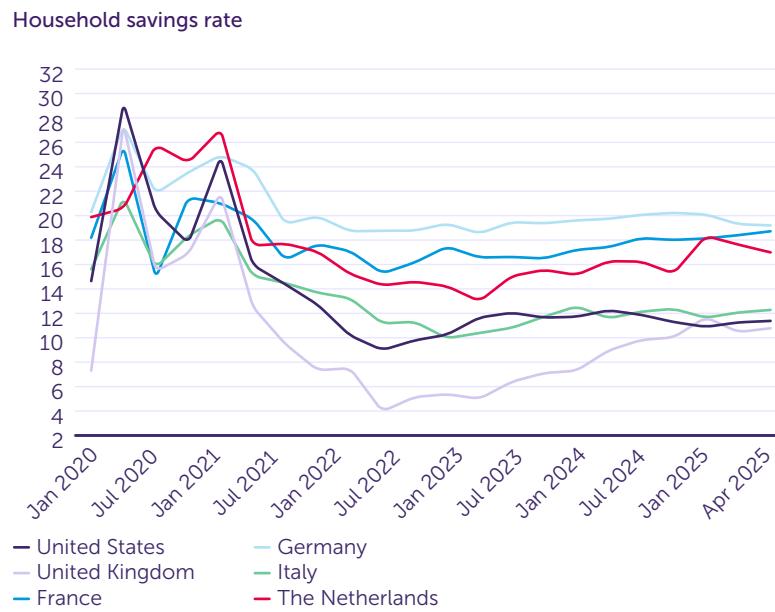


Figure 7: Disposable income 2020 to April 2025 (source: Households' economic well-being: the OECD dashboard)

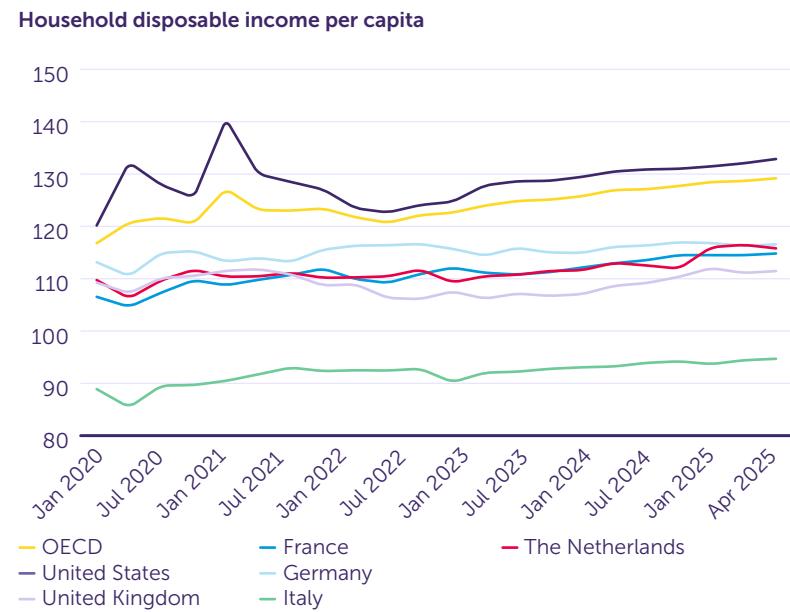
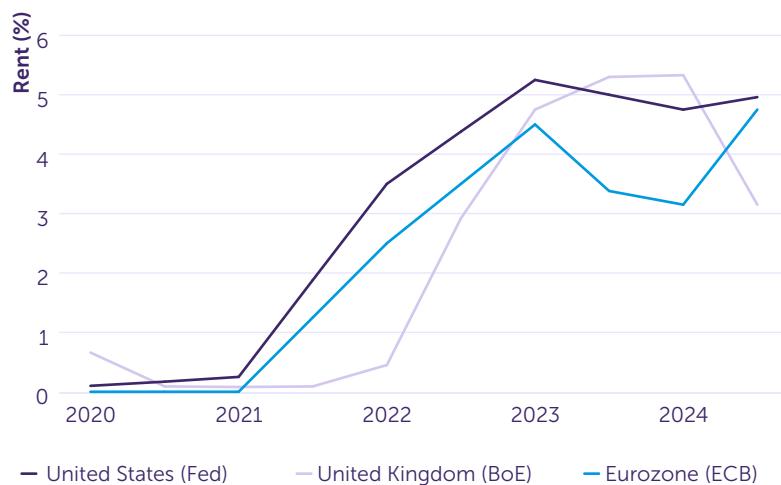


Figure 8: Interest rates 2020-2024 (source: Fed, BoE & ECB)



For comparison, the amount of losses registered by the police in the Netherlands is also included: €75.7 million, which amounts to €5.17 per capita. This is lower than most international extrapolations, which indicates that the actual losses in the Netherlands may be underestimated. The spread between the countries underlines the uncertainty of this method, while also providing a valuable indication of the potential range of damage caused by investment fraud in the Netherlands.

5.1.3 Extrapolation based on amount of losses per capita

To calculate the estimated scale of losses in the Netherlands, we extrapolate the registered amount of losses from the countries in the benchmark comparison to the Dutch situation. To do this, we calculate the amount of losses per capita by dividing the total amount of losses by the number of inhabitants in that country aged 18 years and over. We then multiply this amount of losses per capita by the number of residents in the Netherlands aged 18 years and over.

Table 5 shows that the extrapolation based on this method leads to a wide spread of outcomes. For example, the amount of losses per capita varies from €2.89 in Italy to €17.98 in the United States. When these amounts are applied to the Dutch population, this results in an estimated size of losses of between €42 million (Italy) and €263 million (United States). The United Kingdom and France provide an extrapolation of €259 million and €134 million respectively. Germany comes in at approximately €45 million.

Table 5: Extrapolation overview per capita

Country	Population >18 years	Registered amount of losses per year	Losses per capita	Extrapolation to NL
Netherlands	15 million ⁷⁷	€75.7 million	€5.17	N/a
United States	266 million ⁷⁸	€4.8 billion ⁷⁹	€17.98	€263,219,954
United Kingdom	42 million ⁸⁰	€743 million ⁸¹	€16.76	€258,981,442
France	55 million ⁸²	€500 million (estimate)	€9.17	€134,308,229
Germany	70 million ⁸³	€216 million	€3.10	€45,368,048
Italy	50 million	€145 million	€2.89	€42,285,689
Average				€148,829,720

5.1.4 Extrapolation based on GDP

In addition to the extrapolation based on population size, we also examine the ratio between the total losses registered and the size of that country's GDP. We divide the registered amount of losses by GDP to calculate the damage as a percentage of GDP. We then multiply this percentage by the GDP of the Netherlands.

Table 6 shows that the damage rates vary from 0.0049% (Germany) to 0.0220% (United Kingdom) per country. When these percentages are applied to the Dutch GDP, this results in extrapolations between approximately €53 million (Germany) and €242 million (United Kingdom). The United States and France amount to €209 million and €182 million respectively. Italy yields an extrapolation of approximately €72.5 million.

The average of these extrapolations is approximately €150 million, which is in line with the previously calculated range based on the number of inhabitants. This GDP-based approach provides a macroeconomic perspective and is less sensitive to demographic differences but remains dependent on the quality of the underlying data on losses per country.

It is striking that the amount of losses registered by the police in the Netherlands (€75.7 million) amounts to only 0.0067% of GDP, which is considerably lower than in most other countries, except for Italy and Germany. This suggests that the actual damage in the Netherlands may be underestimated and that additional correction or refinement of the estimate is desirable.

77 14,639,597 inhabitants aged 18 and over (Source: <https://opendata.cbs.nl/#/CBS/nl/dataset/03759ned/table?dl=C51E6>).

78 US Census Bureau - Population Estimates by Age (18+): 1 July 2024.

79 USD/EUR 0.8683 (Exchange rate of 3 September 2025).

80 [Population aged 18 to 64 years - Business Environment Profile Report | IBISWorld](#).

81 GBP/EUR 1.16 (Exchange rate of 12 August 2025).

82 [Age-sex pyramid on 1st of January 2025 | France](#)

83 [Population pyramid: Age structure of Germany from 1950 - 2070.](#)

Table 6: Extrapolation overview of damage as a percentage of GDP

Country	GDP	Registered amount of losses per year	Losses as a percentage of GDP	Extrapolation to NL
Netherlands	€1,100 billion ⁸⁴	€75,7 million	0.0069%	N/A
United States	€25,272 billion ⁸⁵	€4,8 billion	0.0190%	€208,926,876
United Kingdom	€3,375 billion ⁸⁶	€743 million	0.0220%	€242,162,963
France	€3,019 billion ⁸⁷	€500 million	0.0166%	€182,179,530
Germany	€4,447 billion ⁸⁸	€216 million	0.0049%	€53,435,286
Italy	€2,200 billion ⁸⁹	€145 million	0.0066%	€72,500,000
Average				€151.840.931

5.1.5 Limitations

The methodology used to estimate the scale of investment fraud in the Netherlands has several limitations. For this reason, the estimate should be considered an indication of the actual size. It is also a numerical basis for the assumption that investment fraud is an increasing problem in the Netherlands. This estimate therefore informs policymaking, risk assessment and prioritisation of supervision and detection. The methodology is transparent and reproducible but requires continuous updating and refinement as more data becomes available.

The various limitations are described below.

1. Comparability between countries

Although the countries in the benchmark comparison were selected based on similarities in areas such as risk profile, digital infrastructure and economic context, differences remain in definitions of investment fraud, how reports and claims are registered, legal frameworks and supervisory and detection capacity.

⁸⁴ <https://www.cbs.nl/nl-nl/nieuws/2025/19/nederlandse-bbp-per-inwoner-op-vierde-plek-in-eu-in-2024>

⁸⁵ United States Country Information | Ondernemersplein

⁸⁶ United Kingdom Country Information | Ondernemersplein

⁸⁷ France country information | Ondernemersplein

⁸⁸ Germany country information | Ondernemersplein

⁸⁹ <https://ondernemersplein.overheid.nl/landeninformatie/italie/>

2. Quality and completeness of data

Not all countries report loss amounts in the same way. Some figures are based on reports to a specific authority and others are official crime figures. In France, for example, the difference between the losses reported to the AMF (€68 million) and the estimated losses (€500 million) is significant. At the same time, we have also shown that, given the results of the surveys of French investors, both amounts may be a conservative representation of the actual damage. This incompleteness of data makes it difficult to use uniform starting points.

3. Use of extrapolation

The extrapolation based on population and GDP is indicative and assumes a linear relationship between the extent of fraud and demographic or economic factors. In reality, behavioural and cultural factors play a major role, such as trust in financial institutions, investment culture, pension system and digital resilience.

4. Extrapolation based on population

The extrapolation is based on the total adult population, but not every adult invests. A refinement based on the percentage of households that invest would provide a more accurate picture, but reliable and internationally comparable figures on this are lacking.

5. Spread in estimates

The difference between lower and upper limits within the benchmark comparison is large: from approximately €42 million to more than €263 million per year. This makes it difficult to present an unambiguous estimate of losses. The spread is partly the result of the abovementioned limitations. Taking the average and comparing it with the registered damage in the Netherlands increases the reliability of the estimate.

6. Correction for willingness to report

The correction factor for willingness to report is based on limited and partly indirect data. There are no specific figures for the willingness to report investment fraud in the Netherlands. The correction factor used is therefore a rough approximation.