Study

Analysis of the online advertising fraud ecosystem on Meta platforms

December 2025

Austrian Institute of Applied Telecommunications

Disclaimer

Austrian Institute for Applied Telecommunications (ÖIAT)
Ungargasse 64-66/3/404
1030 Vienna

Project lead: Valentine Auer
Authors: Valentine Auer, Lena Müller-Naendrup, Natalie Trell

Executive Summary

Online fraud is a growing global challenge, with social media platforms and search engines becoming key gateways for cybercriminals. This study, commissioned by the Austrian Digital Services Coordinator KommAustria and conducted by the Austrian Institute for Applied Telecommunications (ÖIAT), examines the scale and tactics of fraudulent and problematic online advertising shown to Austrian users on Meta's Facebook and Instagram platforms.

The study aims to: (1) **identify the main fraud schemes** actively advertised on Meta platforms; (2) **estimate the scale of the problem**; and (3) gain insight into **scammers' strategies**, circulating **narratives**, and the specific **targeting of potential victim groups**. In doing so, the study makes an empirical contribution to the assessment of systemic risks as defined in the Digital Services Act (DSA).

Key findings

(1) Extent & Reach: Within just three months, the study identified 634,000 fraudulent or problematic advertisements across eight fraud schemes. Together, these ads generated more than 1 billion impressions across the EU, including approximately 123 million impressions in Austria alone.

Fraud Scheme	Number of Ads	EU Reach	Austria Reach
Online Gambling	448,699	620,572,304	64,790,612
Investment Fraud	83,216	126,665,013	21,961,476
Fake Shops (Brand Imitation)	28,276	65,931,501	2,024,487
Dubious Dietary Supplements	27,171	53,837,455	10,927,574
Job Fraud	18,140	17,265,387	15,757,809
Subscription Scams	17,779	102,402,859	2,891,621
Ghost Stores	9,955	21,407,495	4,751,404
Loan Fraud	805	236,180	121,344
Total	**634,041**	**1,008,318,194**	**123,226,327**

Figures are conservative lower-bound based only on ads identified through keyword searches.

(2) Deletion Rates & Ad Lifespan: 62.4% of all identified ads had already been removed by Meta at the time of data collection, indicating that the platform does detect and take action against some fraudulent content. At the same time, the identified ads tended to remain active only for very short periods, often just a few days or even hours, while new ads continued to appear.

(3) Manipulation Strategies: Across all eight fraud schemes, the qualitative analysis identified recurring manipulation strategies employed to lure victims, such as those outlined below:

DECEPTIVE DESIGN

Fraudulent ads systematically employ manipulative design patterns, including artificial scarcity (e.g. 'Only 2 items left'), manufactured urgency (e.g. 'Today only'), confirmshaming (e.g. framing inaction as a personal failure), and interface interference (e.g. prominent call-to-action buttons alongside barely visible exit options or links to terms-and-conditions).

CURIOSITY GAP

Ads deliberately create knowledge gaps designed to trigger irresistible impulses to click, for example through claims such as 'Are you smarter than the average?' (subscription scams), supposed insider knowledge about financial markets (investment fraud), or 'He carried a secret no one should know' (dietary supplements).

ABUSE OF ESTABLISHED TRUST ANCHORS

Well-known individuals (politicians, celebrities, entrepreneurs), media brands, and established institutions are systematically impersonated. In some cases, AI-generated deepfakes are used to fabricate video endorsements purportedly made by public figures.

EXPLOITATION OF SITUATIONAL VULNERABILITY

While fraudulent advertisers rarely apply explicit demographic targeting filters based on age or gender, the qualitative analysis reveals that fraudulent ads are designed to reach people in specific, often vulnerable, life situations. These include, for example, individuals experiencing financial distress (credit fraud), those with health concerns or chronic illnesses (dietary supplements), job seekers (job fraud), or people looking for passive income opportunities (investment fraud).

Compliance gaps on Meta

The DSA requires Very Large Online Platforms (VLOPs) such as Meta to provide transparency instruments that enable the independent verification of advertising. The Meta Ad Library is the central instrument intended to fulfil this obligation. The study documented structural deficits that limit the traceability and auditability of fraudulent ads.

(1) Opaque Advertiser Identity: Article 39 of the DSA requires the paying party behind each ad to be disclosed in the Ad Library. In practice, however, the 'payer' field is a free-text entry that Meta does not verify and that fraudsters systematically misuse. The dataset contains entries such as random digit strings, arbitrary character sequences, misappropriated brand names, and even 'facebook' itself listed as the payer for fraudulent ads.

(2) Disappearing Ads: Article 39 of the DSA requires VLOPs to retain ad records in the public repository for at least one year, even after an ad is no longer active. The study found that previously documented ads could no longer be found in later searches.

(3) Continued Ad Activity on Supposedly Disabled Accounts: Many identified ads were already marked as removed by Meta ('This ad was run by an account or Page we later disabled for not following our Advertising Standards'). However, our observation revealed that new ads were later placed under the same Page ID, despite the supposed deactivation of the account. This goes beyond the common practice of fraudsters creating new accounts under slightly modified names.

(4) Ads Not Retrievable via Text Search: Relevant fraudulent ads were found to be unsearchable by their text content, despite being present in the Ad Library when accessed via the account name. As a result, several well-known celebrity names had to be removed from the study's keyword lists, as text-based queries produced no results even though the research team knew that relevant ads existed.

Systemic Risk under the DSA

The study shows that the transparency mechanisms provided under the Digital Services Act offer important entry points for regulatory oversight. The ability to systematically collect and analyse advertisements enables evidence-based documentation of the problem, which can serve as a basis for enforcement action.

At the same time, the findings demonstrate that merely providing an Ad Library is not sufficient to effectively address fraudulent advertising. The study highlights that fraudulent and problematic advertising on Meta platforms is not a marginal phenomenon, but constitutes a systemic risk under the DSA, as it spans eight thematically distinct fraud schemes involving large numbers of ads.

The DSA requires VLOPs not only to identify systemic risks, but also to mitigate them through appropriate measures. The compliance gaps documented in this study indicate that current measures against fraudulent advertising fall short of this obligation.

Contents

Introduction

The damage caused by online fraud has been increasing internationally for years. The Global Anti-Scam Alliance (GASA) documents worldwide scam losses of around $442 billion for 2025, (Abraham, 2025) but estimates actual losses between $442 billion and $1 trillion (Vorster, 2026). Online fraud is also a central problem in Austria: According to the Cybercrime Report, 62,328 cybercrime offences were reported in 2024. While this figure has fallen slightly for the first time in a decade, internet fraud offences remain high, accounting for around half of all cybercrime offences, with 31,768 cases (Bundesministerium für Inneres, 2025).

The increasing shift of fraud into the digital space is not only due to the potential anonymisation of identities and financial flows. A key factor is also the ability to reach a large number of potential victims with a low use of resources. Offenders also face the challenge of promoting their fraudulent offers and bringing them to potential victims. To this end, they are increasingly making use of the **advertising opportunities offered by large online platforms.** Experts in the field of fraud prevention and detection report that advertisements have become an essential gateway for online fraud (vgl. Federal Trade Commission, 2023; OCCRP, 2025).

In particular, on large online platforms (VLOPs) and very large online search engines (VLOSEs) regulated by the Digital Services Act (DSA), fraudulent content can not only be disseminated on a mass scale but also tailored to target groups based on demographic characteristics, interests or behavioural data. A **large number of different online cases are advertised –** from clearly illegal fraud schemes such as dubious investment offers or fake shops to problematic practices such as misleading subscription traps or ghost stores, which mislead users specifically about origin, quality or legal framework conditions.

While the use of online advertising for fraudulent purposes is known in principle, recent investigative research provides for the first time an insight into the extent and **structural anchoring of this problem in the advertising ecosystem of large platforms.** Revelations from Meta's internal documents suggest that fraudulent advertisements on Meta services are not only a marginal phenomenon but are a significant part of the advertising ecosystem. According to internal Meta documents leaked to Reuters, in 2024 alone, Meta projected around $16 billion of ads that lead to scams or the sale of illicit goods – equivalent to about 10% of total advertising revenue. Meta responded to the figures by stating that they were estimates to carry out planning, including anti-fraud planning (Horwitz, 2025a). However, just a short time later, further Reuters research by Meta

shows planned strategies to make it more difficult for regulators to identify fraudulent advertisements (Horwitz, 2025b).

This means **that online advertising plays a key role in the context of online fraud,** not only in enabling it, but also in combating it. This is because, unlike many other actors in the fraud value chain, the platforms on which this advertising is displayed are identifiable and regulatorily tangible.

Against this background, the present study, commissioned by KommAustria as Digital Services Coordinator (DSC), investigates **fraudulent and problematic online advertising** that is displayed to Austrian users on the **Meta services Facebook and Instagram.** The aim of the study is to identify key fraud schemes, to approximate the extent of the problem and to gain insights into perpetrator strategies, prevailing narratives and forms of targeting. The study thus makes an empirical contribution to the assessment of systemic risks within the meaning of the Digital Services Act and provides an evidence-based basis for regulatory, policy and preventive measures.

1. Background and research questions

1.1. Systemic risk under the Digital Services Act

The **Digital Services Act (DSA),** which has been directly applicable to all digital services since February 2024, requires very large online platforms (VLOPs) and online search engines (VLOSEs) to tackle illegal content and address risks arising from the operation of their services. Article 34 of the DSA (EU 2022/2065) requires VLOPs and VLOSEs to regularly identify, analyse and assess risks arising from the use of the respective services. Article 35 of the DSA (EU 2022/2065) requires it to take appropriate, proportionate and effective measures to minimise the risks identified.

Systemic risks within the meaning of the DSA are characterised by the fact that they are not limited to individual cases but arise from structural characteristics of the design and operation of VLOPs and VLOSEs. According to Article 34 of the DSA (EU 2022/2065), these include, inter alia, risks amplified by algorithmic recommendation systems, content moderation systems or providers' data-related practices. It also highlights 'advertising selection and display systems', recognising the advertising ecosystem itself as a potential source of systemic risk.

As a central part of the business model of large platforms, which is actively managed and monetised, the perpetrators in the fraud ecosystem benefit from the same mechanisms through advertising that make legitimate advertising efficient: high reach, personalized targeting and automated playouts.

In order to strengthen transparency and accountability, in particular in the area of advertisements, Article 39 (EU 2022/2065) of the DSA requires VLOPs and VLOSEs **to make publicly available ad libraries.** For each ad placed on the platform, the advertising content, the legal or natural person who placed or financed the advertising, the period of placement and key figures for targeting must be disclosed, among other things. Thus, the advertising libraries enable third parties to systematically analyse and document advertisements and represent a central starting point to empirically investigate the magnitude and structure of fraudulent advertising on large platforms.

Initial surveys by the Austrian Institute for Applied Telecommunications (ÖIAT) and the ÖIAT Watchlist Internet initiative[1] show that there is considerable advertising in Austria for various forms of fraud and problematic offers:

[1] The Watchlist Internet is the largest online platform for Internet fraud in the German-speaking world.

- **Investment fraud:** between January and April 2024, 9,000 advertisements with a daily reach of around 200,000 (Austria) were identified on Meta platforms, in which the names and images of 25 Austrian celebrities are misused (Watchlist Internet, 2024).
- **Ghost Stores:** Between January and April 2025, 36,000 ads were identified on Meta platforms purporting to be a local family business. The online shops infringe applicable consumer protection and competition law provisions, inter alia because their actual registered office is in another EU country and consumers are deliberately misled (Watchlist Internet, 2025b).
- **Dubious offers for dietary supplements:** Between January and July 2025, 4,632 problematic advertisements with a reach of over 21.5 million were documented on Meta platforms, in which in particular the names and images of well-known doctors and health experts were misused. Particularly problematic was the spread of disinformation and the erosion of trust in evidence-based medicine and public institutions (Auer et al., 2025).

Comparable findings are also available at international level: As early as 2022, the British consumer organisation Which? Advertisements for dubious and fraudulent investment platforms (Which, 2022). The European non-profit organisation AI Forensics identified around 46,000 advertisements for unauthorised medicines or misleading health promises across the EU, which were distributed to European users more than 292 million times (Bouchand et al., 2025) in total.

These surveys provide evidence that fraudulent and problematic online advertising **is not a marginal phenomenon,** but potentially a systemic risk within the meaning of the Digital Services Act. This study builds on this work and aims to analyse and document the fraud ecosystem on Meta platforms in an exemplary way.

1.2. Questions

Against this background, the aim of the study is to investigate and document the fraud ecosystem exemplarily on Meta platforms (Facebook, Instagram) in order to highlight the systemic risks of fraudulent advertising. Specifically, the study is intended to provide evidence-based insights into the following topics and questions:

Identification of fraud schemes and keywords

(1) In which fraud schemes are advertisements used?

(2) Which keywords are suitable for identifying fraudulent ads?

Quantitative collection of advertisements

(3) How many fraudulent ads can be found per scam scheme with the identified keywords?

(4) When and how long are the ads active?

(5) What is the reach of the ads per scam scheme?

(6) To which groups of people are the ads displayed?

(7) Who are advertisers, beneficiaries and payers? What patterns can be identified?

(8) Which types of fraud achieve the highest ranges?

Qualitative collection of advertisements

(9) What strategies and narratives are used to promote the fraud traps?

(10) Which target groups are addressed at a content level?

(11) What role do AI/deepfakes play in promoting fraud traps?

(12) What other infrastructure is used when forwarding ads?

(13) Which offender strategies for circumventing security measures and content moderation are observable?

(14) What vulnerabilities have been observed on Meta platform services?

1.3. Limitations

Despite the systematic approach to the collection and analysis of fraudulent and problematic online advertising on Meta platforms, the present study has limited aspects to consider in the subsequent interpretation of the results.

Incomplete population

The study does not seek to fully capture advertisements in individual scam schemes. Such **a full survey** would **not be methodologically feasible,** since an overview of the population of all advertisements is missing. The method of iterative testing of certain keywords particularly ads with recognizable patterns. Fraud ads without eye-catching keywords go undetected, meaning the actual numbers will be significantly higher.

False negatives can also occur within a keyword for various reasons: Ads can go undetected, on the one hand, because fraudulent actors develop tactics and strategies to bypass detection and detection systems. On the other hand, according to internal documents, Meta is itself supposed to use methods that make fraudulent advertising more difficult to find (Horwitz, 2025b). In addition, both the number of search terms and the reporting period had to be reduced in order not to exceed the query limit provided by Meta. The aim of the study is therefore to provide an insight into the magnitude and structural features of the problem.

Focus on German-speaking countries

A large part of the keywords used for the study are **in German** or tailored to the **regional context of the German-speaking area** (e.g. names of well-known personalities from Germany or Austria). Although Meta gives the ranges for the entire EU, in most cases this information refers mainly to the German-speaking countries. For other EU countries, the results are therefore not meaningful.

Limitation by data situation

Although the DSA imposes transparency and ad library obligations on VLOPs such as Meta, there are structural limitations over which the study authors have no influence. The **accuracy, precision and completeness** of the data collected depends on the information provided by Meta, and incompleteness or inaccuracies in such data may affect the analysis. The figures identified in this study should therefore be understood as approximate values based on the data made available by the Meta Ad Library, the accuracy of which cannot be independently verified.

Consideration of grey areas and problematic content

In addition to advertisements for clearly criminally relevant fraud, the study also includes dubious and misleading advertisements that are published with the aim of deceiving users and inducing them

to make a decision that is not advantageous to them. Since the DSA is not only directed against clearly illegal content, but also against manipulative techniques and against risks for consumer rights on platforms, these **grey areas of content** are also relevant. This expanded focus deepens the analytical horizon, but at the same time means that not every recorded case is clearly relevant to criminal law, but rather the collection encompasses a wide range of problematic offers.

2. Identification of fraud schemes and keywords

2.1. Methodological approach

The **identification of relevant fraud schemes forms** the basis of the investigation and was carried out on the basis of two approaches:

(1) Consumer messages to the Watchlist Internet:

Fraud schemes such as investment fraud or the promotion of dubious dietary supplement offers are regularly reported by consumers to the Watchlist Internet and are therefore known as relevant phenomena, in some cases including keywords. These messages form a central basis for the selection of the schemes to be investigated.

(2) Exploratory testing of possible further fraud schemes

For topics that were not yet known by news or media reports, possible matching search terms in the Meta ad library were exploratively tested for relevant results. This approach allowed the identification of additional fraud schemes.

Relevant **keywords were identified for each fraud scheme identified.** Keywords correspond to text phrases that are typically used in fraudulent advertisements – such as product names, promises or celebrity names – and can be used to find relevant advertisements in the ad library. An iterative process was used to identify the keywords:

- Initial keywords were entered into the Meta ad library based on known or newly identified fraud patterns.
- Initial search results were analysed with regard to their fraudulent intent and associated advertisers were identified.
- Additional keywords were identified by the search results, but also by the advertisers and their other ads.

- This process was repeated until saturation was achieved.

2.2. Identified scam schemes & keywords

The study identified eight fraud schemes involving large-scale use of ads via Meta platforms. For each scheme, a detailed analysis was carried out, which in particular provides quantitative insights into the respective fraud ecosystem. The identified scam schemes and keywords are[2] outlined below.

2.2.1. Subscription traps

Subscription traps are an established scam scheme in which websites or online services allegedly offer free or very cheap services. It obscures the fact that those affected – mostly unnoticed – **subscribe to a paid subscription.** The obligation to pay and the duration of the subscription 'are either not presented at all, insufficiently or deliberately misleading. (ÖIAT, 2025) The advertised services typically include low-risk digital services such as IQ testing.

Keywords
'ADHD is Not Laziness'
'Are you smarter than the average German'
'How high is your IQ score'
'if you can solve these 15 questions'
'stop wasting time on 10,000 steps a day'
'Think you're smarter than the average American'
'Train your dog like a professional'
'Change your body, your energy, your life.'
'What is your intelligence type'

2.2.2. Investment fraud

Investment fraud refers to a form of financial fraud in which **supposedly lucrative investment opportunities** are advertised in order to entice those affected to deposit money. In fact, however, the offers serve exclusively to obtain funds from those affected. There is no real investment. (Watchlist Internet, 2022b).

Keywords
'Hoss & Hopf'
'We don't take money – you get the best tips for free.'
'AI trading'

[2] Keywords in quotation marks are searched as exact word order, keywords without quotation marks as free search. The spelling of the keywords in this table follows the search method used.

'ChatGPT Shares'
'Gerald Hörhan'
'Many people don't know how to choose stocks'
'Double your assets on the stock exchange'
'Austrians earn'
'Herbert Kickl'
'For Austrian citizens only'
'The strongest German shares for 2026'
'Digital trends are becoming more and more important'
'Your top 3 stock picks for up to +60% potential'
'Hans Jörg Schelling'
'The new platform has already jeopardised the efficiency of the banking system'
'Armin Wolf'
'Expert advice on difficult investments'

2.2.3. Credit fraud

Credit fraud occurs when supposedly cheap credit, loan or financing offers are advertised without ever intending to actually lend. The aim of the perpetrators is to persuade those affected to **make advance payments** (Watchlist Internet, 2022a).

Keywords
'Private loans without paperwork'
'despite Schufa'
'Check credit status online'
'Learn immediately what credit options you have.'
'Apply for a loan online now and have it paid out immediately!'
'Request card'
'Do you need cash fast?'
'Are you creditable?'
'Even highly indebted people can get loans!'
'Immediate credit without proof of income in Austria'
'Financial discharge sought?'
'You can also get a loan with debt!'

2.2.4. Job fraud

Advertisements advertise **alleged job offers which** in reality do not have a legal profit-making purpose. Instead of regular employment, the aim of this scam scheme is to engage people in criminal activities (e.g. as money mule), obtain sensitive data or induce them to make advance payments. There is no remuneration for the advertised activity (Watchlist Internet, 2025a). Particularly often, simple, location-independent activities without the necessary prior knowledge and with flexible working hours are advertised.

Keywords

'No experience required'
talentway-at.com
'that the WhatsApp number you provided is correct'
'The part-time job I found through this website'
'No experience needed'
'We're hiring - start your remote career today!'
'High salary and flexible working hours! '
'Make your passion your profession and shape your own career path!'
'Zzx0'
We are looking for new colleagues - start now
'Are you looking for a Christmas job? '
WorkAnchor Austria
'Apply now and celebrate Christmas'
'Join us and celebrate the warmest Christmas together'
'Experience is not required, everyone is welcome! '

2.2.5. Untrustworthy dietary supplement offers

Dubious dietary supplements are often advertised with **unapproved promises of action** that violate the Health Claims Regulation (EC 1924/2006). In order to market the products via social media, the names and faces of well-known doctors, health experts or established brand names (e.g. dm or Die Höhle der Löwen) are often misused. The products supplied are often ineffective, overpriced or even harmful to health – or nothing at all is delivered (Auer et al., 2025).

Keywords
'Höhle der Löwen'
'Get rid of your fatty liver'
Prostate problems
We guarantee that you will lose 10 kg in 3 weeks.
Ozempil
Hirschhausen
Cleans the blood vessels
Meryn
Drosten
Tobias Weigl
'Try this evening ritual'
Thomas Binder
Klaus Richter
'Müller Wohlfahrt'

2.2.6. Ghost stores

Ghost stores are problematic online shops that usually pretend to be local, family-run shops based in Austria or Germany and sell high-quality goods. In fact, they are online shops that ship **low-quality goods from other EU countries** – or deliver nothing at all. Consumer protection regulations are often not complied with.

Keywords
Lena boutique
Elle Weber
Fashion house Berfeld
Moser Vienna
Muller Graz
Mirella fashion house
Vienna fashion house
Schneider Salzburg
Thera Boutique
Weber atelier
Greta Helene
Velser Vienna
Werner & Martha

2.2.7. Fake shops (brand imitation)

Fake shops pretend to be legitimate online shops. If you order there, you will receive either none at all or a completely different product than the ordered one. The focus of this research was on **fake shops that imitate well-known brands** by abusing their names and logos and mimicking the website.

Keywords
lidl discount
Hofer Garmin
swarovski hofer
'Bosch sale'
'birkenstock outlet'
hofer gopro
Birkenstock sale
Hofer Black Friday sale
Swarovski 130.
swarovski mega sale
swarovski billa

2.2.8. Online gambling

Gambling is strictly regulated in Austria: only operators with a valid licence – which are mainly held by the Austrian Lotteries and Casino Austria AG[3] – are allowed to offer gambling offers. However, social media promotes massively **fraudulent casino apps and mini-gambling** such as 'Plinko' or 'Chicken Road' – fake apps where winnings are not repayable in the first place, credit card data is stolen or further deposits are blackmailed. Since some tens of thousands of ads are shown per

[3] https://www.bmf.gv.at/themen/gluecksspiel-spielerschutz/gesetzliche-grundlagen-gluecksspiel/konzessionaere-ausspielbewilligte.html

week in this area and Meta limits the number of requests within a query period, the keyword selection here was deliberately kept small.

Keywords
Casino Austria
Casinos Austria
Plinko
Chicken Road

3. Quantitative collection of advertisements

3.1. Methodological approach

For the detailed analysis, a crawler connected to the API of the Meta ad library was used. The survey covered the period from **September to November 2025.**[4]

The identified keywords per scam scheme were passed to the crawler and the results cleaned up by first removing duplicate entries using the unique Ad ID for each ad. Subsequently, the data was checked for legitimacy in a manual screening procedure, in particular by screening page name, URL and ad text. Ads that clearly came from legitimate companies were removed from the record. Due to the manual nature of this process, isolated misclassifications – both false-positive and false-negative – cannot be ruled out.

The adjusted data were analysed to produce a descriptive statistic per fraud scheme. In order to answer the questions outlined above, the raw data were converted into multidimensional pivot tables, which enabled a systematic aggregation of the different key figures.

Specifically, analyses were carried out on the following key figures:

- **Number of ads**; includes those ads with unique Ad ID
- **Ad Runtime**; includes the time that advertisers play an ad
- **Deletion rate**; includes the proportion of ads that have already been deleted by Meta – either because the underlying account (advertiser) has been disabled due to violations of the Advertising Guidelines or because the content itself violates the Advertising Guidelines
- **Targeting by age, gender and location**; includes information from advertisers on whether certain target groups are deliberately included or excluded when displaying ads
- **Range**[5]; includes:
    - the reach within the EU (mainly German-speaking countries are relevant due to the selection of keywords)
    - the overall coverage in Austria, broken down by gender and age groups
- **Advertisers;** includes the Facebook page or account that served the advertisement

[4] The period refers to whether impressions of the ad were recorded in this date range.
[5] In this study, reach refers to the number of accounts reached per ad shown by Meta. By merging multiple ads, it is possible for individual accounts to be included multiple times if they have seen different ads. The key figure is an estimate.

- **Beneficiaries and payers**; includes a person identified by advertisers as a beneficiary or payer
- **Keywords**; includes the share of a keyword in all identified advertisements

3.2. Overall overview: ranges, deletion rates, targeting

3.2.1. Number of ads & reach

Over the eight fraud schemes, a total of **634,000 fraudulent and problematic advertisements were identified within** 3 months, which were displayed 1 billion times to users within the EU and almost 123 million times to users in Austria.

Looking at the figures according to fraud schemes, there are clear differences – both in the number of ads and in their reach. Online gambling accounts for the most significant numbers, followed by investment fraud. At the bottom of the list, with the lowest number of ads, is credit fraud.

Fraud scheme	Number of Ads	Scope of EU	Range AT
Online gambling	448.699	620.572.304	64.790.612
Investment fraud	83.216	126.665.013	21.961.476
Supplements	27.171	53.837.455	10.927.574
Fake shops	28.276	65.931.501	2.024.487
Job fraud	18.140	17.265.387	15.757.809
Subscription traps	17.779	102.402.859	2.891.621
Ghost stores	9.955	21.407.495	4.751.404
Credit fraud	805	236.180	121.344
Overall	**634.041**	**1.008.318.194**	**123.226.327**

Table1: Number of ads and reach per scam scheme

3.2.2. High deletion rates

The high dynamics of the advertisements are striking: **62.4%** of all identified advertisements were already **removed by Meta due to a violation during the survey period.** This can be seen by an indication that the account behind it was blocked due to violations of the advertising guidelines (46.9% of all advertisements) or, less frequently, the content itself violated the advertising guidelines (16.2%).

At the same time, the fraudulent actors also rely on **short ad runtimes** of only a few days or even hours (see 3.3.2 Short ad runtimes). Instead, it is set to many and fast-changing ads. It is to be assumed that the moderation on the part of the platform is to be avoided or that new not yet discovered advertisements replace the moderated and removed advertisements.

3.2.3. Broad demographic target group approach

If you place an ad on Meta, you can play it out specifically to certain target groups. Among other things, demographics, interests, behaviors or *lookalike audiences* (i.e. users who resemble existing customers) can be included or excluded. Even if no specific targeting metrics are specified during ad creation, Meta's data-driven algorithms can automatically find relevant users via *Advantage+ Audience*[6].

In the ad library, any targeting is only displayed according to **demographic indicators (age, gender, location).** However, the analysis shows that fraudulent actors hardly act in a targeted manner according to these parameters. The location is still most likely to be used: Germany and Austria were actively included as the target region in 36% of all advertisements. In terms of gender, 93% were played to all genders, the remaining 7% targeted to men, and 64% of ads used the standard age of 18-65 as their target group.

The evaluation of the reach data for Austria provides insights into which target groups the ads have actually reached. It shows that, overall, fraudulent and problematic ads address a **broad demographic spectrum.** Male users accounted for 53.5% of the reach, while female users accounted for 44.6%, indicating a slight overrepresentation of men.

The age distribution also points to a broad approach, only a slight **tendency towards a more purchasing target group** can be seen, since the largest proportion of users are of middle and older working age: the age groups 35-44 years (22.9%) and 45-54 years (22.0%) together make up almost half of the persons reached. Younger age groups were reached less frequently, only 8.7% of 18-24 year olds and 11.7% of 25-34 year olds were reached. The following detailed analyses per fraud scheme show clearer targeting in some areas, both gender and age.

3.3. Structural similarities in the fraud ecosystem

The analysis of the various fraud schemes reveals structural similarities across all topics, which point to both systematic strategies of the advertisers and compliance gaps at Meta itself.

[6] https://www.facebook.com/business/help/744354708981227?id=2469097953376494

3.3.1. Non-transparency of paying persons

Article 39 of the DSA (EU 2022/2065) requires the ad library to show 'the natural or legal person who paid for the advertising'. This **transparency obligation** is intended to ensure traceability with regard to the persons responsible for the advertisements.

However, the detailed analyses show that, across fraud schemes, neither the names of the advertisers nor those of the payers actually provide information about the persons or organisations responsible. The field for the paying persons is a free field ('beneficiary and payer') and can be filled accordingly. As our datasets show, this is actually used – among the payers, for example:

- Number series such as '369', '1' or '222'
- Arbitrary letter series such as 'SMB' or 'wsdggggg'
- Abuse of brand names such as 'Die Höhle der Löwen' (especially in the case of food supplements), often even 'facebook' itself is indicated as a payer
- Names of people who are either invented or abused without their knowledge
- Names of fake companies (e.g. in the case of the Ghost Stores 'Lena Boutique')

The example from the analysis of the fraud scheme Job fraud is particularly striking: in this type of fraud alone, a payer with the name or rather the number '1' is responsible for 11,712 advertisements with an EU-wide reach of almost 600,000.

This shows that the **transparency provided for in the DSA is not guaranteed in practice** and that this compliance gap is structurally used by advertisers to hinder traceability. In addition, there is a high degree of fragmentation with countless different numbers, which makes it difficult to identify organized structures.

3.3.2. Short ad runtimes

Another consistent pattern across all investigated scam schemes is the extremely short runtime of the ads. A large proportion of fraudulent advertisements are **only active for a few hours to a maximum of a few days**. For some types of fraud, over two-thirds of ads were active for less than a day.

It can be assumed that this strategy serves the purpose of targeted circumvention of security measures and content moderation. The high number of short-lived ads makes it more difficult for both automated and manual review systems to identify and remove problematic content in a timely

manner. The advertisers rely on **quantity instead of long-term runtime** and achieve considerable overall reach through the permanent re-engineering despite short runtimes.

3.4. Subscription traps

BASIC DATA

Advertisements: 17,779

Range EU: 102.402.859

Range Austria: 2,891,621

HIGHLIGHTS

Lowest deletion rate of all fraud schemes

Long runtime

High keyword concentration

Despite the moderate number of advertisements compared to other fraud schemes, the identified ads that lead to subscription traps reached a high reach, also in Austria. This can be explained above all by the **low deletion rate of Meta (4.5%)** and the simultaneously **long ad runtime:** Ads that are played undetected for longer automatically reach more users. The low deletion rate also suggests that these advertising formats often operate in a **regulatory grey area** between misleading and clearly fraudulent advertising.

At the same time, the analysis of keywords shows a high concentration of only a few keywords: Two keywords cover over 80% of all identified ads:

- 'ADHD is Not Laziness' (50.4%)
- 'How high is your IQ score' (30.7%)

3.4.1. Targeting by gender, age and location

Advertisers did not target subscription traps based on gender, age or location. The range analysis for Austria shows that **male users are slightly overrepresented** (51.8% vs. 45.7% female). In terms of age, reach is relatively evenly spread across all age groups, with the highest proportions at 35-44 (29.6%) and 45-54 (26.8%), while younger (18-24 years, 4.1%) and older users (65+, 9.8%) are less reached.

Category	Reach	Proportion
Gender		
female	1.320.781	45,7%
male	1.498.763	51,8%
unknown	72.077	2,5%
Ages		
18-24 years	118.464	4,1%
25-34 years	331.441	11,5%
35-44 years	856.859	29,6%
45-54 years	774.475	26,8%
55-64 years	526.018	18,2%
65+ years	284.324	9,8%
unknown	40	0,0%

Table 2: Subscription traps – coverage by gender and age groups

3.4.2. Advertisers

Advertisers' analysis of subscription traps shows a highly fragmented picture: there are a variety of different accounts using either **generic names, references to the advertised offer** (e.g. IQ tests or dog training) or **apparent company names.** A large part of the ads is concentrated on a few advertisers: around 70% of the ads come from only three accounts.

Advertisers	Number of ads
Betty Holland	5.110
International IQ Test	4.757
Alison Todd	2.600
My IQ	623
Innerly	426
Jacob Holland	412
Testora	409
Max – Your Dog Training Coach	240
Today is the day	154
Cerebrum IQ	153

Table 3: Subscription traps – Ads by advertiser

3.5. Investment fraud

BASIC DATA

Advertisements: 83.216

Reach within the EU: 126,665.013

Range in Austria: 21,961,476

HIGHLIGHTS

High deletion rate

High keyword concentration

70% of the reach in Austria was for men

Investment fraud takes second place after online gambling in terms of the number of advertisements and reach within the fraud schemes investigated. At the same time, this category has a **high deletion rate (78.2%).** Keyword analysis shows a strong dominance of fewer terms. Four keywords cover over 90% of all ads ('Hoss & Hopf', 'We don't take money – you get the best tips completely free', 'AI trading', 'ChatGPT shares').

3.5.1. Targeting by gender, age and location

In the area of investment fraud, no specific targeting was carried out by the advertisers. Geographically, the focus is on Germany and Austria (40% of the ads), to a lesser extent Belgium and Luxembourg were included as target regions.

The analysis of the reach in Austria shows a clear focus on **male users (71%).** The age distribution, on the other hand, is relatively balanced, with a slight focus on middle to older age groups.

Category	Reach	Proportion
Gender		
female	5.997.786	27%
male	15.595.367	71%
unknown	368.323	2%
Ages		
18-24 years	2.066.159	9%
25-34 years	3.102.779	14%
35-44 years	4.790.038	22%
45-54 years	4.608.649	21%
55-64 years	4.265.388	19%
65+ years	3.128.364	14%
unknown	99	0%

Table 4: Investment fraud – coverage by gender and age groups

3.5.2. Advertisers

Advertisers use **trend terms, well-known company names or celebrity names** to convey seriousness. The focus on a few key players is striking: 'Trade-Republic Analyze' posted almost 16,000 ads, followed by several accounts around 'Hoss & Hopf'.

advertisers	Number of Advertisements
Trade-Republic analysis	15.999
Hoss & Hopf	3.836
T-R	3.030
Hoss	2.979
Philip Hopf	2.477
Chat gpt 5	1.608
Hoss & Hopf	1.462
Gerald Hö rhan	1.282
Fxalgo Media	1.105
Cooper Phillip	929

Table 5: Investment fraud – Ads by advertiser

3.6. Credit fraud

BASIC DATA

Advertisements: 805

Range EU: 236.180

Range Austria: 121.344

HIGHLIGHTS

Comparatively low deletion rate

Austria accounts for a large share of the reach

Austrian reach is reserved for people over 55 years of age

Credit fraud has the **lowest number of advertisements compared to** other fraud schemes. These comparatively low numbers may be due to methodological reasons, since at the beginning of the survey there was still no reliable knowledge about which keywords are suitable for identification and with which narratives or terms the fraud scheme is advertised. The keyword 'private loans without paperwork' dominated with 50.3%. Other typical keywords such as 'despite Schufa' make it clear that fraudulent actors are targeting people in financial distress. What is also striking is a **low deletion rate of 11.8%** compared to the other fraud schemes.

3.6.1. Targeting by gender, age and location

Advertisers did not target specifically by gender or age. Geographic targeting shows a strong focus on German-speaking countries: the vast majority of ads (over 80%) target **Austria, Germany and Luxembourg,** with some ads including Sweden.

Nevertheless, at 51.4%, the proportion of users reached in Austria is significantly above the average of 12.2%. The range analysis for Austria also shows that 67.4% of the users reached are male. In terms of age distribution, the focus is on older target groups: the 55-64 age group represents the largest proportion with 27.3%, followed by 65+ with 25.7%. Together, **53% of the reach is for people over the age of 55.**

Category	Reach	Proportion
Gender		
female	38.360	32%
male	81.799	67%
unknown	1.185	1%
Ages		
18-24 years	13.496	11%
25-34 years	2.518	2%
35-44 years	15.873	13%
45-54 years	25.194	21%
55-64 years	33.072	27%
65+ years	31.188	26%
unknown	3	0%

Table 6: Credit fraud – coverage by gender and age groups

3.6.2. Advertisers

The analysis of advertisers shows a highly fragmented picture with a variety of different accounts with generic names.

Advertisers	Number of ads
F&M GLOBAL BRANDS SERVICOS LTDA	323
Media Hub	147
BLOG DIGITAL	79
F & M GLOBAL BRANDS	30
OBMedia LLC	20
NewsTrends	18
AG MARKETING DIGITAL LTDA	16
RL Media Sp z oo Sp k	15
Eduarda Oliveira	14

Table 7: Credit fraud – Ads by advertiser

3.7. Job fraud

BASIC DATA

Advertisements: 18.140

Reach EU: 17.265.387

Reach Austria: 15,757,809

HIGHLIGHTS

Very strong focus on Austria with 91.3% of total EU reach

High deletion rate & high keyword density

Mostly reached by persons of working age

Job fraud shows by far the highest proportion of all fraud schemes in Austria: 91.3% of the EU-wide reach is attributable to Austrian users. This indicates a very targeted campaign orientation towards Austria. At the same time, we see both a **high deletion rate of 78%** and a high keyword density – the keyword 'no experience needed' accounts for 89%.

3.7.1. Targeting by gender, age and location

Advertisers hardly targeted by age or gender. Unlike other fraud schemes, however, there is a much stronger focus on the **Austrian market:** Austria accounts for 15.8 million of the total EU reach

of 17.3 million. Ads with very specific local targeting (e.g. individual cities) or wider geographical regions (EU, EEA) were only occasionally identified.

The range analysis for Austria also shows a focus on **persons of working age:** the age group 35-44 represents the largest proportion with 33.2%, followed by 45-54 years with 26.7%. In total, 50.7% of the reach is for people aged 45 and over. In addition, 62% of the users reached are female.

Category	Reach	Proportion
Gender		
female	9.847.003	62%
male	5.557.742	35%
unknown	353.064	2%
Ages		
18-24 years	344.286	2%
25-34 years	2.186.612	14%
35-44 years	5.236.441	33%
45-54 years	4.213.032	27%
55-64 years	2.579.193	16%
65+ years	1.197.729	8%
unknown	516	0%

Table 8: Job fraud – coverage by gender and age groups

3.7.2. Advertisers

In the field of job fraud, people rely heavily on **unknown names.** Since the majority of these pages were no longer online at the end of December, it is not clear whether they are compromised user accounts or accounts with fake personas created specifically for the fraud meshes.

Advertisers	Number of ads
Natalia Scully Brady	1.119
Brandon Ryan McDaniel	434
Smith Roy Peffley	366
Grace Ruggeri Emily	363
Jr. Deanna dagger	312
Manaayy Conomon Collazo	251
Tabitha Onions2	217
Miller Malik Mills	200
Elwell Certesio Karma	200
Katie Seelig Barbara	199

Table 9: Job fraud – Ads by advertiser

3.8. Untrustworthy dietary supplement offers

BASIC DATA

Advertisements: 27,171

Reach EU: 53.837.455

Reach Austria: 10.927.574

HIGHLIGHTS

Massive abuse of the 'Höhle der Löwen' programme

74% of people over the age of 45

Women in reach overrepresented

With an **EU-wide reach of more than 53 million,** ungodly dietary supplement offers reach a very large number of users. The deletion rate of 52% shows that Meta recognises about half of the ads as problematic at the time of the survey, while the other half is played out unhindered – which is particularly problematic with regard to the stricter rules in the context of health advertising according to the Meta Advertising Guidelines. What is also striking is the systematic misuse of the name of the TV show 'Die Höhle der Löwen' – this keyword accounted for 78% of all advertisements.

3.8.1. Targeting by gender, age and location

Advertisers did not target 94% of their ads by age or gender. However, the range analysis for Austria shows a clear pattern: 74% of the range is for **people aged 45 and over,** with the 65+ group accounting for the largest share, with just under 30%. Women are also over-represented at 60%. This corresponds to the typical target group for health products.

Category	Reach	Proportion
Gender		
female	6.532.996	60%
male	4.241.489	39%
unknown	153.089	1%
Ages		
18-24 years	1.848.431	17%
25-34 years	167.250	2%
35-44 years	859.146	8%
45-54 years	1.917.918	18%
55-64 years	2.890.556	26%
65+ years	3.244.244	30%
unknown	29	0%

Table 10: Untrustworthy dietary supplements – Reach by gender and age groups

3.8.2. Advertisers

The naming of the advertisers gives an insight into how the dubious providers work: this shows a strong dominance of the advertiser names of different **variations of the name 'Die Höhle der Löwen'**. This shows that the well-known investment program is massively abused in this area in order to give credibility to the advertised products.

Advertisers	Number of ads
Die Höhle der Löwen	1.700
Höhle des Löwen	1.327
Die Höhle der Löwen	1.070
Höhle der Löwen	956
Clinic VitalLuft Munich	930
Die Höhle der Löwe	916
Fabuleux	686
Dr. Leon Schulte	626
Die Höhle der Löwen - VOX 2023	534
vital life	465

Table 11: Untrustworthy dietary supplements – Ads by advertiser

3.9. Ghost stores

BASIC DATA

Advertisements: 9,955

Reach EU: 21,407,495

Reach Austria: 4,751,404

HIGHLIGHTS

Low deletion rate

Women and the elderly are overrepresented

Ghost Stores have **the second lowest deletion rate of all fraud schemes at 26.9%.** This is also accompanied by the fact that the offers operate in a grey area and are not criminally relevant. Instead, they violate the Unfair Competition Act and other consumer protection laws due to misleading advertising practices.

3.9.1. Targeting by gender, age and location

For the vast majority of ads, advertisers did not target specifically by age or gender. Only in **12.8% of cases** were the ads targeted at **men** and in 3.2% at women. The reach analysis for Austria shows a clearer focus – but less on men than on women, at the same time reaching a rather older target

group: the 65+ age group represents the largest share with 26%, followed by the 55-64 age group with 22%. At the same time, women accounted for 60% of the reach.

Category	Reach	Proportion
Gender		
female	2.851.510	60%
male	1.819.518	38%
unknown	80.376	2%
Ages		
18-24 years	846.379	18%
25-34 years	295.030	6%
35-44 years	581.269	12%
45-54 years	733.441	15%
55-64 years	1.037.942	22%
65+ years	1 257 283	26%
unknown	60	0%

Table 12: Ghost Stores – Reach by gender and age groups

3.9.2. Advertisers

The analysis of the advertisers shows a high correspondence between the names of the advertising accounts and the advertised shop names (including the actual shop domains). Advertisers such as 'Elle Weber', 'Modehaus Berfeld' or 'Lena-Boutique' simultaneously match the keywords identified for ghost stores.

Advertisers	Number of ads
Elle Weber	2.256
Fashion house Berfeld	1.887
Lena boutique	1.830
Lena Boutique Berlin	1.105
Moser Vienna	1.074
Muller Graz	518
Mirella fashion house	466
Alpina fashion house Vienna	183
Thera Boutique Graz	106
Weber atelier	104

Table 13: Ghost Stores – Ads by advertiser

3.10. Fake shops (brand imitations)

BASIC DATA

Advertisements: 28,276

Reach EU: 65.931.501

Reach Austria: 2,024,487

HIGHLIGHTS

Dominance of Lidl abuse

Mostly reached men

Broad EU targeting

Fake shops with brand imitations show a strong concentration of content: **86.4%** of all ads are attributed to the **keyword 'Lidl Discount'.** This confirms observations by Expert:innen of the Watchlist Internet, which in recent months documented a cluster of fake shops that misuse the name of the discounter. The deletion rate is 41.6%.

3.10.1. Targeting by gender, age and location

For the vast majority of ads (94%), advertisers did not target specifically by age or gender. Only 5.2% of ads targeted men, less than 1% targeted women. However, geographical targeting is more widespread than other fraud schemes and often targets the whole of Europe or the EU area. Accordingly, **only 3.1% of the EU's reach is accounted for by Austria.** 71% of the users reached are male. The age distribution is 48.5% for people over the age of 55.

Category	Reach	Proportion
Gender		
female	547.436	27%
male	1.444.321	71%
unknown	32.730	2%
Ages		
18-24 years	321.385	16%
25-34 years	60.212	3%
35-44 years	284.011	14%
45-54 years	377.169	19%
55-64 years	471.440	23%
65+ years	510.262	25%
unknown	60	0%

Table 14: Fake shops – Reach by gender and age groups

3.10.2. Advertisers

The top advertisers use names such as **'Discount Store'** or **mimic well-known supermarkets such as Lidl or Hofer,** with names slightly different from the actual brand names: for example, 'H0Fer' replaces 'O' with 'Zero (0)'.

Advertisers	Number of ads
Discount store	2.328
Online discount stores	2.148
Discount shop	1.556
Discount stores	1.288
L&i Wholesale Mall	913
LiDL Shop	848
Online discount shop	770
Online-Discount.Shop	596
Lidl discount mall	593
H0FER	591

Table15: Fake shops – Advertiser's ads

3.11. Online gambling

BASIC DATA (extrapolated)

Advertisements: 448,699

Reach EU: 620.572.304

Reach Austria: 64.790.612

HIGHLIGHTS

Highest number of ads and reach despite low keyword count

Highest deletion rate (82%)

25% of advertisements were targeted at men

Online gambling is by far the **biggest scam scheme,** both by number of ads and by reach, despite the fact that the number of keywords has been limited to four search terms. At the same time, the survey period had to be reduced to one week (instead of three months) for the keyword 'chicken road'. The reason for these limitations is that the search for fraudulent online gambling offers would have significantly exceeded the rate limit of the Meta API. In order to ensure comparability with the other fraud schemes, all key figures were extrapolated. The determined ad numbers were extrapolated linearly over the entire survey period of three months (factor ×13).

448,699 advertisements with an EU-wide reach of just over 620 million were extrapolated over the survey period. What is striking about this scam scheme is that Meta has **already removed 82% of the ads identified.**

3.1.1.1. Targeting by gender, age and location

While 75% of ads were not targeted by advertisers based on age or gender, **25% were targeted at men.** The range analysis shows a similar picture: 70% of the users reached are male, only 28% female. The age distribution shows a focus on target groups between 25 and 55 years, which accounts for a total of 80% of the reach.

Category	Reach	Proportion
Gender		
female	18.063.938	28%
male	45.286.921	70%
unknown	1.439.753	2%
Ages		
18-24 years	842.189	1%
25-34 years	13.497.856	21%
35-44 years	21.762.612	34%
45-54 years	16.423.450	25%
55-64 years	8.751.400	14%
65+ years	3.512.839	5%
unknown	266	0%

Table 16: Online gambling – Reach by gender and age groups

3.11.2. Advertisers

A total of 1,368 individual advertisers were identified with 7,558 beneficiaries/payers. The top advertisers use names such as 'Chicken Road' or variations thereof. Generic names such as 'Big Win', 'Touch of Fortune' or 'Glücksspiel Österreich' are also often used. In some cases, the names of well-known casinos are also imitated, such as 'Casino Austria' or 'Casino Wien'.

Advertisers	Number of ads
Chicken road	44.952
Chicken Road slots	37.140
Chicken Road 2	22.404
Best games	9.912
Ćhićken Røad Româŋiα	7.980
Chicken game	7.812
Epic Adventure	7.620
Chicken Road2	5.892
Bonus slot	5.388
Chicken Road X100	5.172

Table 17: Online gambling – Advertiser's ads

3.12. Conclusion

The quantitative analysis documents the scale of fraudulent and problematic advertising on Meta platforms: **634,000 ads** reached more than 1 billion impressions across the EU and 123 million in Austria within three months. As illustrated in Chapter 3.3 (3.3. Structural similarities in the fraud ecosystem), structural similarities can be identified across all fraud schemes, in particular **short ad runtimes** and lack of information about the advertisers or those paying for an ad.

At the same time, the data show clear differences between the fraud schemes – both in terms of size and targeting, as well as the active removal of ads from Meta.

Online gambling dominates with just under 450,000 ads and a reach of over 620 million both in volume and reach – although the survey had to be limited to just four keywords and a shortened period of time. Investment fraud follows with 83,000 ads and the second highest reach, while in the area of credit fraud with 805 ads, the fewest ads were found.

There are also schema-specific profiles when it comes to **targeting target groups:** dietary supplements disproportionately reach women and persons aged 45 and over, while investment fraud and credit fraud primarily reach men over 55, job fraud reaches women of working age and online gambling predominantly reaches men.

The **overall deletion rate is 62.4%,** but varies significantly between fraud schemes: While online gambling, job fraud and investment fraud ads have high deletion rates, subscription traps, ghost stores and especially credit fraud are hardly removed. The reasons for this gap are not clearly comprehensible – it does not consistently correlate with the criminal relevance of the content nor with its extent. However, it becomes clear that some of the fraud schemes are less covered by the existing content moderation.

4. Qualitative analysis

4.1. Methodological approach

For the qualitative description of the respective fraud schemes, a **criteria-based sampling** was carried out, which aims to capture those advertisements that are most effective on users due to their frequency and reach.

This selection was based on the crawler results of the quantitative survey. For each scam scheme, the five keywords with the highest number of individual advertisements were used. Within these keywords, the ad descriptions were sorted by frequency and the ads with the highest EU reach were selected for the most common descriptions.

In cases where a selected ad had already been removed from Meta or the landing page was no longer reachable, a new search in the ad library identified similar ads. **For each scam scheme,** the sample set includes **ten exemplary advertisements.** When selecting these, attention was also paid to thematic variance per fraud scheme in order to be able to collect different narratives.

The selected advertisements were then evaluated along the following analysis dimensions:

- Narratives used
- Visual strategies, including the use of AI-based image and video generation
- Content target group approach
- Forwarding infrastructure used
- Observable perpetrator strategies to bypass content moderation

The recurring patterns identified were condensed into overarching strategies.

4.2. Perpetrator strategies to circumvent security mechanisms

Offenders use various methods and strategies to circumvent the content moderation and security mechanisms of the platforms when placing fraudulent advertisements. These practices make it more difficult for researchers, regulators and also platforms' content moderation to systematically review and document problematic and fraudulent advertisements – and thus also represent a methodological limitation for the present study. In the following, the circumvention strategies identified in the analysis are presented and embedded in the context of existing research and regulatory findings.

4.2.1. Cloaking

Cloaking displays a different version of the linked website to the **platform's verification systems** (including searches via the ad library) than the actual users, who click on an advertisement, for example, while scrolling through their feed. While automated verification systems and people who click on an ad via the ad library see an unobtrusive and neutral website (the so-called 'white page'), users are redirected from the feed to the actual fraudulent content and sales pages (the so-called 'black page').

This strategy has been known for a long time: as early as 2020, Meta itself sued the provider 'LeadCloak', whose software was used, among other things, to circumvent automated ad verification systems (Sapra, 2020). The providers of these cloaking technologies are becoming increasingly professional. Security researchers speak of a growing ecosystem of 'cloaking-as-a-service' providers (Burt, 2025) that now offer their services openly. This increased availability and accessibility lowers the technical barrier to entry and also enables less technically savvy fraudulent actors to use this circumvention strategy.

4.2.2. Use of compromised accounts

Another workaround is to use compromised accounts. Compromised users' accounts – often **verified profiles of celebrities** – are used to serve fraudulent advertisements. This phenomenon is also not new and is documented by various security researchers. In 2023, for example, several verified and compromised accounts became known, renamed after official companies such as 'Meta Ads', 'Meta Ads Manager' or 'Google AI', and as such spread malware through the placement of advertisements (Hatmaker, 2023). By using such compromised accounts, the ads are given additional credibility, while large follower numbers already ensure increased visibility of organic content.

4.2.3. Multiple ad versions & 'Chameleon ads'

Displaying multiple ad versions within a single campaign is another identified bypass strategy. This is made possible by the **dynamic ad design** function provided by Meta, in which different versions are played out depending on the target group. While most of these ad versions seem harmless, at least one ad contains problematic or fraudulent content. Not only the ad image or video as well as the ad text can differ from version to version, but also the link to which it is forwarded.

This strategy makes both automated detection and manual verification difficult, as the fraudulent content is hidden behind seemingly unsuspicious material. In addition, security researchers also suspect that another tactic called **'Chameleon ads'** is being used. When creating the

advertisement, fraudsters initially only upload the harmless-looking advertisements. Once the ad has been approved, images, texts and links will be replaced by fraudulent content (Social MediaLab, 2025).

4.3. Narratives, targeting & used infrastructures

The qualitative analysis of the individual fraud schemes shows clear similarities despite thematic differences. These relate to the narratives and strategies used, the target group approach and, in some cases, the infrastructures used in the further course of the fraud. The following are three patterns that could be observed in many of the investigated fraud schemes in varying degrees: (1) the use of Deceptive Design, (2) the targeted creation of knowledge gaps ('curiosity gaps') and (3) the misuse of established trust anchors.

4.3.1. Deceptive design

Deceptive design – originally coined by Harry Brignull and known as 'dark patterns' – refers to user interfaces that, through the **targeted use of manipulative design elements, entice users** to act against their own interests, such as rushed purchasing decisions (Brignull, 2023). In the digital space, we encounter such patterns in a variety of forms, often also in combination: online shops, for example, work with artificial shortages ('Only 2 items available!') and thus generate a purchase pressure. The bait-and-switch trick appears to promote 'free' offers, which later turn out to be expensive subscriptions. And sentences such as '386 people have already bought this product today' fake social pressure to encourage purchases (Beltzung et al., 2024).

Deceptive design is problematic for several reasons: it undermines informed user choice, creates a structural power imbalance for the benefit of businesses or advertisers, and can lead to measurable harm, such as unintended contracts, unintended data sharing or financial losses (Brignull, 2023). In view of these risks, Deceptive Design is increasingly becoming the focus of consumer protection authorities.

In the fraud schemes investigated, such design elements form a central basis of the narratives used by advertisers to entice consumers into quick and ill-considered actions. Particularly common are **artificial shortages** and an equally **artificially generated urgency** – from temporary loan offers ('only today!') to limited places in supposed investment communities ('only for the first 1000 applicants') to expiring discount campaigns at ghost stores and fake shops.

In addition, **'confirmshaming'** is widely used: the decision-making of users is to be influenced by the triggering of unpleasant emotions. For example, by implicitly framing non-participation in IQ tests or ADHD screenings (see subscription traps) as an admission of ignorance or passivity, or staging non-participation in supposed insider groups (investment fraud) as a missed opportunity.

Another deceptive design element is **interface interference,** i.e. manipulations of the user interface that highlight certain actions vis-à-vis others in order to at least visually limit the options for action (Gray et al., 2018). This element is used in particular on the landing pages to which the advertisements redirect. On some of the landing pages, large-scale, colour-emphasized call-to-action buttons (e.g. 'buy now', 'test for free') dominate the visual hierarchy, while options to cancel or contract terms are barely visible due to smaller font sizes, lower contrast or placements at the edge.

4.3.2. Curiosity gap

In several fraud schemes, the so-called curiosity gap is systematically used – i.e. the **targeted construction of a knowledge gap** that should generate a strong impulse for action among consumers. If a person is made aware that he or she lacks certain information, a perceived state of tension arises, which can only be solved by closing the knowledge gap. In the context of online advertising, and not just fraudulent advertising, this mechanism is used in a targeted manner. A prominent example are clickbait headings, which are intended to entice you to click with phrases such as 'This new method will surprise you' or 'No one knows this trick'. The simultaneous use of superlatives or other intensifying words increases the perceived relevance of the missing information and thus also the impulse to fill the knowledge gap (Scott, 2021).

Unsurprisingly, the Curiosity Gap is also targeted in the context of fraudulent and problematic advertisements: starting with subscription traps that create **self-related knowledge gaps** ('How high is your IQ really?' or 'Are you smarter than the average German?'), **referring to alleged insider knowledge** in the area of investment fraud ('The new platform has already jeopardised the efficiency of the banking system' or 'Many people don't know how to choose stocks'), to advertisements of dubious food supplements that are often combined with **fear-inducing elements** ('He carried a secret inside him that nobody should know'). The latter also shows that the Curiosity Gap is often combined with emotional activation and thus has an increased effect. Statements such as 'Your IQ is probably lower than you think' or 'Only for Austrian citizens' can also affect the critical assessment of information. It specifically addresses internal influences (*visceral influence),* such as self-doubt, urgency and a sense of exclusivity (Langenderfer & Shimp, 2001).

4.3.3. Abuse of established anchors of trust

Another overarching pattern is the systematic abuse of acquaintances – be they persons, brands, institutions or the reference to regionality. The advertisers analysed use this strategy because people are more likely to rate and follow information and requests as credible if they come from a source perceived as authoritative (Stajano & Wilson, 2011). The Elaboration Likelihood Model (ELM), which was developed back in 1986, is now also used in the context of online fraud (Norris et al., 2019). According to this model, when confronted with a message, people – if they lack motivation or skills to check – use cues such as familiar names, logos or prominent faces as a basis for assessment. This behavior becomes particularly relevant on social networks, as they are often accompanied by low attention spans and a high flood of information at the same time.

In the ads analysed, established trust anchors are abused by different strategies:

(1) In several fraud schemes, **names, images and AI-generated deepfake videos of well-known personalities are deliberately misused** in order to lend credibility to the advertised offers. In the area of investment fraud, people such as former Austrian Finance Minister Hans Jörg Schelling or finfluencer Philip Hopf are used to apply. In the area of dubious dietary supplements, however, it is medical authorities, such as the doctor and cabaretist Eckhart von Hirschhausen or the ORF doctor Siegfried Meryn.

(2) In addition to using the authority of certain people, it also relies on the **prominence and trust of commercial and media brands.** In the case of dubious offers of food supplements, for example, the systematic misuse of the TV programme 'Die Höhle der Löwen' (name, logo, investors) dominates. Fake shops specifically imitate brands or food chains such as Lidl, Hofer, Swarovski or Birkenstock; online casinos adorn themselves with names such as 'Casino Austria' or 'Casino Baden' and investment fraudsters use names and logos of media such as oe24, ORF or Kronen Zeitung.

(3) A third expression is based less on authority in the narrow sense, but on the assumption that **regional offers are considered plausible and trustworthy.** This construction of local affiliation is used in particular by actors of the fraud scheme Ghost Stores, by business names such as 'Schneider Salzburg' or 'Muller Graz' suggesting a local – mostly family-run – operation.

4.3.4. Exploitation of situational vulnerabilities

In targeting the analysed advertisements, people are deliberately addressed who are more susceptible **to fraud in their specific life situations.** It must be assumed that it is not primarily

demographic indicators that characterise vulnerability, but rather specific life situations (Europäische Kommission et al., 2016), such as financial stress or acute stress experiences, as well as the associated situational physical or emotional states such as fear, greed or despair.

This becomes tangible in the area of credit fraud, for example, by targeting people who **are in financial distress** and have little access to credit in other ways ('despite private credit' or 'credit without proof of income'). In the area of job fraud, **jobseekers** with low formal qualifications or fragile employment biographies who hope for low-threshold career entry are addressed ('no experience necessary'). Vulnerabilities are also skilfully addressed when promoting dubious food supplements, for example by addressing **people with chronic diseases** and exploiting their hope for the advertised miracle cures.

4.3.5. Infrastructure used

An analysis of selected landing pages, which can be reached via the advertisements, shows that behind the fraud ecosystem is a **professionalized and partly shared technical infrastructure.** A recurring feature, for example, is the use of Cloudflare as a so-called reverse proxy: the entire traffic of a website is routed via Cloudflare servers before the actual target server is reached. This makes it impossible for outsiders to see where a website is hosted. Almost all examined domains use this mechanism and thus make it difficult to trace. Ghost stores, on the other hand, often use Shopify as a platform base.

In addition, the websites rely on **established tracking and analysis services** on a large scale (especially from Facebook, but also Google Tag Manager, TikTok Pixel and Klaviyo). These services make it possible to follow the behaviour of users on a website in detail – and to analyse which pages are accessed, where they are clicked and who actually buys. The data collected in this process flows back into the advertising platforms and allows for precise targeting of the ads – a mechanism that legitimate advertisers also use, but which, in the context of fraudulent advertisements, favours the targeted targeting of vulnerable target groups.

In addition, based on a similarity analysis of the HTML source code, several **clusters of websites** that are allegedly operated by the same actors can be identified. Websites for dubious dietary supplements consistently rely on the Funnelish service – a tool that specializes in conversion optimization and works similarly to Shopify. At the same time, these websites use identical images that are hosted on Funnelish and at least partially created using generative AI. The source code of these landing pages is also very similar. The HTML sources of the selected landing pages of the fake shops, in turn, are almost identical, contain code comments in Chinese and refer to their images

from a Chinese-configured web server registered with Alibaba. Despite Cloudflare obfuscation, they have a supposedly shared server address that indicates a China-based actor. Several domains share the same email server, which is hosted by Hetzner in Germany and presumably also serves as a web server for the actual landing pages. A search for this server revealed **more than 300 other comparable fraudulent websites,** indicating a much larger, coordinated network.

4.4. Subscription traps

For the fraud scheme subscription traps, fraudulent advertisements can be found in a wide range of topics: from intelligence tests, self-tests for neurodivergent manifestations (e.g. ADHD) to productivity analyses or dog training programmes. While the specific content differs depending on the target group and the advertised subscription, there are overarching similarities in the visual design, the approach as well as in the underlying strategic patterns.

Addressing self-doubt and optimization needs

A frequently used strategy lies in the targeted addressing of everyday uncertainties and the **socially widespread pressure for self-optimization.** The advertisements address topics that many users can identify with, such as difficulty concentrating, procrastination, suspected ADHD symptoms or the question of their own intelligence. On the one hand, there are statements such as 'Your IQ is probably lower than you think' or 'ADHD is not laziness', which reinforce existing self-doubt or problematise everyday difficulties. On the other hand, the wording is enhanced, such as 'only very intelligent people solve these questions' or 'you are smarter than you think'. This combination uses the **Curiosity Gap** (see 4.3. Narratives, targeting & used infrastructures): Uncertainty addresses a self-related knowledge gap and creates a need to close it, while flattery acts as an incentive to give in to this need by clicking. It addresses in particular people who already feel insecurities about their cognitive abilities, productivity or mental health.

Everyday problems are either pathologized or framed as undiscovered potential. Difficulty concentrating appears as a possible sign of ADHD and average test results as evidence of underestimated giftedness. These narratives are often accompanied by pseudo-scientific explanations of ADHD, neurodivergence, productivity or brain power. Terms such as 'show studies', 'scientifically proven' or 'PhD-level questions' are used to further underline the seriousness and scientific base of the advertisements.

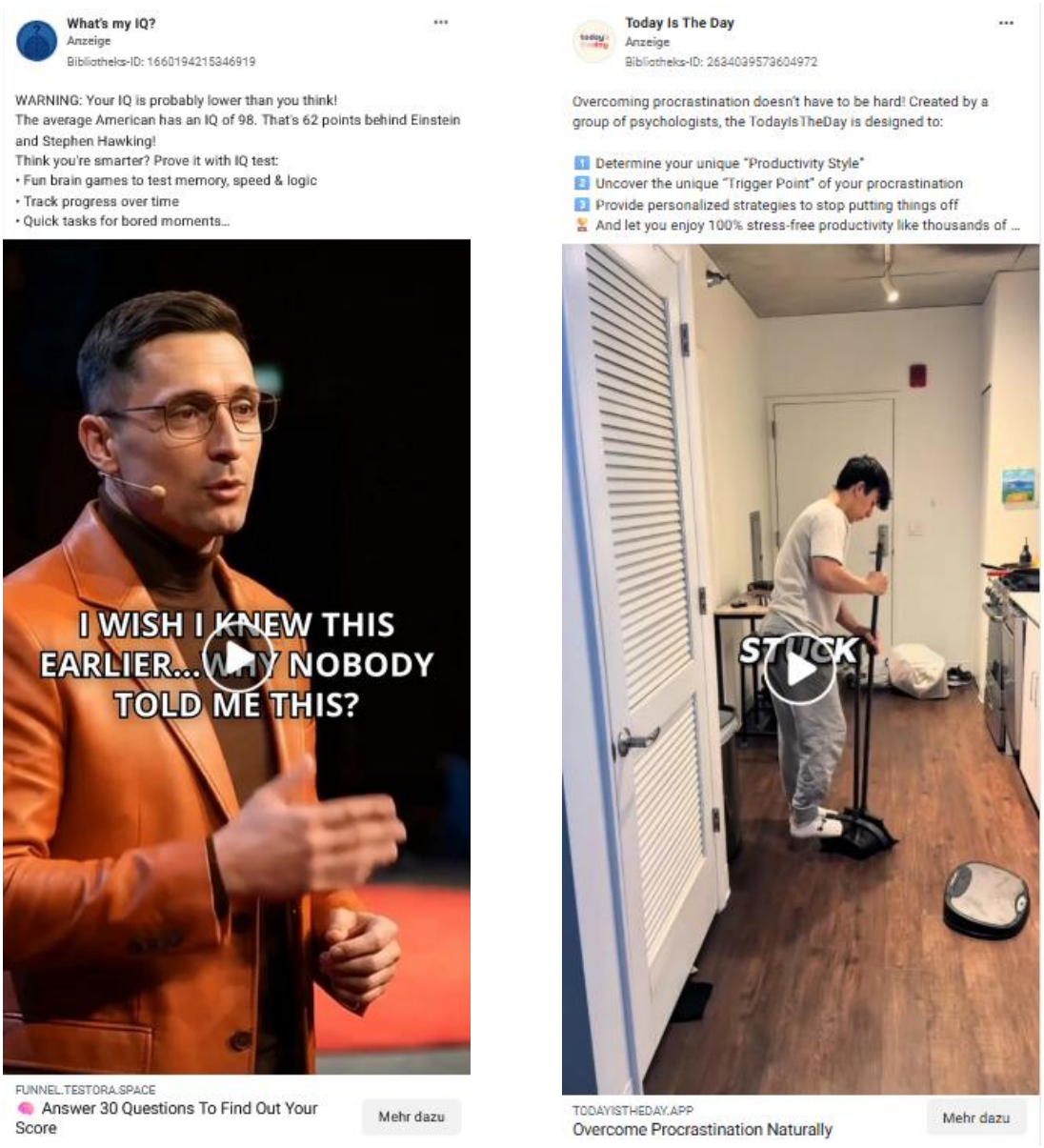

Figure 1: Fraudulent ad on IQ Test and ADHD Test

Visually, these messages are additionally supplemented with supposed expert videos, some of which are AI-generated. In these videos, people explain in a factual, calm tone why their own self-assessment is probably incorrect and why a short test could provide reliable insights within a few minutes. These representations are supplemented by graphics of IQ scales or striking brain representations.

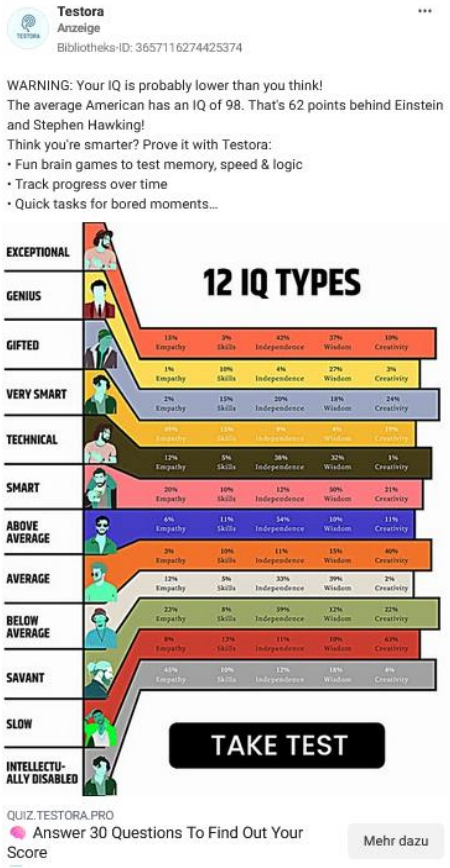

Figure 2: Fraudulent ad on IQ classification

Low-threshold interaction

Another identified strategy is to promote as low-threshold interactions as possible. The introduction to the offer is deliberately described **simply and without obligation.** Wordings such as '1 minute test', 'only 30 questions' or 'start now' give the impression of a quick, simple gain of knowledge without much effort. This significantly reduces the threshold for participation.

Further course: Click-through tests & alleged individualization

Clicking on the ad link leads to visually and structurally similar 'click-through' tests, in which users answer questions step by step. Progress bars and personalized response reinforce the impression of an **individual diagnostic process.** Users answer questions about concentration, thinking behavior, everyday situations or specific behavioral patterns of their animals. Progress indicators, personalized salutation forms and interim evaluations reinforce the impression of a personalized diagnostic or analysis process.

In the end, the opportunity is offered to receive a detailed evaluation of the test results or a personalized training/exercise plan by e-mail. It is only at this point – often less prominently – that the fee-based subscription structure becomes apparent.

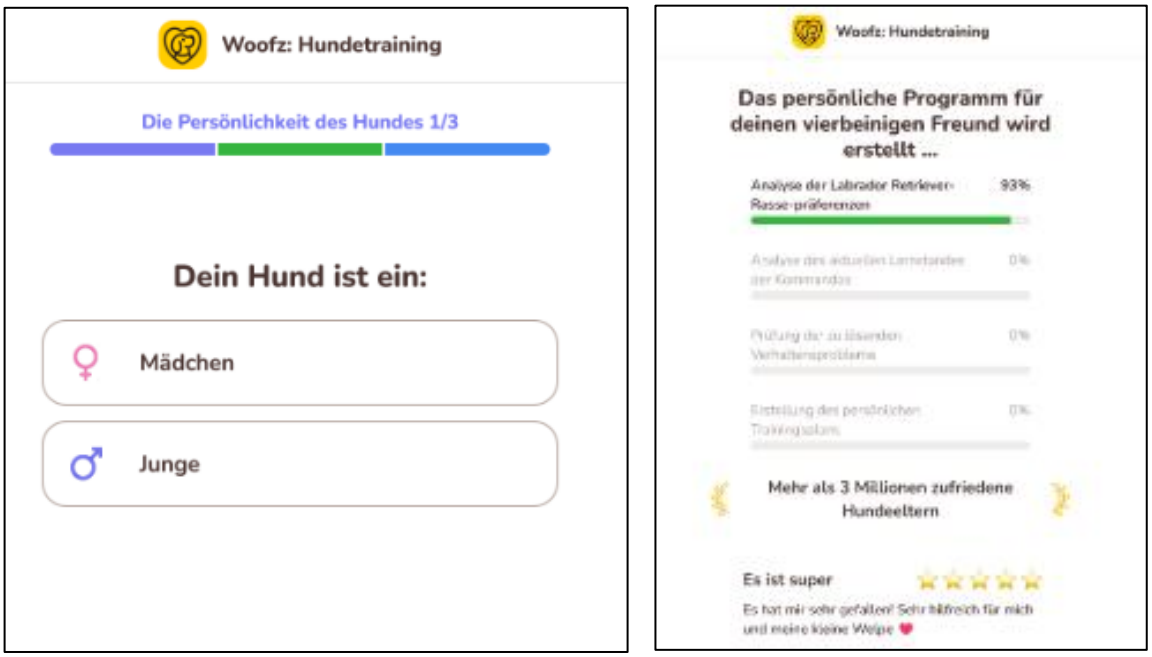

Figure 3: Landing page Woofz Academy

The user interfaces of the landing pages are also often designed in such a way that they entice users to interact with them much and quickly. Large-scale 'call-to-action buttons', reduced amount of text, emotional reinforcements ('You are almost at your destination!') as well as countdown elements or time-limited offers can be clearly assigned to the methods of Deceptive Design and thus manipulatively increase the incentive to interact. Contract details, terms or references to automatic renewals are formally available, but often only visible in further links or extensive terms of use.

4.5. Investment fraud

Among the analysed advertisements in the area of investment fraud, several overarching strategies can be identified that are structurally similar despite thematic variations, such as AI-based trading or insider trading communities.

Technological innovation as a promise of return

A central strategy lies in the instrumentalization **of current technology developments,** in particular artificial intelligence, in order to suggest a supposed competitive advantage. Ads systematically use buzzwords such as 'AI trading', 'ChatGPT shares' or 'AI strategy'. Formulations such as 'artificial intelligence analyses the stock market every day to find high-quality stocks for you'

or 'how I make €1000 every day with ChatGPT without experience' suggest that complex financial market analyses are made accessible to laypersons through AI.

Particularly perfidious is the use of specific accuracy rates – such as 'AI accuracy up to 98%' – which pretend to be an empirical validation of the method. These figures not only serve to build trust, but also communicate pseudoscience. The 'modernisation' of financial market access is presented as technological progress that overcomes rational investment barrier.

Figure 4: Fraudulent ads referring to ChatGPT

Exclusivity through community model

A second strategy is to **build exclusive communities** and shift communication to **messenger platforms.** About a year ago, dominant advertisements, which in the next step led to fake news pages and from there on to the fraudulent platforms, now redirect the ads to a large extent to messenger platforms: 87% of all ads collected by us and not yet removed did not redirect to a landing page, but to 'fb.me' – i.e. the Facebook messenger. It can be assumed that from there, in turn, WhatsApp chat groups will be forwarded, as advertised in the advertisements.

This shift to private chat groups **weakens** the comprehensibility for authorities and researchers, at the same time uses the supposed privacy of messenger services to build trust and gives users the feeling of being part of an exclusive community. Formulations such as 'Exclusive profit opportunities – benefit now', 'Pre-market trading strategy' or 'Join the equity analysis VIP group' create an artificial sense of privilege and suggest that 'normal investors' do not have access to this information.

A strategic shift in the target group approach is also striking: a few months ago, for example, the telephone number was often queried on fake news pages or directly on investment pages and the persons concerned were contacted by telephone by a 'personal advisor' or a 'personal advisor'. With the shift to chat groups, the focus is more on low-threshold interaction, continuous information supply and group dynamic effects.

Deceptive design elements

The combination of artificial scarcity and free offers is particularly effective. Statements such as 'only for the first 1000 applicants', 'only 100 places available' or 'limited participation' create urgency and exclusivity pressure, while at the same time stressing 'we do not take money – you get the best tips completely free'.

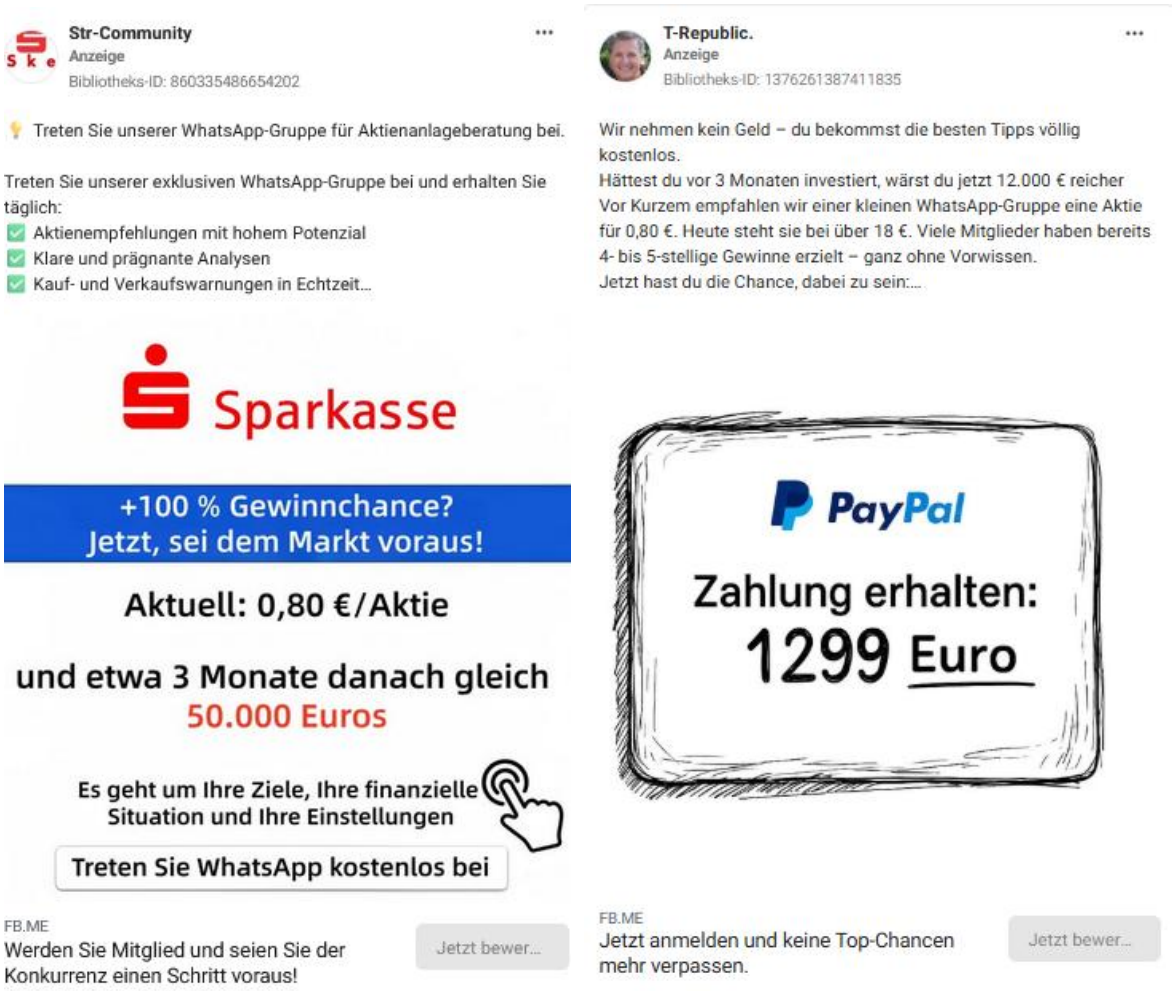

Figure 5: Fraudulent ads with community model

The community model also works on the **principle of social proof: when there are supposedly many 'members** already present', it creates the impression of an established and legitimate investor community.

Construction of authority and trust, e.g. through the use of deepfakes

The third strategy is based on the systematic misuse of prominent names and the construction of supposed expert identities. Authorities from the world of finance are particularly frequently abused, such as former Austrian Finance Minister Hans Jörg Schelling, finfluencer Philip Hopf (or the heavily criticised podcast duo Hoss & Hopf) or 'Investmentpunk' Gerald Hörhan.

Figure 6: Finfluencer Philip Hopf's name abused in a fraudulent ad

Technologically, this strategy is supported by the **use of deepfake videos.** These videos show seemingly authentic footage of people promoting fraudulent investments or calling for participation in WhatsApp groups. In a video, for example, Philip Hopf appears and announces an exclusive 'insider tip' for a high-growth stock, coupled with the prospect of fast and secure profits.

Here, too, a shift can be observed in the selection of the abused celebrity: While about a year ago ORF or Puls4 moderators (e.g. Armin Assinger, Nadja Bernhard, Armin Wolf, Barbara Fleißner) were increasingly used, the focus is now more on persons with explicit financial expertise or political authority. Instead of relying on widespread awareness, professional **credibility** is increasingly being staged. At the same time, the selection of celebrities partly appeals to a younger target group.

The yield promises are systematically unrealistic: statements such as '€0.80 per share and around €50,000 3 months later' or '+100% profit opportunity?' promise exceptionally high and risk-free profits at the same time. These promises are complemented by urgency narratives – 'only a few places left', 'be ahead of the market', typical deceptive design mechanisms of artificial scarcity.

4.6. Credit fraud

The core of the credit fraud strategy is to target financially vulnerable individuals through a combination of (1) guaranteed credit accessibility, (2) radically simplifying the credit process, and (3) artificially generated urgency. The resulting narrative suggests hope, relief and immediate problem solving and is a particular danger for people in financially vulnerable situations.

Figure 7: Fraudulent ads Credit fraud (left: credit despite poor creditworthiness, right: simplified presentation of the credit process)

Exploitation of financial vulnerability through low-threshold and urgency

The target group of these advertisements includes in particular **persons in financially precarious situations who** are excluded from the regular credit market due to their life situation or who perceive themselves in this way. The target group is suggested that despite exclusion criteria in lending processes, they are able to apply for a loan. The classic selection logic of serious lending – credit check, proof of income, risk assessments – is deliberately reversed rhetorically: inclusion instead of exclusion. Wordings such as 'loan despite credit bureau', 'loans without proof of income' or 'without credit check' communicate this counter-narrative to the formal banking system and actively address the need for a 'second chance'.

Another key element is the simplification of the application process. Statements such as 'just a few clicks' or 'no documents needed' usually represent a complex, lengthy financial decision as a seemingly **casual, uncomplicated digital interaction.** The scope of a credit agreement, of interest and maturities over contractual terms, remains obscured and non-specific in the presentations. Instead, the focus is on speed, low-threshold, and minimal data entry.

Deceptive design elements

Visually, the display of various manipulative elements is used: formulations such as 'only today', 'only few places left' or 'the offer will end soon' convey a picture of urgency, which should entice users to make quick decisions. Especially for people in financial distress, this **staged shortage can reinforce existing** stressful situations and increase the willingness to act outside serious institutions and the associated examination modalities.

Further course: Click-through tests

Following the ad link often leads to 'click-through tests' that follow similar strategies as Subscription traps outlined in the section – personalised credit offers, 'call-to-action buttons' and emotional reinforcement.

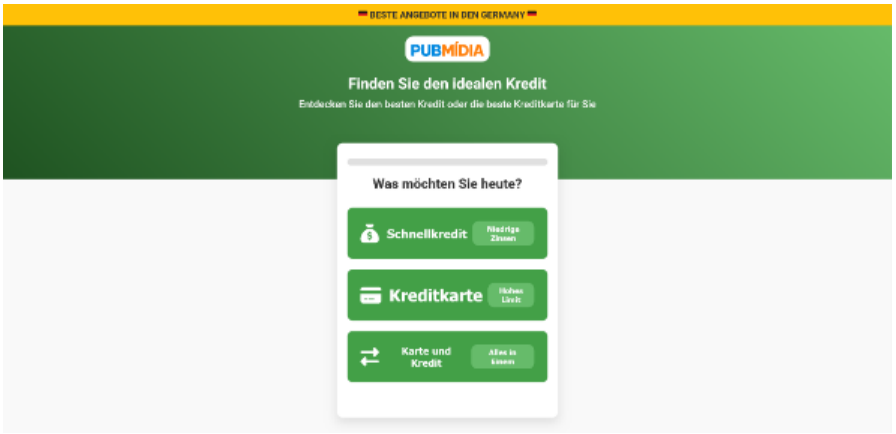

Figure 8: Unreliable credit fraud website

4.7. Job fraud

Fraudulent advertisements in the field of job fraud serve a broad thematic field and vary their narrative design partly seasonal or event related. Two overarching strategic methods can be consistently identified: the mediation of low-threshold employment promises on the one hand and the illusion of legitimacy and plausibility on the other.

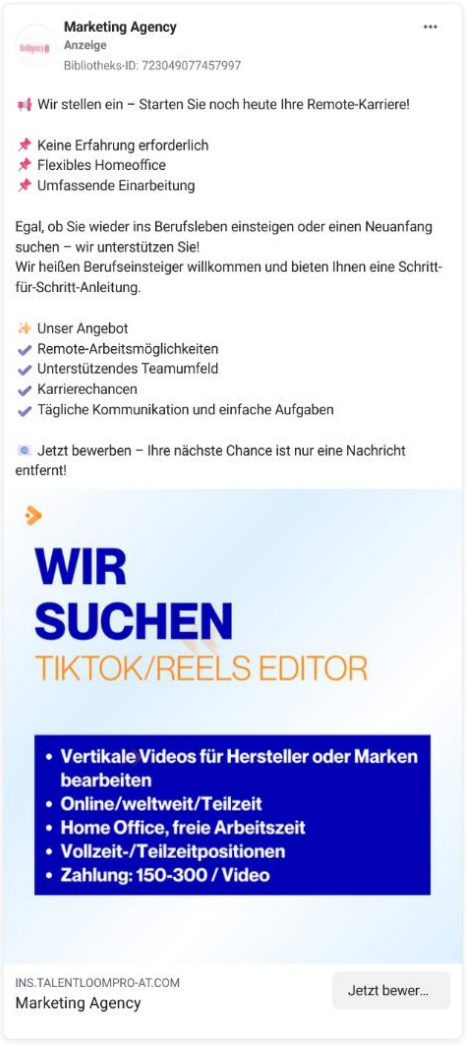

Figure 9: Fraudulent ads for alleged job offers

Low-threshold employment promise

At the heart of many advertisements is the presentation of an **effortless career entry**, which is almost independent of qualification, experience or formal requirements. Wordings such as 'no experience required' or 'no experience? No problem!' suggest that anyone can apply and start immediately.

This low-threshold invitation is reinforced by other elements: activities are described as 'small tasks', team spirit and support are emphasised, and free training is envisaged.

At the same time, the application process is greatly deformalized. Statements such as 'Start today', 'Our professional team will get back to you within 24 hours' or 'Apply immediately' shorten the usual application process to immediate action.

It is often called for contact via messenger services, which further reduces the institutional distance. This is also confirmed in the data, as 58% of all ads not yet removed were directed to 'fb.me', i.e. the Facebook Messenger. The complex and multi-stage selection process of regular employment relationships is thus presented as a spontaneous, almost incidental interaction.

Another key element of this strategy is unrealistic or at least severely excessive compensation

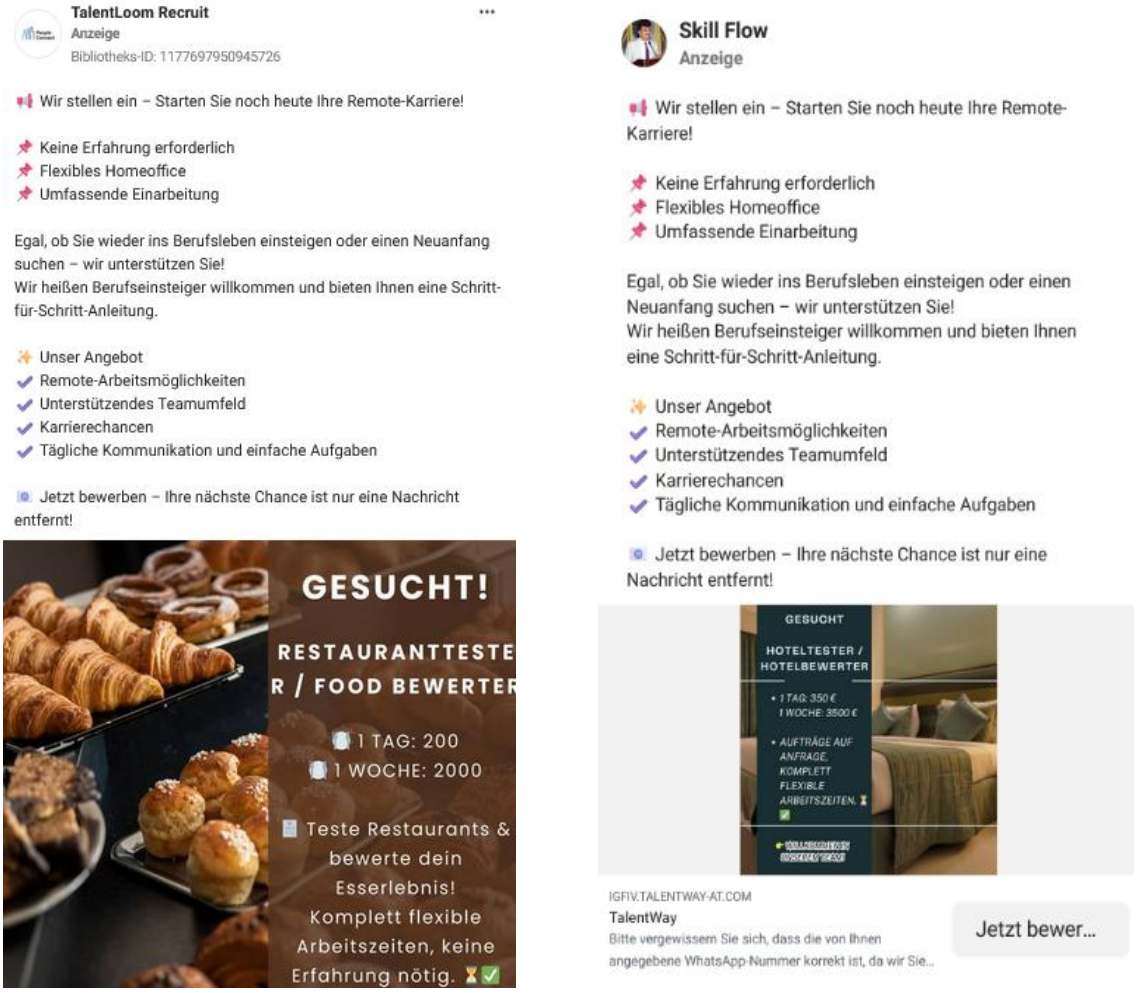

Figure 10: Fraudulent ads about alleged dream jobs

promises. Statements such as '€200 per day', '€150-300 per video' or 'pay your rent at 1-2 hours of work per day' create a significant **mismatch between performance and income.** The activity itself often remains vague or non-specific, while financial reward is clearly and prominently communicated. In combination with 'dream professions', such as hotel or restaurant testers, a deceptively enticing work picture is created that combines status, flexibility and financial security.

Pretence of legitimacy and plausibility

In the area of job fraud, on the one hand, a low-threshold, highly attractive employment promise is constructed, which removes central hurdles in the labour market and opens up unrealistic income prospects. On the other hand, the adoption of real job advertisements, the use of well-known brand names and local and event-related contexts simulate legitimacy. Parallel to the construction of an attractive job offer, work is being carried out to reduce potential scepticism. This is done by pretending seriousness and constructing supposed legitimacy – for example by taking over real or realistic job advertisements from well-known companies. In some cases, job advertisements are even copied in the same wording and replayed via advertisements with a deviating, dubious link. For example, the job advertisement of a Tyrolean advertising agency was completely taken over and provided with a fraudulent forwarding. Instead of building one's own credibility, existing reputation is taken over.

In addition, the **mention of prominent brands** such as Lidl, dm or Lego is often used without establishing a comprehensible link between the advertised activity and the company. This practice aims to transfer brand trust and recognition value. The mere presence of a known name or logo may be enough to increase the perceived legitimacy of the ad.

In addition, a strong local connection is used – despite jobs that can mainly be carried out remotely. Advertisements explicitly refer to specific cities such as Vienna, Salzburg or Linz or are linked to seasonal and event-related contexts, such as Christmas jobs, major sports events (e.g. World Cup football) or short-term promotional activities. This situational embedding creates the impression that it is a real, temporally and spatially clearly located employment offer.

Figure 11: Fraudulent job advertisements with event and local reference and reference to well-known companies

4.8. Untrustworthy dietary supplement offers

In the case of dietary supplements (NEM), fraudulent advertisements for various health areas as well as clinical pictures can be observed: from decrease to erectile dysfunction to diabetes or blood sugar problems. While narratives and audiences depend on the product and differ, across-the-board similarities in ads and strategies can be identified, including misuse of trade names, misuse of medical, media or government authority, and pseudo-scientific narratives.

Abuse of trademarks and the 'Höhle der Löwen' show

One strategy is to fake cooperation with **established brands such as** dm or Rewe, or to advertise with the **TV start-up show 'Die Höhle der Löwen'.** Examples of such advertisements can be observed especially in the area of diets and weight loss. Among the top five keywords with the most ads were three on weight loss, including 'Die Höhle der Löwen'. This strategy is exemplified by Figure 12 example. In the advertisements themselves, the dm logo is often misused and a seal with the statement '60 days money back guarantee' is used to demonstrate additional legitimacy. Visually, AI-generated images and unrealistic representations, e.g. of abdominal fat, are used to display 'yellow

balls', for example, before and after images. Impossible promises such as '-14 kg in 3 weeks' or '12 kg in just 2 weeks' suggest a quick weight loss effect of the product.

Figure 12: Fraudulent ads for weight loss products

Pseudoscientific character

Another strategy is **pseudoscientific narratives** designed to convey trust and expertise. In some cases, simple studies are simulated that have never existed before: statements such as 'Clinically tested on more than 27,000 women and men (18 - 75 years)' or the effects would be 'undoubtedly confirmed' can be found in the display texts. And – often AI-generated videos – seemingly evidence-based claims such as 'You may think a strict diet or total alcohol-free diet is the only way to control your fatty liver. But science shows that this is a fatal error.' These statements are accompanied by anatomical representations and animations reminiscent of medical documentation (such as a liver that becomes 'sick', turns brown and 'shrinks'), as well as by the enumeration of non-specific symptoms such as 'fatigue' or 'bloating'.

At the same time, the clips work with **scary narratives** ('fatal error', 'acts like a creeping poison', 'results in further health problems'). In addition, vague references to experts are used to increase authority, such as formulations such as 'according to leading hepatologists' – in this case, too, pseudo-scientific assertions are made without comprehensibly proving them.

Abuse of medical, media or state authority

An even stronger manifestation of this strategy is the abuse of existing medical, media or state authority. Well-known doctors and health experts are abused by AI-generated or manipulated

videos in order to promote fraudulent NEM offers. Some of these videos are staged in the style of news articles in which well-known moderators such as Armin Wolf or Susanne Höggerl appear. Fear-mongering **anti-establishment narratives** such as 'the evil pharmaceutical companies want to keep you sick' or 'the government banned this remedy' are also spread (Auer et al., 2025). In some cases, advertisements are also served by accounts whose names are also intended to convey medical authority, such as 'Dr. Katharina Wolff' or 'Dr. Leon Schulte'. The corresponding profile images are AI-generated and depict people in white gowns and stethoscopes.

An exemplary example also shows a frequently represented combination of celebrity or expert staging, promise of action and institutional assertion of authority: a video claims that the German doctor and cabaret artist 'Dr. Eckhart von Hirschhausen' 'discovered a natural method to strengthen the erection' – 'without risks, dependency or side effects'. As a supposed 'method', everyday home remedies are presented, which create the **impression of a simple, immediately implementable solution.** In addition, an alleged 'support programme of the German Government' is addressed, which is aimed at 'all men over 45' and is intended to prevent them from suffering from 'chronic impotence at 60 or 80' or from being dependent on the consumption of '2-3 Viagra pills'. Risks of established drugs are dramatised (e.g. claiming that Viagra can 'increase the risk of stroke or heart attack by 46%') and the prospect is that the advertised solution can improve not only physical problems but also the relationship with the partner. **Conspiracy narratives** are also used, suggesting that the 'true reason' for erectile problems is concealed by 'German pharmaceutical companies and doctors'.

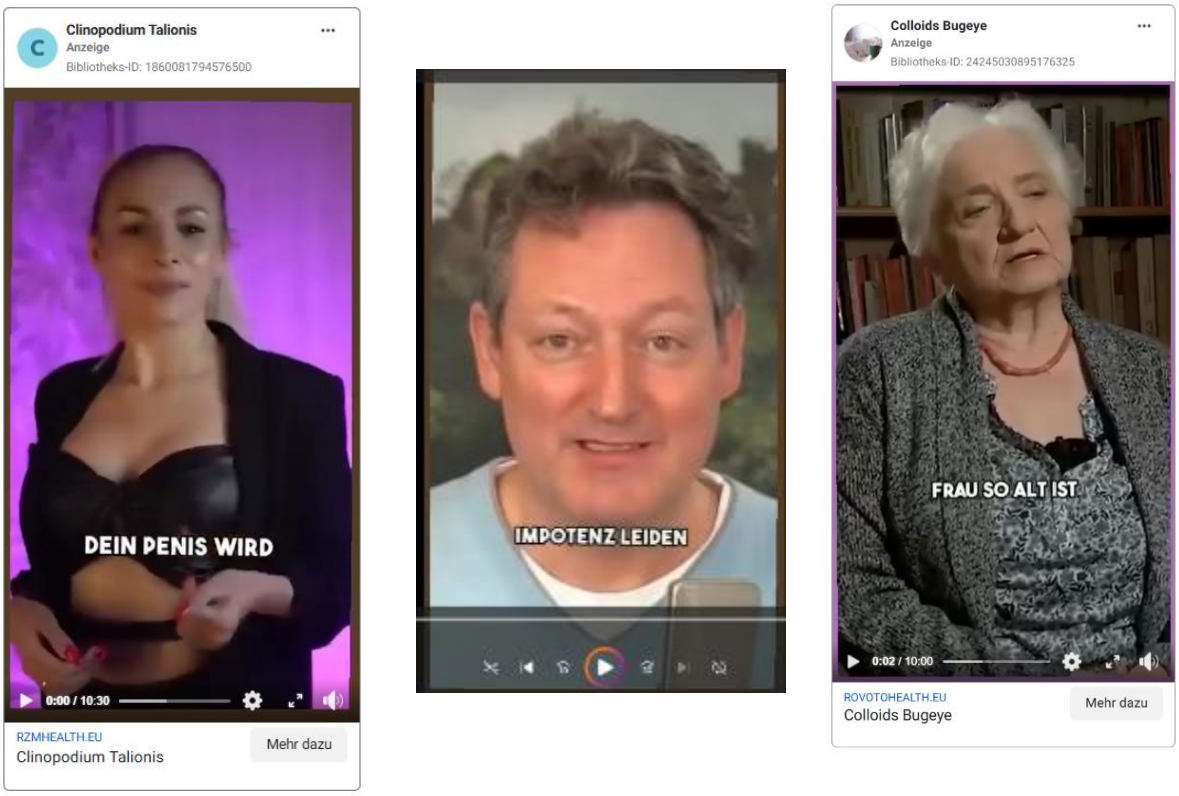

Figure 13: Fraudulent ads about dietary supplements with alleged impotence cure and further video with AI-generated image of Dr. Eckart von Hirschhausen (in the middle)

Adressing chronic diseases

A particularly problematic dimension of these advertisements is the targeted content of persons with chronic diseases – including diabetes, hypertension, prostate complaints, erectile dysfunction or liver diseases. The advertisements specifically build on the hopes and despair of those affected and present advertised products as supposed alternative medicine. A survey by ÖIAT shows that the manipulation goes so far that consumers were recommended in downstream consultations and sales discussions to discontinue their actual medications – for example in the case of diabetes – and instead to rely on the advertised food supplements (Auer et al., 2025).

4.9. Ghost stores

The ads for Ghost Stores follow a consistent pattern: The advertisers stage themselves as regionally anchored family and traditional businesses in Austria and Germany. Emotional farewell narratives legitimize large discounts on alleged quality goods.

Emotional farewell narrative

The central strategy of ads for ghost stores is to combine large **discounts with emotional farewell narratives.** It often mentions supposedly personal stories and motives for the closures of the business – from illnesses and deaths to financial hardships or happy news such as the birth of grandchildren. Also popular is the narrative that the 'big corporations would have won', and the small Austrian shops are now giving up 'the fight' after decades.

With phrases such as 'With a lot of emotion, we want to share an important message. After many wonderful years full of passion and dedication for our boutique, we have made the decision to close our business' is deliberately emotionalised. Accompanied by thank-you statements to loyal customers, the online shops advertise with large discounts on supposedly high-quality goods, which must be quickly removed from stock.

Regionality

These narratives are linked to the **construction of local affiliation:** on the one hand, business names with an explicit regional reference (e.g. 'Muller Graz', 'Moser Wien') are chosen, which suggest a local operation. On the other hand, AI-generated images of supposed business premises are placed on the landing page to which the advertisements lead, feigning a physical location at the specified company headquarters. This strategy makes targeted use of trust in regionality and small-scale structures.

Deceptive design elements

In addition to legitimizing offering incredible discounts due to the impending business closure, there is also the strategy of offering **time-limited sales or special promotions.** This is underscored by statements such as 'Only 50% discount today' or 'Only for a short time – As long as stocks last'. Thus, an artificially generated urgency is created to encourage buyers to buy quickly.

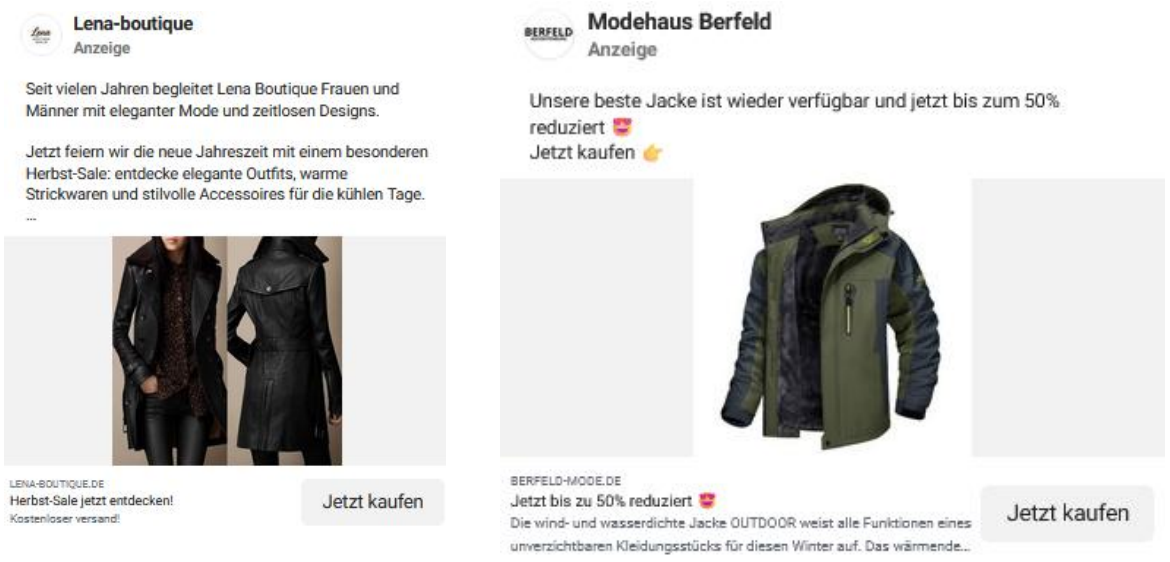

Figure 14: Fraudulent ads on ghost stores

4.10. Fake shops (brand imitations)

The fraud scheme of fake shops and brand imitations combines imitation brand identities, unrealistic price promises and a technically veiled but structurally uniform infrastructure. For consumers, the deception is particularly difficult to see through, because the confidence signals used – known logos, serious warranty promises and realistic product images – deliberately undermine those protective reflexes that would apply to apparently dubious offers.

Abuse of established anchors of trust

This strategy consists in the active imitation of well-known brands firmly anchored in Austria. Two variants can be observed, some of which also occur in combination: On the one hand, **well-known retail chains** such as Lidl or Hofer are imitated, whose logos are embedded directly in the product images. On the other hand, brands from particularly high-quality manufacturers, such as Birkenstock, Bosch, Swarovski, Garmin or Philips, are used as product promises. In part, this is

connected by suggesting supposed cooperation or partnership between the retail chains and the manufacturers.

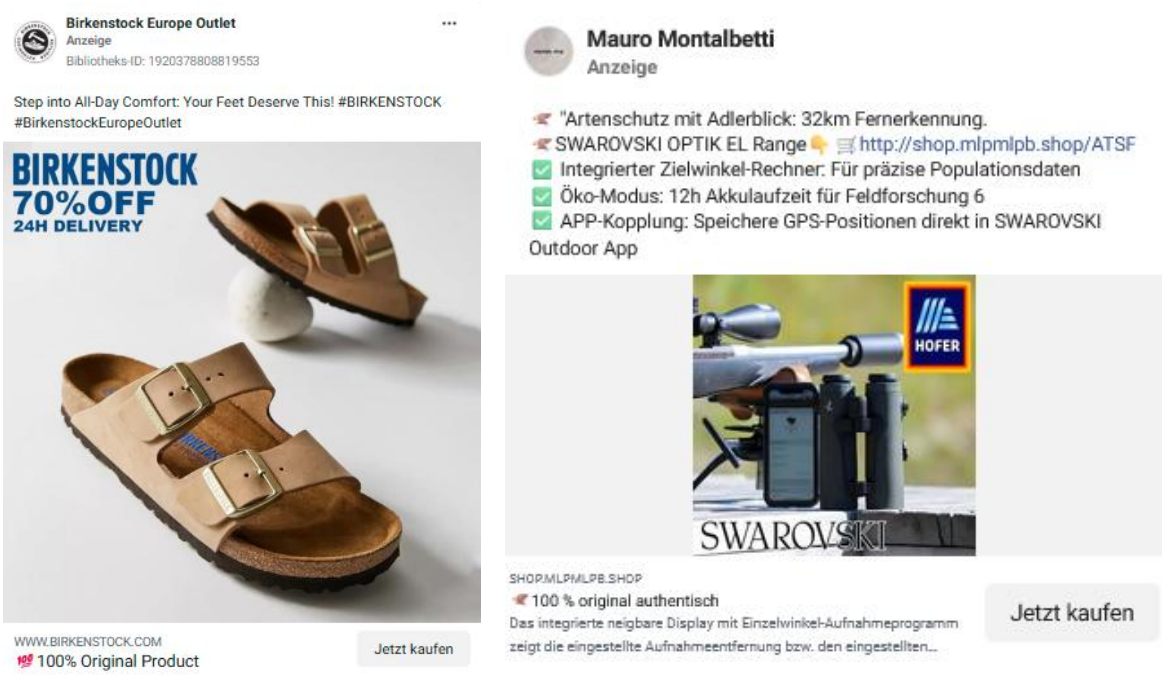

Figure 15: Fraudulent ads for fake shops (left: Birkenstock, right: Hofer and Swarovski)

The main narrative behind this strategy is that of **officiality and authenticity:** formulations such as '100% Original Product' or '100% Original Authentic' emphasise authenticity where it could be most doubted. This is complemented by a local narrative, 'HOFER – Opening new branches in Austria!', 'Versand aus Österreich/Deutschland', which suggests regional roots and proximity. Reputable dealer promises such as '5 year guarantee', '100 days free return' or 'Shipped within 48 hours' complete the picture of a trusted incumbent supplier. The links in the advertisements partially display the official links, for example 'www.birkenstock.com', but are then redirected to a fake shop with a slightly modified URL.

Discounts as bait

The second central strategy is advertising with very **low prices for high-quality branded products.** Bosch refrigerators or washing machines are offered for €89.99, Swarovski binoculars at a fraction of their market price, Birkenstock sandals with '70% OFF'. These prices are systematically well below any realistic market level and aim at a targeted surprise: the offer is obviously too good to be true – but is nevertheless perceived as plausible by the familiar brand context. This is achieved on the one hand by the exact product description, as well as by the product images, which often show the advertised product in a physical store.

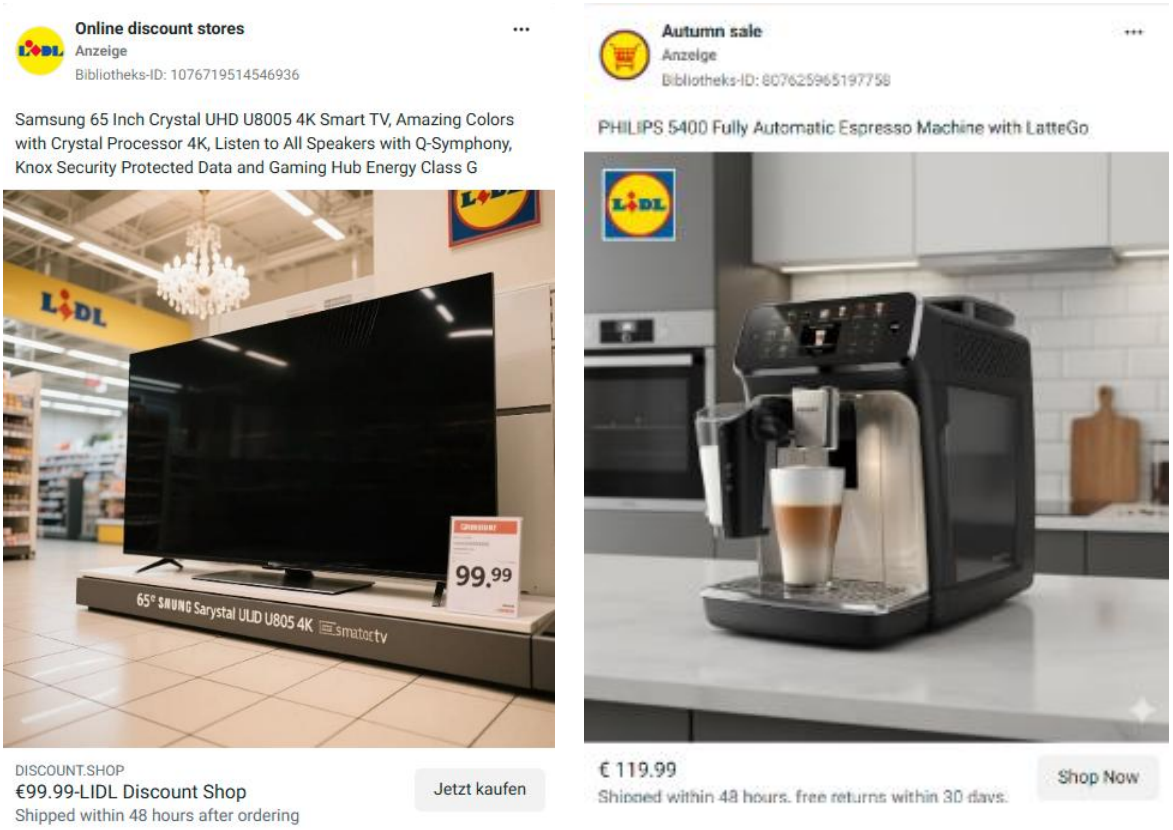

Figure 16: Fraudulent advertisements about brand imitations from the Lidl chain

Wordings such as 'The lowest prices ever! Don't miss out!' or seasonal allusions such as 'autumn sale' and fake store openings create an artificial urgency and also suggest a legitimate selling context. The offer is presented as a unique opportunity that should not be missed.

4.11. Online gambling

In the fraud scheme online gambling is mainly advertised with references to official casinos such as Casino Wien or Casino Baden or with the online gambling games 'Chicken Road' or 'Plinko'. Three overarching strategies for promoting this scam can be observed on the basis of the advertisements collected. All pursue the goal of gaining the trust of users and attracting them to the respective fraudulent platforms or apps.

Limitation fiction by imitating well-known casinos

One of the most striking features of the analysed gambling ads is the targeted **imitation of established, licensed local (Austrian) casinos.** The advertised offers, including 'Casino Wien online' and 'Casino Baden is now officially online', give the impression that it is the official digital

extension of Casinos Austria. In fact, however, these are standalone, unlicensed offers that redirect to dubious, similarly named domains.

Figure 17: Fraudulent online casino ads

This strategy uses two key narratives: First, a strong **prestige and local identity narrative** is built. Formulations such as 'Style. class. Vienna' or 'Where history and innovation meet' present gambling as a culturally located, respectable activity. Second, statements reinforce this with a **convenience narrative.** The online offer is presented as an equivalent but more comfortable alternative to the physical casino visit.

On a visual level, too, the ads make use of well-established legitimation signals: Real architectural photos of well-known casino buildings are provided with digital neon overlays and thus capture the authenticity of real places. All in all, this creates a visually coherent surface that suggests seriousness and institutional affiliation without actually possessing them. The inclusion of official payment logos from Visa, Mastercard, App Store and Google Play in almost all advertisements suggests trust and seriousness on the part of well-known providers, regardless of whether there is a genuine payment partnership.

Incentive manipulation through bonus promises

A second strategy primarily addresses newcomers. A large number of all ads analysed promise **generous welcome bonuses, such as** up to €1,500 in bonus credits or 250 free spins, which are shown as an explicit offer for 'new players'. This practice is a classic acquisition tool. The advertised bonus lowers the psychological barrier to entry and creates the feeling of an asymmetrically good deal, in which the:the user:in apparently risks little and can win a lot. Mandatory information on risks, risk of addiction or bonus conditions is completely missing from the advertisements or is designed in such a way that they are hardly noticed.

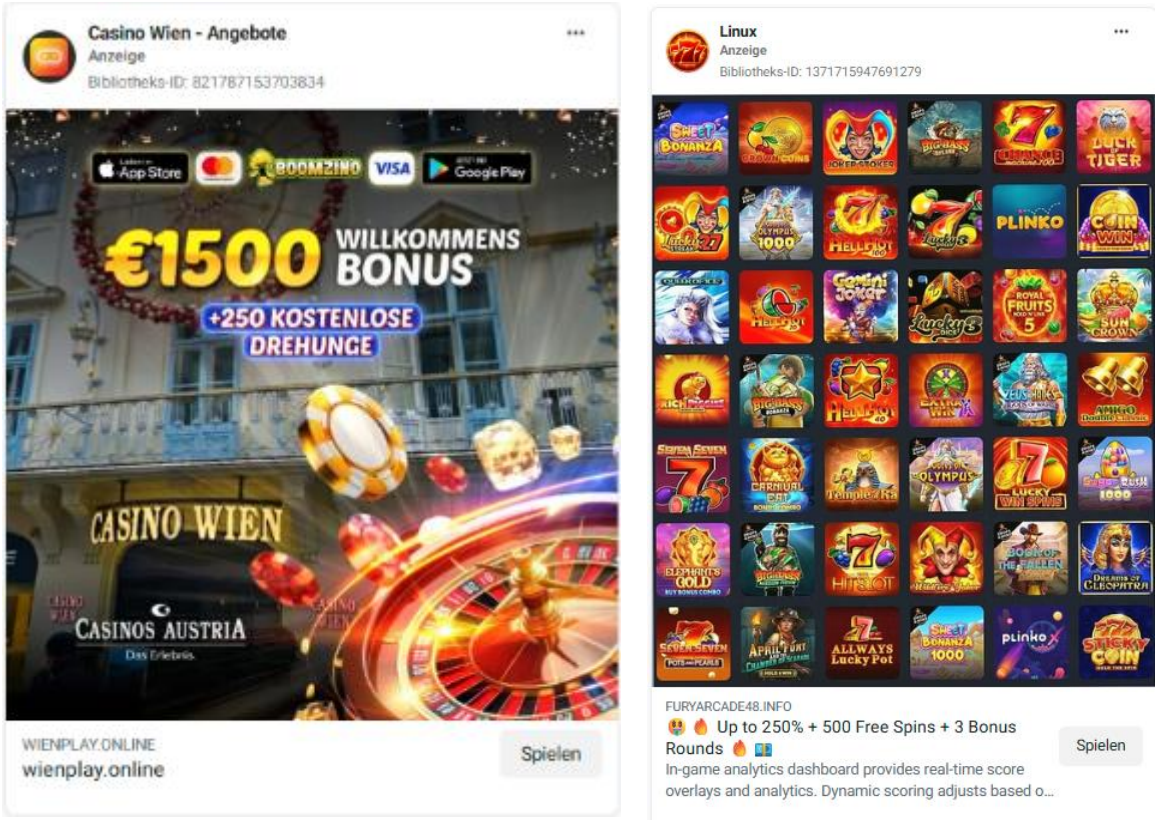

Figure 18: Welcome bonus for beginners in fraudulent online gambling

Social validation and deceptive design

A third strategy, especially seen in the Chicken Road and Plinko Gold ads, combines the use of social prominence and Deceptive Design Element. The aim is to create trust through recognition and supposed authenticity, as well as to get users to click through irrelevant, emotionally appealing content.

At the level of **social validation,** Portuguese football pro Cristiano Ronaldo in particular is used as a testimonial for Chicken Road. The association with one of the best-known sports personalities in the world is intended to transfer success, prosperity and trustworthiness to advertising – without any recognizable official licensing. This is complemented by staged user-generated content

aesthetics: selfie videos of (mainly) men in front of villas or explanatory videos imitate authentic testimonials with the advertised games.

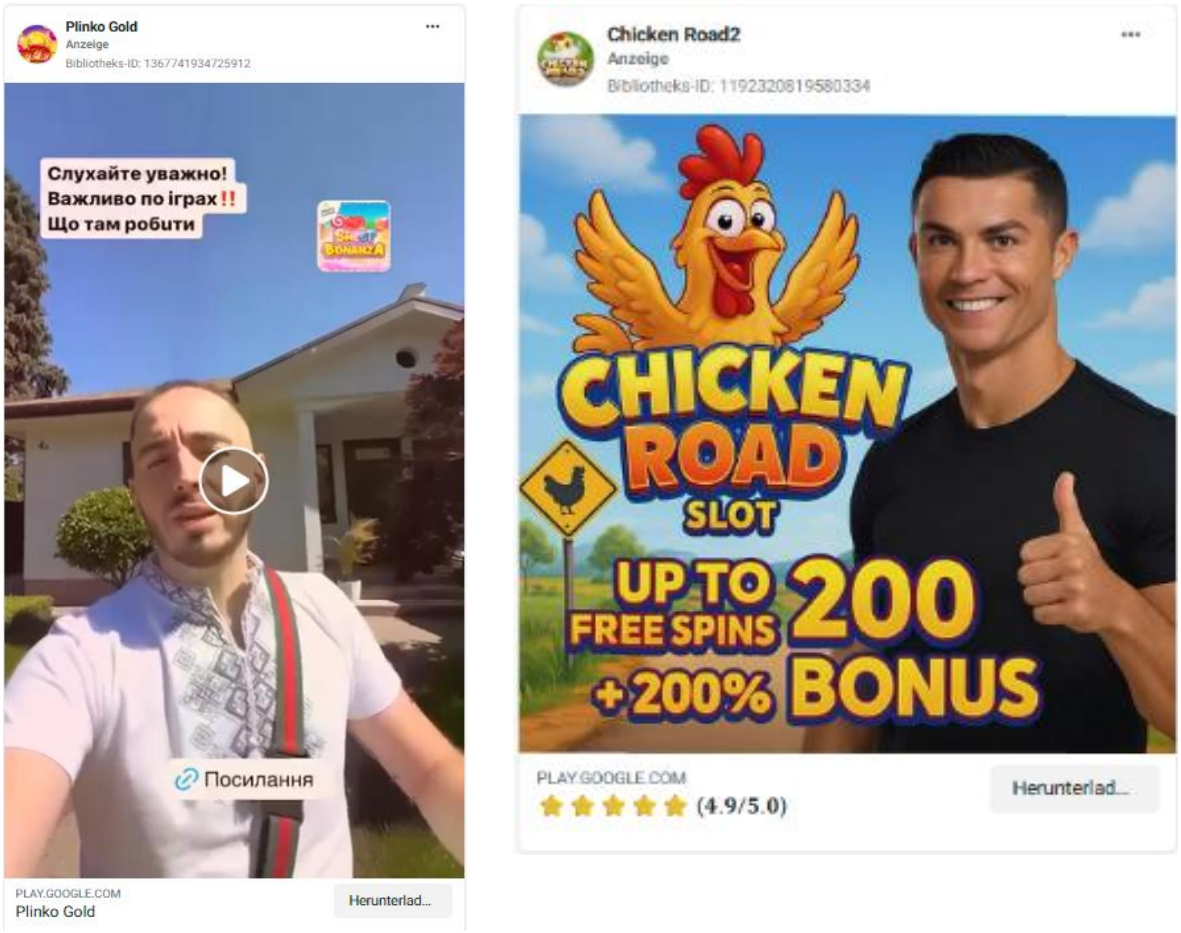

Figure 19: Social validation by celebrities or user-generated content videos

In addition, a classic **bait-and-switch method** is used: The ad preview for some Chicken Road advertising videos shows a Golden Retriever puppy – an emotionally effective but completely irrelevant image content. After clicking on the video, a unique promotional video for the actual

game product is played. The deception is not accidental, but strategic: the emotional entry maximizes the click-through rate before the actual content is revealed.

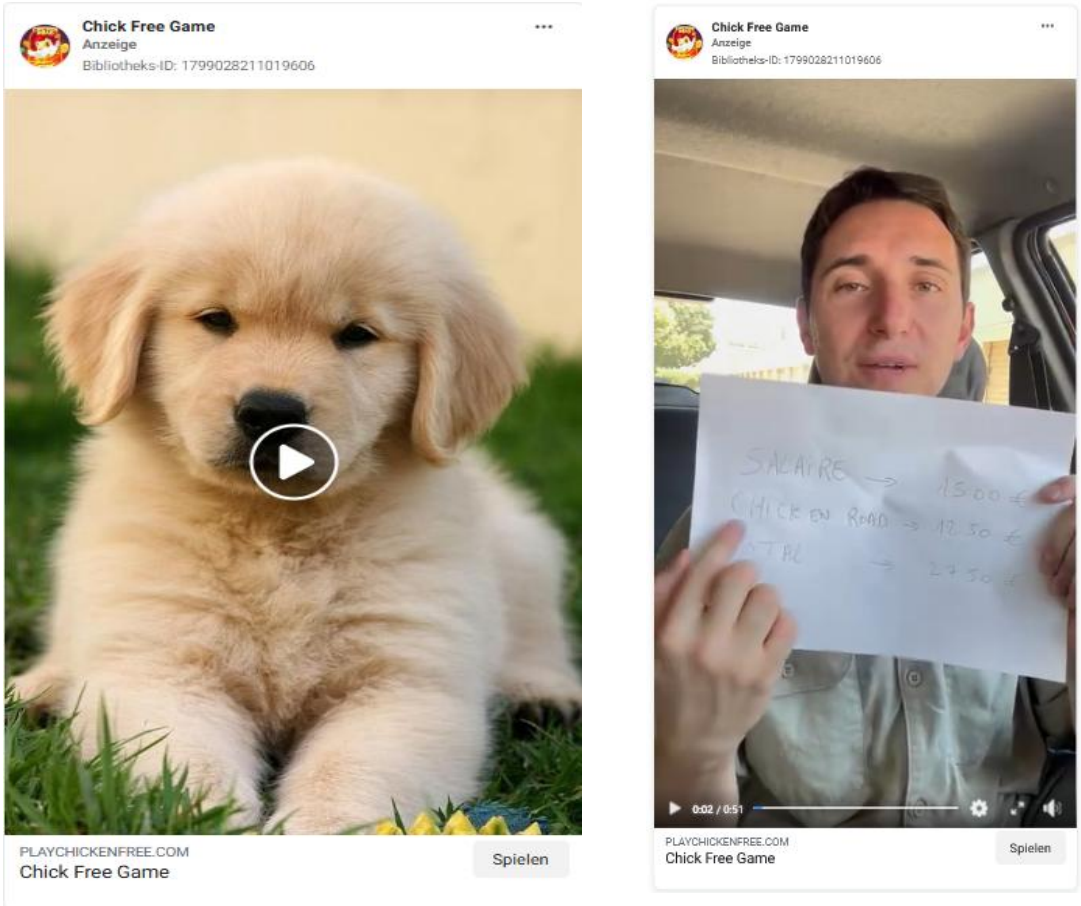

Figure 20: Example of the bait-and-switch method when applying for 'Chicken Road Game' (left: thumbnail; right: actual video)

4.12. Conclusion

In the qualitative analysis, the quantitative findings were deepened and examined with which strategies, narratives and infrastructures fraudulent advertisements operate on Meta platforms.

At the content level, fraudulent actors use **manipulation strategies** across all fraud schemes to induce users to engage in ill-considered interaction – from deceptive design to the targeted construction of knowledge gaps to the systematic misuse of established anchors of trust – the latter also using artificial intelligence and deep fakes. With regard to the target group approach, it can be seen that situational vulnerabilities are not primarily addressed to demographic groups, but to situational vulnerabilities.

A particularly relevant development is the increasing **shift from landing pages to messenger services**, which has been observed in particular in the area of investment fraud. This shift deprives fraudulent activities of traceability by authorities and researchers and at the same time uses the supposed exclusivity of private chat groups as a trust mechanism.

Finally, the complementary infrastructure analysis shows that the seemingly fragmented fraud ecosystem is driven by **professional actors,** recognizable by shared server structures, unified platform solutions and shared tracking services.

5. Security and compliance gaps on Meta services

The Digital Services Act requires VLOPs such as Meta to provide transparency tools that allow independent review of advertisements. The Meta ad library is a key tool to ensure this transparency. However, the quantitative and qualitative analysis identified several structural deficiencies that limit the traceability and verifiability of fraudulent advertisements.

5.1. Non-transparency of paying persons

Article 39 of the DSA (EU 2022/2065) requires the ad library to provide, inter alia, insight into 'the natural or legal person in whose name the advertisement is displayed' or 'who pays for the advertisement'. This is to ensure that those responsible are identifiable. As already explained in the quantitative analysis, this **transparency is not guaranteed in practice.** The input field is a free field and can be filled accordingly by the advertisers. The collected data set includes numerical series, arbitrary letter sequences and brand names that are misused.

This compliance gap is structural in nature: it affects all investigated fraud schemes and is systematically used to make it more difficult to trace. Closely related to this is the lack of identity verification. For example, a standard user account is sufficient for the placement of an advertisement, for which only the name, e-mail address (or telephone number) and a date of birth must be provided – information that the users enter themselves and which is not verified.

According to internal Meta documents leaked to Reuters, Meta pursues a 'reactive only' strategy. It deliberately decided against the widespread introduction of universal identity verification and only introduced it where it is explicitly required by regulations. At the same time, the same documents show that, according to internal tests carried out by Meta itself, universal verification would significantly reduce the proportion of fraudulent advertisements by up to 29% (Horwitz, 2025b).

5.2. Advertisements that can no longer be found

In the course of the research, it became apparent that advertisements documented as part of the quantitative survey could no longer be found at a later stage via the ad library. A concrete example concerns the keyword 'Ella Weber' (ghost stores): almost 2,300 advertisements were identified for this keyword during the survey period. In a new manual search as part of the qualitative analysis, the same keyword no longer yielded any results.

Article 39 of the DSA (EU 2022/2065) requires VLOPs to keep information on advertisements in a publicly available repository for at least one year, even if they are no longer active. Failure **to find previously documented ads** therefore raises the question of whether Meta fully complies with this retention obligation.

The disappearance of advertisements can also be assessed with regard to the aforementioned Reuters research: internal documents are intended to prove that Meta employees specifically search the ad library for keywords that are used by regulatory authorities, researchers and journalists to remove the advertisements found in the process. Internally, this approach is called **'prevalence perception management',** as it aims to reduce the perceived frequency of fraudulent content in external audits. This strategy was first tested in Japan and then rolled out globally, including in Europe and the USA. Meta rejected this presentation in a statement to Reuters, stating that removing ads from the ad library was by no means misleading – on the contrary, less visible fraud ads in the library also meant less fraudulent ads on the platform (Horwitz, 2025b).

5.3. Further advertising activity for (supposedly) deactivated accounts

The quantitative survey found many ads that have already been removed by Meta, including because of a page or account that has been disabled ('This ad was run by an account or page we later disabled for not following our advertising standards'). However, in the context of further surveys, it could be observed that at a later stage advertisements were again displayed on the same account with the same Page ID – despite the alleged deactivation of this account. This phenomenon goes beyond the already known practice of deactivated accounts reappearing under slightly changed names (e.g. 'Höhle der Löwen' or 'Schneider Salzburg' in numerous variants).

5.4. Advertisements cannot be found via text search

Another observable gap on the part of Meta concerns the search function of the ad library. For example, in particular in the case of the investment fraud scheme, fraudulent advertisements are repeatedly identified that cannot be found via a text search. One example is an advertisement with the text 'EXCLUSIVE: Benko admits where the money really went', which was placed by the 'Sorglode' account. The display can be found by searching for the account name 'Sorglode'. However, **a search for text phrases** from the ad text, such as 'Benko confesses', **did not yield any results**. For this reason, some celebrity names had to be removed from the keywords list in

investment fraud – although it was known that advertisements for these keywords exist, no results were achieved with the text search.

Whether this is a technical deficit or a targeted restriction cannot be conclusively assessed from the outside. However, in the context of the documented 'prevalence perception' strategy, such blurring (Horwitz, 2025b) seems to be systematic.

5.5. Multiple ad versions not visible

As described in chapter 4.2 'Perpetrator strategies to circumvent security mechanisms', fraudulent actors often use the **dynamic ad delivery** function to 'hide' fraudulent content in one of several ad versions. While the version initially visible in the ad library appears harmless, one of the other variants contains the problematic content – normally the different versions can be clicked to see the problematic version (usually towards the end).

However, as part of the research, it became increasingly apparent that this function no longer works reliably. In several cases, it was shown that several versions of an ad exist, but only one version was visible. This deficit prevents the screening of dynamic ads and deprives regulators and researchers of an important screening opportunity for hidden fraudulent content.

6. Summary

This study uses Meta's DSA-mandated ad library to systematically capture the scale of fraudulent and problematic advertising. For this purpose, eight central fraud schemes were identified: subscription traps, investment fraud, credit fraud, job fraud, dubious dietary supplement offers, ghost stores, fake shops (focus on brand imitation) and online gambling. The scale of the advertisements placed for these schemes on the Facebook and Instagram platforms was quantitatively collected and supplemented with a qualitative analysis of exemplary advertisements per fraud scheme.

Quantitative survey: Key results

Within three months, **634,000** fraudulent or problematic ads were identified across eight fraud schemes. These reached **more than 1 billion impressions across the EU,** compared to around 123 million in Austria alone. In particular, online gambling dominates (nearly 450,000 ads), followed by investment fraud (83,216) and dubious dietary supplement offers (27,171 ads), while credit fraud (805) has the lowest number of ads.

However, these figures are to be understood as a conservative lower limit: The study does not claim to be exhaustive, as keyword-based search only captures ads with recognizable patterns, so the actual numbers are likely to be significantly higher. In addition, the data depends on the completeness and accuracy of the information provided by Meta.

62.4% of all ads identified in the study were already **removed** by Meta due to non-compliance at the time of collection. At the same time, the identified ads usually have very **short runtimes** of a few days or even hours, and new ads with comparable content appear continuously.

In addition, there are structural patterns in targeting across schemas: While fraudulent actors hardly differentiate by gender or age in demographic targeting, the actual reach data reflect a **targeted approach to situationally vulnerable groups,** which could also be collected as part of the qualitative analysis. For example, advertisements for dietary supplements reached an older target group in particular, while job fraud advertisements targeted people of working age in particular.

Qualitative analysis: key results

Across all fraud schemes, there are four recurring patterns in narratives and the associated targeting:

- **Deceptive design:** Artificial scarcity, staged urgency or 'confirmshaming' are consistent deceptive design strategies designed to induce users to make quick, ill-considered decisions
- **Curiosity Gap:** The systematic construction of knowledge gaps – for example through IQ tests or alleged insider knowledge of financial markets – is used in many fraud schemes to translate the curiosity of users into impulses for action.
- **Abuse of established anchors of trust:** Known personalities, logos and names of media houses or even the establishment of regional references are systematically abused in order to imitate credibility and to use trust in the known. The additional use of AI-generated deepfakes can amplify this effect, e.g. when celebrities are put words in their mouths that they have never said before.
- **Exploitation of situational vulnerabilities:** In the majority of fraud schemes, the narratives used address vulnerable people in a targeted manner – not so much by demographic characteristics, but by individual circumstances. For example, people in financial distress (credit fraud), with health concerns (dietary supplements) or unemployed people (job fraud) are addressed by the content of the advertisements.

At the same time, these content-related strategies go hand in hand with criminal tactics in order to be able to act on the platforms as undetected as possible. For this purpose, different security measures of the platforms as well as content moderation are circumvented. These include:

- Cloaking, whereby users are redirected to a fraudulent website with a click on an advertisement, but verification systems are shown a harmless 'white page';
- the use of compromised and often verified accounts, and
- the placement of multiple ad versions using the Dynamic Ads feature to hide fraudulent ads among seemingly innocuous ads.

This interplay of content and technical strategies shows a fraud ecosystem in which the infrastructure of the platforms is exploited in the same way as the vulnerabilities of the target groups.

A complementary infrastructure analysis of selected routing targets also shows that the fraud ecosystem operates on a professionalized, partly shared technical basis: Cloudflare is used across the board to obfuscate the actual server locations and make traceability more difficult. At the same time, embedded tracking services enable continuous optimization of targeting. HTML similarity

analyses also reveal clusters of websites that are likely to be operated by the same actors despite different appearances.

Meta compliance gaps

In the course of the qualitative analysis, structural deficits on the part of the platform itself were also documented:

- **Intransparency in the case of paying persons:** The free field for paying persons is systematically filled by the fraudsters with false or meaningless information. There is no identity verification. This is in breach of Article 39 of the DSA (EU 2022/2065).
- **Disappearance of documented advertisements:** Previously recorded advertisements could no longer be found in the ad library during later searches. A complete analysis or comprehensibility of the ads placed on Meta is thus made more difficult.
- **Persistence of deactivated accounts:** Even after disabling an account or a page due to non-compliance with policy requirements, advertisements were again displayed at a later date under the same Page ID.
- **Restricted text search:** Relevant advertisements could not be found via the text search – this also makes systematic checks by authorities and researchers more difficult.
- **Incomplete ad versions:** Especially in recent months, it has been observed that the verifiability of multiple ad versions in dynamic ad campaigns is sometimes only possible to a limited extent, as in several cases only one of several versions was visible in the ad library. The fraudulent advertisements could not be detected.

While some of these shortcomings may be due to technical causes, the overall view of documented compliance gaps in conjunction with the internal Meta documents published by Reuters, including a reactive only verification strategy and a global playbook on regulatory perception management, suggests a systematic approach.

Systemic risk within the meaning of the DSA

The study shows that the transparency mechanisms provided for in the Digital Services Act (DSA) provide important starting points for regulatory supervision. The ability to systematically capture and analyse advertisements enables evidence-based documentation of the issue, which can serve as a basis for enforcement action.

At the same time, the results show that simply providing an ad library is not enough to tackle fraudulent advertisements. The study also shows that fraudulent and problematic advertising on Meta platforms is not a marginal phenomenon, but a systemic risk within the meaning of Article 34 of the DSA (EU 2022/2065): the phenomenon is not limited to individual cases but affects numerous ads with billions of reach across eight thematically different fraud schemes.

The DSA provides that VLOPs must not only identify systemic risks but also minimise them through appropriate measures (Article 35 DSA). However, the shortcomings raised suggest that current measures against fraudulent advertisements do not work well enough.

7. Bibliography

Abraham, J. (2025). *Global State of Scams 2025*.

Auer, V., Trell, N., & Brugger, M. (2025). *Dubiose Werbung auf Meta-Plattformen: Wie Celebrity-Ärzte zur Bewerbung von Nahrungsergänzungsmitteln missbraucht werden*. https://research.oiat.at/fileadmin/Research/Dokumente/Safe-NEM-Bericht.pdf

Beltzung, L., Krickl, J., Hölzl, I., & Lindley, A. (2024). *Platform Compliance—Fallstudien zu manipulativen Tricks in der Gestaltung von Interfaces und Prozessen*.

Bouchand, P., Salvatore Romano, Raziye Buse Çetin, Marc Faddoul, Karla Pajares Sangay, & Jinyu Liu. (2025). *Meta's Failing Ad Moderation: Health Scams Targeting EU Users*. AI Forensics. https://aiforensics.org/work/meta-health-ads

Brignull, H. (2023). *Deceptive Patterns*. Deceptive Patterns. https://www.deceptive.design/

Bundesministerium für Inneres. (2025). *Cybercrimereport 2024*. https://www.bmi.gv.at/magazin/2025_11_12/01_Cybercrime_Report.aspx

Burt, J. (2025, Juli 17). Emerging Cloaking-as-a-Service Offerings are Changing Phishing Landscape. *Security Boulevard*. https://securityboulevard.com/2025/07/emerging-cloaking-as-a-service-offerings-are-changing-phishing-landscape/

Europäische Kommission, London Economics, VVA Consulting, & Ipsos Mori. (2016). *Consumer vulnerability across key markets in the European Union*.

Europäisches Parlament & Rat der Europäischen Union. (2006). Verordnung (EG) Nr. 1924/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über nährwert- und gesundheitsbezogene Angaben über Lebensmittel. Amtsblatt der Europäischen Union, L 404, 9–25. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32006R1924

Europäisches Parlament & Rat der Europäischen Union. (2022). Verordnung (EU) Nr. 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste). Amtsblatt der

Europäischen Union, L 277, 1–102. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2065

Federal Trade Commission. (2023). FTC Issues Orders to Social Media and Video Streaming Platforms Regarding *Efforts to Address Surge in Advertising for Fraudulent Products and Scams*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-issues-orders-social-media-video-streaming-platforms-regarding-efforts-address-surge-advertising

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, CHI '18*, 1–14. https://doi.org/10.1145/3173574.3174108

Hatmaker, T. (2023, Mai 5). Hacked verified Facebook pages impersonating Meta are buying ads from Meta. *TechCrunch*. https://techcrunch.com/2023/05/05/hacked-verified-facebook-pages-impersonating-meta-are-buying-ads-from-meta/

Horwitz, J. (2025a). Meta is earning a fortune on a deluge of fraudulent ads, documents show. *Reuters*. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Horwitz, J. (2025b, Dezember 31). Meta created 'playbook' to fend off pressure to crack down on scammers, documents show. *Reuters*. https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763–783. https://doi.org/10.1002/mar.1029

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, *34*(3), 231–245. https://doi.org/10.1007/s11896-019-09334-5

OCCRP. (2025). *Scam Operations Relied on Third-Party Marketing Companies for Steady Stream of Potential Victims*. https://www.occrp.org/en/project/scam-empire/scam-operations-relied-on-third-party-marketing-

companies-for-steady-stream-of-potential-victims

Österreichisches Institut für Angewandte Telekommunikation. (2025). *Verbreitung von Abo-Fallen durch Google Ads*. ÖIAT. https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf

Sapra, B. (2020). *Facebook just filed a lawsuit against a software engineer who it says was helping scammers dodge its ad-review system and post ads related to coronavirus, cryptocurrency and diet pills*. Business Insider. https://www.businessinsider.com/facebook-sues-engineer-leadcloak-helping-covid-19-scammers-ads-2020-4

Scott, K. (2021). You won't believe what's in this paper! Clickbait, relevance and the curiosity gap. *Journal of Pragmatics*, *175*, 53–66. https://doi.org/10.1016/j.pragma.2020.12.023

Social MediaLab. (2025, April 21). The Hidden Game: How Scammers Use 'Chameleon Ads' to Bypass Meta's Moderation. *Social Media Lab*. https://socialmedialab.ca/2025/04/21/the-hidden-game-how-scammers-use-chameleon-ads-to-bypass-metas-moderation/

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, *54*(3), 70–75. https://doi.org/10.1145/1897852.1897872

Vorster, A. (2026). *Fraud and Scams in 2026: What Benelux Banks Can Learn from The Global State of Scams*. https://thebankingscene.com/opinions/fraud-and-scams-in-2026-what-benelux-banks-can-learn-from-the-global-state-of-scams

Watchlist Internet. (2022a). *So schützen Sie sich vor betrügerischen Kreditangeboten*. https://www.watchlist-internet.at/news/so-schuetzen-sie-sich-vor-betruegerischen-kreditangeboten/

Watchlist Internet. (2022b, März 1). *So schützen Sie sich vor betrügerischen Investmentplattformen*. Watchlist Internet. https://www.watchlist-internet.at/news/so-schuetzen-sie-sich-vor-betruegerischen-investmentplattformen/

Watchlist Internet. (2024). *Promis als Lockvögel: Werbung für betrügerische Investmentplattformen erreicht täglich 200.000 Österreicher:innen*. Watchlist Internet. https://www.watchlist-internet.at/news/werbung-promis-investmentbetrug/

Watchlist Internet. (2025a). *Betrügerische Jobangebote*. Watchlist Internet. https://www.watchlist-

internet.at/liste-jobangebote/

Watchlist Internet. (2025b). *Betrügerische Werbeanzeigen: Mehr als 30 Millionen Mal an Personen in Österreich ausgespielt*. Watchlist Internet. https://www.watchlist-internet.at/news/betruegerische-werbeanzeigen-mit-vermeintlicher-geschaeftsschliessung/

Which. (2022). *TOWARD A FUTURE WITHOUT FRAUD: How platforms can do more to tackle misleading and fraudulent adverts online*. Site. https://www.which.co.uk/policy/policy/digital/9228/toward-a-future-without-fraud-how-platforms-can-do-more-to-tackle-misleading-and-fraudulent-adverts-online