

RECHT · PLATTFORMHAFTUNG

Haftung digitaler Werbeplattformen bei Recovery-Scams

Wann werden Google Ads zum Einfallstor organisierter Anlagebetrüger? Die Kategorisierungslücke: rechtlicher Rahmen, internationaler Vergleich, Ökonomie und ein Verifizierungskonzept für Recovery-Anbieter. 2., erweiterte Auflage.

Wer einen Kreditvermittler verifizieren kann, kann auch einen „Vermögensermittler“ verifizieren

Recovery-Agenturen unterliegen bei Google Ads keiner mit klassischer Finanzwerbung vergleichbaren Verifizierungspflicht — nicht weil eine Prüfung unmöglich wäre, sondern weil die Kategorie „Asset Recovery“ im Regelwerk schlicht nicht als eigene, zertifizierungspflichtige Kategorie existiert.

FINANZ-FORENSIK · FINANCIAL INTELLIGENCE & BLOCKCHAIN FORENSICS

RESEARCH REPORT 08 / 2026

10.500+

IC3-Beschwerden zu Recovery-Scams, USA 2025

1,4 Mrd. \$

gemeldeter Recovery-Scam-Schaden, USA 2025 (IC3)

27%

der gemeldeten Betrugsanzeigen tatsächlich entfernt (BEUC/vzbv)

7–16 Mrd. \$

interner Meta-Umsatz aus Risiko-Anzeigen p. a. (Reuters)

Zentrale These dieses Whitepapers: Recovery-Agenturen unterliegen bei Google Ads bislang keiner mit klassischer Finanzwerbung vergleichbaren Verifizierungspflicht – nicht weil eine Prüfung technisch unmöglich wäre, sondern weil die Kategorie „Vermögensermittlung“ bzw. „Asset Recovery“ im Regelwerk schlicht nicht als eigene, zertifizierungspflichtige Kategorie existiert. Diese Kategorisierungslücke lässt sich, wie Kapitel 6 und 7 im Detail zeigen, unmittelbar am offiziellen Wortlaut der Google-Ads-Richtlinien nachweisen.

Für Opfer von Anlagebetrug beginnt die zweite Katastrophe oft dort, wo sie Hilfe suchen: bei Google. Wer nach einem Verlust durch eine gefälschte Handelsplattform nach Begriffen wie „Geld von Betrügern zurückholen“ sucht, trifft in den Anzeigenplätzen regelmäßig auf vermeintliche „Vermögensermittler“ – von denen ein erheblicher Teil selbst Betrüger sind. Google verifiziert Anbieter von Krediten, Schuldnerberatung und Kryptowährungen nachweislich seit Jahren; für „Vermögensermittler“-Anzeigen existiert dagegen keine gesonderte, öffentlich dokumentierte Prüfkategorie.

Dieses Whitepaper verbindet vier Ebenen, die bewusst getrennt gehalten werden: erstens den europäischen und deutschen Rechtsrahmen (E-Commerce-Richtlinie, DSA, deutsche Störerhaftungs-Rechtsprechung), zweitens einen internationalen Vergleich (USA, Vereinigtes Königreich, Australien), drittens eine ökonomische Analyse des anzeigenfinanzierten Geschäftsmodells und viertens qualitative Beobachtungen aus der forensischen Fallarbeit von finanz-forensik.de. Rechtsprechung wird als Rechtsprechung zitiert, Studienergebnisse Dritter als solche gekennzeichnet, eigene Fallbeobachtungen ausdrücklich als qualitativ und nicht-repräsentativ ausgewiesen.

Die wichtigsten Belege im Überblick: Allein in den USA registrierte die FBI-Meldestelle IC3 2025 mehr als 10.500 Beschwerden zu Recovery-Scams mit einem Schaden von rund 1,4 Milliarden US-Dollar. Der Bericht „Sponsored by Scammers“ von BEUC und vzbv zeigt, dass von rund 900 gemeldeten Finanzbetrugs-Anzeigen bei Google, Meta und TikTok nur 27 % entfernt wurden. Und eine Reuters-Recherche auf Basis interner Meta-Dokumente legt offen, dass ein einzelner Plattformbetreiber nach eigener in-

terner Kalkulation jährlich rund 7 bis 16 Milliarden US-Dollar Umsatz mit Anzeigen erzielt, die als Betrug oder Verstoß eingestuft werden. Das Problem ist damit nicht nur ein juristisches – es ist, wie Kapitel 8 zeigt, auch ein ökonomisches.

METHODISCHER HINWEIS

Dieses Whitepaper unterscheidet strikt zwischen extern erhobenen, mit Quellenangabe zitierten Rechtsprechungs- und Studienergebnissen (insbesondere Kapitel 3, 4, 5 und 6) und qualitativen, anonymisierten Beobachtungen aus der forensischen Fallarbeit von finanz-forensik.de (insbesondere Kapitel 7.2 und 11). Letztere stellen ausdrücklich keine repräsentative Stichprobe und keine eigene Statistik dar. Die in Kapitel 2.2 dargestellten Fallmuster sind illustrative, anonymisierte Komposit-Szenarien, die wiederkehrende, auch von Dritten (z. B. der USAufsichtsbehörde CFTC) beschriebene Vorgehensweisen veranschaulichen – sie geben keine realen Einzelfälle mit realen Beträgen wieder.

01 Einleitung: Der Recovery-Scam als zweiter Angriff

Recovery-Scams setzen an einem psychologisch besonders verwundbaren Punkt an: dem Moment, in dem ein Opfer den Verlust seines Investments bereits erkannt hat und aktiv nach einem Ausweg sucht. Die US-Terminaufsicht CFTC beschreibt dieses Muster in einer eigenen Verbraucherwarnung als klassischen „Advance-Fee-Fraud“ – Vorschussbetrug, bei dem für die Aussicht auf eine größere Rückzahlung zunächst eine kleinere Zahlung verlangt wird – und weist darauf hin, dass Recovery-Betrüger gezielt bereits Geschädigte erneut ins Visier nehmen.

Anders als beim ursprünglichen Anlagebetrug, der häufig über Messenger-Kontakt oder soziale Netzwerke eingeleitet wird, erfolgt der Erstkontakt beim Recovery-Scam in vielen Fällen über eine aktive Suche des Opfers selbst – und damit über einen Kanal, den die Werbepattform unmittelbar kontrolliert: bezahlte Suchanzeigen. Diese Kontrollmöglichkeit ist der Ausgangspunkt der rechtlichen Fragestellung dieses Whitepapers.

02 Anatomie eines anzeigenbasierten Recovery-Scams

2.1 Typischer Ablauf

In der von finanz-forensik.de beobachteten Fallarbeit folgt der anzeigenbasierte Recovery-Scam typischerweise einem wiederkehrenden Muster:

- **Erster Verlust:** Das Opfer verliert Geld über eine gefälschte Handelsplattform oder eine andere Anlagemasche und erkennt den Verlust.
- **Aktive Suche:** Das Opfer sucht selbst nach Begriffen wie „Krypto-Betrug Geld zurückholen“ oder „Vermögensermittler Betrug“.
- **Gesponserte Anzeige:** Unter den Suchergebnissen erscheint eine bezahlte Anzeige eines vermeintlichen Vermögensermittlers – professionell gestaltet, oft mit nachgeahmten Gütesiegeln oder Verweisen auf angebliche Kooperationen mit Strafverfolgungsbehörden.
- **Kontakt und Vorkasse:** Nach einem Erstgespräch wird eine Vorabgebühr für „Ermittlungskosten“ oder „Freischaltungskosten“ verlangt.
- **Zweiter Verlust:** Die versprochene Rückholung bleibt aus.

Die CFTC beschreibt in ihrer Verbraucherwarnung „Don't be Re-Victimized by Recovery Frauds“ zwei ergänzende, empirisch dokumentierte Taktiken, die dieses Grundmuster verstärken: Erstens platzieren Täter gezielt scheinbar redaktionelle Presseartikel über angebliche „Fraud-Recovery-Experten“ bei lokalen Nachrichtenportalen, um Vertrauen aufzubauen, bevor die eigentliche Anzeige überhaupt geschaltet wird. Zweitens verkaufen oder recyceln Täter „Opferlisten“ aus vorangegangenen Betrugsfällen, sodass Geschädigte gezielt – teils unter Vortäuschung eines Behörden- oder Anwaltskontakts – erneut angesprochen werden. Die CFTC verweist dabei auf kriminologische Forschung, wonach die Mehrheit der Betrugsoffer mehrfach viktimisiert wird und bereits Geschädigte mit überdurchschnittlicher Wahrscheinlichkeit erneut zur Zielscheibe werden.

2.2 Illustrative Fallmuster

Die folgenden drei Szenarien sind anonymisierte, illustrative Komposit-Darstellungen wiederkehrender Muster – keine Wiedergabe realer Einzelfälle mit realen Beträgen. Sie verbinden die in 2.1 beschriebene anzeigenbasierte Kontaktaufnahme mit den von der CFTC unabhängig dokumentierten Betrugstaktiken.

MUSTER A · DER DIREKTE ANZEIGENKLICK

- Ausgangspunkt ist ein vorangegangener Krypto-Anlagebetrug.
- Das Opfer sucht bei Google gezielt nach Möglichkeiten, das verlorene Geld zurückzuerhalten.
- Es klickt auf eine gesponserte Anzeige eines „Vermögensermittlers“ mit professionell gestalteter Website.
- Nach einem unverbindlichen Erstgespräch wird eine Vorabgebühr für „Ermittlungs- und Rechtskosten“ verlangt.
- Die versprochene Rückholung bleibt aus; der Kontakt bricht ab, sobald keine weiteren Zahlungen mehr erfolgen.

MUSTER B · DIE „FAKED-NEWS“-VARIANTE

- Vor dem eigentlichen Anzeigenkontakt stößt das Opfer online auf einen scheinbar redaktionellen Artikel über einen „erfolgreichen Vermögensermittler“ – ein von der CFTC beschriebenes Täuschungsmuster, bei dem Täter Presseartikel über Presseverteiler-Dienste platzieren.
- Dieser Artikel erhöht die wahrgenommene Glaubwürdigkeit der anschließend geklickten Anzeige zusätzlich.
- Der weitere Ablauf entspricht Muster A.

MUSTER C · WIEDERANSPRACHE ÜBER RECYCELTE KONTAKTDATEN

- Das Opfer hatte bereits zuvor Kontaktdaten bei einem ersten – nicht notwendig anzeigenbasierten – Betrugsversuch hinterlassen.
- Wochen oder Monate später wird es erneut kontaktiert, diesmal unter dem Vorwand eines „Ermittlungserfolgs“ oder einer bevorstehenden Gerichtsentscheidung zu seinen Gunsten.
- Die CFTC beschreibt dieses Vorgehen als Verkauf bzw. Wiederverwendung von „Opferlisten“ zwischen Tätergruppen.

03 Der rechtliche Rahmen

Die Haftung von Werbepattformen für Werbekundeninhalte ist keine neue Rechtsfrage – sie wurde bereits im Zusammenhang mit Markenrechtsverletzungen bei AdWords-Anzeigen und mit ehrverletzenden Autocomplete-Vorschlägen höchststrichterlich verhandelt. Der Digital Services Act hat diesen Rahmen seit 2024 grundlegend erweitert und um eine präventive, systemische Dimension ergänzt.

3.1 Das Ausgangsprinzip: Haftungsprivileg für Hosting-Anbieter

Sowohl die frühere E-Commerce-Richtlinie (Art. 14) als auch ihr Nachfolger, der Digital Services Act (Art. 6), privilegieren Anbieter, die fremde Inhalte lediglich speichern oder verbreiten, ohne deren Inhalt zu kennen oder zu kontrollieren: Solange der Anbieter keine tatsächliche Kenntnis von der Rechtswidrigkeit hat und nach Kenntniserlangung zügig handelt, haftet er grundsätzlich nicht wie ein eigener Inhalte-Anbieter. In Deutschland setzte zunächst das Telemediengesetz (TMG) dieses Haftungsprivileg um; es wurde 2024 durch das Digitale-Dienste-Gesetz (DDG) abgelöst, das den DSA in nationales Recht einbettet. Die allgemeine Störerhaftung nach klassischem TMG-Verständnis wurde dabei weitgehend zurückgebaut – gesonderte Regelungen bestehen im DDG nur noch für WLAN-Betreiber.

Für Werbeplattformen bedeutet dies im Ausgangspunkt: Eine rechtswidrige Anzeige eines Werbekunden begründet nicht automatisch eine Haftung der Plattform selbst. Diese Privilegierung ist jedoch an Bedingungen geknüpft, die im Fall organisierter, anzeigenbasierter Recovery-Scams zunehmend infrage stehen.

3.2 Deutsche Rechtsprechung: von der Störerhaftung zur Kenntnis-Schwelle

Der Bundesgerichtshof hat die Grundlinie für die Haftung von Suchmaschinenbetreibern im sogenannten Autocomplete-Urteil gezogen (BGH, Urteil vom 14.05.2013, Az. VI ZR 269/12): Ein Suchmaschinenbetreiber haftet für automatisch generierte, ehrverletzende Vorschläge erst ab Kenntnisnahme der Rechtsverletzung, nicht bereits ab automatisierter Generierung des Inhalts durch einen Algorithmus. Übertragen auf Werbeanzeigen bedeutet dies: Der Umstand, dass eine Anzeige automatisiert – etwa im Rahmen eines Bietverfahrens – ausgeliefert wird, entlastet die Plattform nicht grundsätzlich, sobald sie konkrete Kenntnis von deren Rechtswidrigkeit erlangt hat.

Spezifisch zu AdWords-Anzeigen hat das OLG Frankfurt am Main entschieden (Beschluss vom 27.02.2020, Az. 6 U 240/19), dass die markenrechtliche Störerhaftung für die Verwendung fremder Marken in AdWords-Kampagnen in erster Linie den werbenden Kunden trifft, nicht den Suchmaschinenbetreiber – solange dieser keine eigene, aktive Rolle bei der Gestaltung des beanstandeten Inhalts einnimmt. Beide Entscheidungen etablieren im Ergebnis ein Kenntnis-Modell: Solange die Plattform keine positive Kenntnis von der Rechtswidrigkeit einer konkreten Anzeige hat und nach Meldung zügig reagiert, bleibt sie haftungsprivilegiert.

Für Recovery-Scam-Anzeigen ist diese Kenntnisschwelle der entscheidende Hebel: Sobald eine Plattform wiederholt Meldungen zu strukturell vergleichbaren Anzeigen desselben oder eines erkennbar verbundenen Werbekunden erhält, wird die Berufung auf fehlende Kenntnis zunehmend schwerer haltbar.

3.3 Der Digital Services Act: von Reaktion zu Systemverantwortung

Der DSA verändert diesen Rahmen in zweierlei Hinsicht. Erstens konkretisiert er das reaktive Melde-Modell: Art. 16 DSA verpflichtet Hosting-Anbieter zu einem funktionierenden Melde- und Abhilfeverfahren („Notice-and-Action“), Art. 22 DSA führt einen privilegierten Meldeweg für sogenannte Trusted Flagger ein. Zweitens verpflichten Art. 34 und 35 DSA sehr große Online-Plattformen und Suchmaschinen (VLOP/VLOSE, definiert über mehr als 45 Millionen monatliche Nutzer in der EU) zu einer systemischen Risikobewertung und -minderung. Google Search und Google Ads erfüllen als VLOSE bzw. im Kontext der Google-Dienstflotte die Schwellenwerte für diese verschärften Pflichten.

Ergänzend verpflichtet Art. 39 DSA VLOPs und VLOSEs zu umfassender Werbetransparenz: Anzeigeninhalt, Auftraggeber und grobe Zielgruppenparameter müssen in einer öffentlich zugänglichen Anzeigendatenbank dokumentiert werden – für die forensische Nachverfolgung von Recovery-Scam-Kampagnen von unmittelbarer praktischer Bedeutung. Bei Verstößen gegen die systemischen Pflichten aus Art. 34/35 DSA drohen Bußgelder von bis zu 6 % des weltweiten Jahresumsatzes des Konzerns.

3.4 Die „aktive Rolle“-Doktrin des EuGH

Der Europäische Gerichtshof hat in seiner Rechtsprechung zu Online-Marktplätzen und Suchmaschinenwerbung (grundlegend in der Google-France/Louis-Vuitton-Entscheidungslinie sowie in der L'Oréal/eBay-Rechtsprechung) ein Kriterium entwickelt, das über den DSA-Wortlaut hinaus Bedeutung behält: Das Haftungsprivileg entfällt, sobald ein Anbieter eine „aktive Rolle“ einnimmt, die ihm Kenntnis von oder Kontrolle über die betreffenden Daten verschafft.

Für Google Ads ist dies keine rein akademische Frage: Das Anzeigen-Ranking, die algorithmische Zielgruppenauswahl (Targeting) und qualitätsbasierte Gebotsmechanismen sind gerade keine neutrale, rein technische Weiterleitung, sondern eine aktive redaktionelle und kommerzielle Gestaltungsleistung der Plattform. Diese Spannung zwischen der EuGH-Doktrin und dem tatsächlichen Geschäftsmodell datengetriebener Anzeigenauslieferung ist nach Einschätzung von finanz-forensik.de einer der am wenigsten diskutierten, aber rechtlich zentralen Aspekte der gesamten Debatte.

04 Internationaler Vergleich

Die in Kapitel 3 beschriebene europäische Entwicklung steht nicht isoliert. In den USA, im Vereinigten Königreich und in Australien lassen sich unabhängig voneinander vergleichbare Trends beobachten: eine wachsende regulatorische und gerichtliche Bereitschaft, Werbeplattformen nicht mehr nur als neutrale Vermittler, sondern als Mitverantwortliche für die von ihnen monetarisierten Anzeigeninhalte zu behandeln.

4.1 USA: Section-230-Erosion und die Größenordnung des Problems

Die US-amerikanische Internet-Meldestelle IC3 (FBI Internet Crime Complaint Center) registrierte 2025 mehr als 10.500 Beschwerden speziell zu Recovery-Scams mit einem geschätzten Gesamtschaden von rund 1,4 Milliarden US-Dollar. Das FBI-eigene „Recovery Asset Team“ konnte im gleichen Jahr rund 679 Millionen US-Dollar in 3.900 Vorfällen einfrieren – eine Erfolgsquote von 58 %, die zugleich zeigt, wie viel Schaden trotz funktionierender Rückverfolgung bereits eingetreten ist, bevor überhaupt eingegriffen werden kann.

Die US-Terminaufsicht CFTC warnt in einer eigenen Verbraucherinformation ausdrücklich vor Recovery-Betrug als Form des Advance-Fee-Fraud (siehe Kapitel 2.1) und empfiehlt Betroffenen konkrete Warnsignale (Kapitel 12).

Rechtlich bemerkenswert ist die Entwicklung der Section-230-Rechtsprechung: Die Consumer Federation of America verklagte Meta mit der Begründung, der Konzern täusche Nutzer über das tatsächliche Betrugsrisiko auf seinen Plattformen und profitiere gezielt von betrügerischen Anzeigen. Meta berief sich zunächst auf die weitreichende Haftungsimunität aus Section 230 des Communications Decency Act. Der Ninth Circuit Court of Appeals entschied jedoch, dass Section 230 Meta nicht vor Ansprüchen schützt, die sich auf gebrochene vertragliche Zusagen in den eigenen Nutzungsbedingungen stützen – ein Präzedenzfall, der die Reichweite der klassischen Plattformimmunität in den USA spürbar einschränkt. Parallel verklagte auch der kalifornische Bezirk Santa Clara County Meta mit der Begründung, der Konzern profitiere systematisch von betrügerischen Anzeigen auf Facebook und Instagram.

Wie groß dieser wirtschaftliche Anreiz sein kann, legte eine Investigativ-Recherche von Reuters (Ende 2025 / Anfang 2026) anhand interner Meta-Dokumente offen: Demnach zeigte Meta Nutzern durchschnittlich rund 15 Milliarden als „höheres Risiko“ eingestufte Anzeigen pro Tag; für 2024 kalkulierte der Konzern intern mit einem Umsatz von rund 7 Milliarden US-Dollar aus solchen Anzeigen, mit einer internen Projektion von bis zu 16 Milliarden US-Dollar (rund 10,1 % des Gesamtumsatzes) aus Werbung für Betrug und verbotene Produkte insgesamt. Die Dokumente sollen zudem ein internes „Playbook“ beschreiben, das eine bewusst reaktive Durchsetzungsstrategie vorsah und Verifizierungspflichten nur dort einführte, wo dies rechtlich zwingend war. Diese Zahlen betreffen ausdrücklich Meta, nicht Google; sie werden hier als Beleg dafür herangezogen, dass das strukturelle ökonomische Anreizproblem anzeigenfinanzierter Plattformen real und dokumentiert ist – nicht als Aussage über Googles konkrete interne Kalkulation (vertieft in Kapitel 8).

4.2 Vereinigtes Königreich: vom Kulanz-Modell zur bindenden Aufsichtspflicht

Der britische Online Safety Act 2023 (Royal Assent am 26. Oktober 2023) führt erstmals eine gesetzliche Pflicht zum Schutz vor betrügerischer Werbung ein und beauftragt die Medienaufsicht Ofcom mit deren Durchsetzung. Am 10. Juli 2026 – nur zwei Wochen vor Fertigstellung dieses Whitepapers – eröffnete Ofcom eine Konsultation zu knapp 40 konkreten Maßnahmen eines „Fraudulent Advertising Code of Practice“, der erstmals verbindliche Pflichten für als Kategorie-1- oder Kategorie-2A-Dienst eingestufte Plattformen bei bezahlter Werbung vorsieht. Verstöße können mit Bußgeldern von bis zu 18 Millionen Pfund oder 10 % des weltweiten Konzernumsatzes geahndet werden – je nachdem, welcher Betrag höher ist. Nach Ofcom-Schätzungen verlieren britische Verbraucher jährlich rund 200 Millionen Pfund allein durch betrügerische Werbeanzeigen.

Dass regulatorischer Druck in Großbritannien bereits vor dem Online Safety Act wirksam war, zeigt die Rolle der Finanzaufsicht FCA: Sie erwirkte bereits 2023 die Rücknahme oder Änderung von mehr als 10.000 irreführenden Finanzwerbe-Anzeigen und leitete gezielte Maßnahmen gegen sogenannte „Finfluencer“ ein, die Finanzprodukte ohne erforderliche Zulassung bewarben. Genau dieser Druck war es, der Google 2021 zur Einführung seiner ersten Finanzwerbe-Verifizierung im Vereinigten Königreich bewog (siehe Kapitel 5.3).

4.3 Australien: ACCC gegen Meta als Vergleichsfall

Die australische Wettbewerbs- und Verbraucherschutzbehörde ACCC führt ein Verfahren gegen Meta, in dessen Rahmen eigene Untersuchungen der Behörde ergaben, dass ein erheblicher Anteil – nach ACCC-Angaben rund 58 % – der überprüften, gemeldeten Krypto-Werbeanzeigen tatsächlich gegen Plattformrichtlinien verstieß oder betrügerischer Natur war. Dieser Befund stützt die These, dass das beschriebene Muster keine Besonderheit einer einzelnen Plattform oder Jurisdiktion ist, sondern ein strukturelles Problem des anzeigenbasierten Geschäftsmodells insgesamt.

4.4 Zwischenfazit: eine konvergierende Entwicklung

Die EU (DSA), das Vereinigte Königreich (Online Safety Act/Ofcom-Code), die USA (Section-230-Erosion durch Gerichte) und indirekt Australien (ACCC-Verfahren) bewegen sich unabhängig voneinander in dieselbe Richtung: weg von einer rein reaktiven Kenntnis-Schwelle, hin zu einer proaktiven Systemverantwortung für Werbeplattformen. Keine dieser Entwicklungen adressiert bislang jedoch spezifisch die in Kapitel 6 und 7 beschriebene Kategorisierungslücke bei Recovery-Anzeigen.

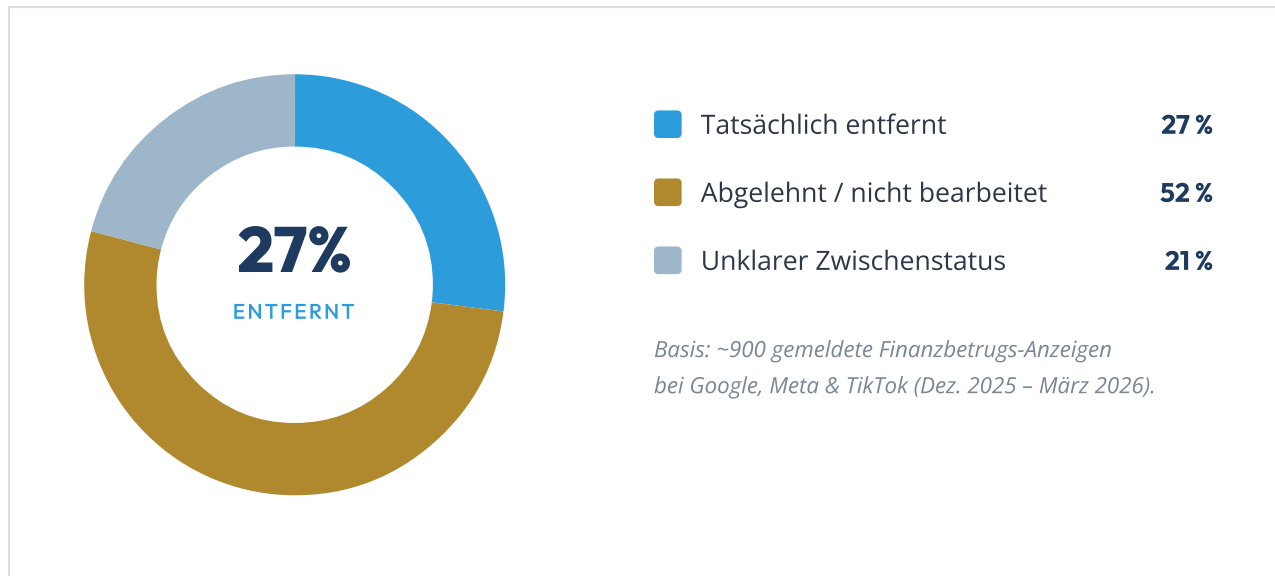
05 Wenn Regeln auf Realität treffen: die Beschwerdelage in der EU

5.1 „Sponsored by Scammers“: der BEUC/vzbv-Bericht

Im Mai 2026 veröffentlichten der Europäische Verbraucherverband BEUC und 13 nationale Mitgliedsorganisationen – in Deutschland der Verbraucherzentrale Bundesverband (vzbv) – den Bericht „Sponsored by Scammers“. Die Organisationen hatten zwischen Dezember 2025 und März 2026 rund 900 mutmaßlich rechtswidrige Finanzwerbe-Anzeigen bei Google, Meta und TikTok gemeldet und die Plattformreaktionen systematisch ausgewertet.

Das zentrale Ergebnis: Nur 27 % der gemeldeten Anzeigen wurden tatsächlich entfernt; 52 % wurden abgelehnt oder schlicht nicht bearbeitet, die übrigen 21 % verblieben in einem unklaren Zwischenstatus. Ramona Pop, Vorständin des vzbv, wird in der Pressemitteilung sinngemäß mit der Aussage zitiert, Google, Meta und TikTok täten nicht genug gegen Werbung für betrügerische Angebote wie Fake-Shops oder unseriöse Finanzberatung; die Anbieter müssten sicherstellen, dass Verbraucher über ihre

Plattformen nicht Opfer von Betrug würden, und sowohl die EU-Kommission als auch nationale Behörden müssten für Konsequenzen sorgen. Die Verbraucherorganisationen reichten auf dieser Grundlage im Mai 2026 formelle DSA-Beschwerden gegen alle drei Plattformen ein.



Plattformreaktion auf gemeldete Betrugsanzeigen. Nur gut ein Viertel der gemeldeten Anzeigen wurde tatsächlich entfernt. Quelle: BEUC/vzbv, „Sponsored by Scammers“, Mai 2026.

5.2 Das Auskunftersuchen der EU-Kommission

Im September 2025 richtete die Europäische Kommission im Rahmen ihrer DSA-Aufsichtsbefugnisse ein förmliches Auskunftersuchen (Request for Information) unter anderem an Google, mit dem Ziel, Informationen zu Maßnahmen gegen Finanzbetrugs-Anzeigen zu erhalten. Ein solches Auskunftersuchen ist regelmäßig der erste förmliche Verfahrensschritt vor einem möglichen DSA-Aufsichtsverfahren.

5.3 Der Machbarkeitsbeweis: Googles eigener Verifizierungs-Rollout

Besonders aufschlussreich ist, dass Google selbst seit Jahren zeigt, dass eine wirksame Vorab-Prüfung von Finanzwerbung technisch und organisatorisch möglich ist – wenn regulatorischer Druck hoch genug ist. Nach anhaltendem Druck der FCA (Kapitel 4.2) führte Google 2021 im Vereinigten Königreich eine verpflichtende Verifizierung für Finanzwerbetreibende ein; seit Januar 2023 setzt Google dort Verstöße durch Kontosperrung durch. Im Juni 2025 wurde diese Verifizierungspflicht in Deutschland auf den Bereich Schuldnerberatung ausgeweitet. Am 23. Juli 2026 tritt die Verifizierungspflicht für Finanzwerbung planmäßig in 24 weiteren EU- und EWR-Staaten in Kraft.

Dieser Rollout entkräftet die spätere Argumentation, eine lückenlose Vorab-Prüfung sei technisch unmöglich oder unverhältnismäßig aufwendig: Wenn Google in der Lage ist, Werbetreibende im Bereich regulierter Finanzdienstleistungen europaweit zu verifizieren, stellt sich die Frage, warum eine strukturell vergleichbare Prüfung nicht auch für Recovery- bzw. Vermögensermittlungs-Dienstleistungen erfolgt.

06 Die Google-Ads-Richtlinien im Detail

Um die in der Management Summary formulierte These zu belegen, lohnt ein systematischer Blick in den öffentlichen Wortlaut der Google-Ads-Werberichtlinien zu Finanzprodukten und -dienstleistungen (Stand: Recherche Juli 2026).

6.1 Was Google bereits reguliert

Die offizielle Richtlinie „Financial products and services“ definiert Finanzprodukte und -dienstleistungen als Produkte und Dienstleistungen im Zusammenhang mit der Verwaltung oder Anlage von Geld und Kryptowährungen, einschließlich individueller Beratung, und listet folgende, ausdrücklich benannte und jeweils mit eigenen Offenlegungs- oder Zertifizierungspflichten versehene Unterkategorien auf:

- **Privatkredite (Personal loans)** – u. a. Pflichtangaben zu Rückzahlungsfrist, effektivem Jahreszins und Gesamtkosten.
- **Hochzins-Privatkredite (USA-spezifisch)** – Anzeigen für Kredite mit einem effektiven Jahreszins ab 36 % sind untersagt.
- **Umschuldung/Loan Modification** – u. a. Verbot von Erfolgsgarantien und Vorabgebühren außerhalb anwaltlicher Leistungen.
- **Kreditreparatur-Dienstleistungen (Credit repair services)** – Anzeigen sind generell nicht zulässig.
- **Schuldnerdienstleistungen (Debt services)** – nur in ausgewählten Regionen und nach Zertifizierung zulässig.
- **Binäre Optionen** – Anzeigen sind generell nicht zulässig.
- **Komplexe spekulative Finanzprodukte** (u. a. CFDs, Forex) – nur für lizenzierte Anbieter nach Zertifizierung.
- **Kryptowährungen und verwandte Produkte** – mit und ohne Zertifizierung, je nach Zielregion.
- **Prediction Markets** – nur nach Zertifizierung als regulierter Terminmarkt-Vertrag.

Für alle zertifizierungspflichtigen Kategorien gilt zudem eine allgemeine Offenlegungspflicht: Werbetreibende müssen die physische Geschäftsadresse, sämtliche Gebühren sowie – sofern eine Zugehörigkeit behauptet wird – Nachweise für Dritt-Akkreditierungen klar und unmittelbar sichtbar angeben.

6.2 Was Google bereits verbietet, aber nur reaktiv durchsetzt

Unabhängig von den in 6.1 genannten Finanzkategorien untersagt die Richtlinie „Unacceptable business practices“ allgemein, Nutzer durch Verschleierung oder Falschdarstellung zu täuschen – etwa durch das Vortäuschen einer Zugehörigkeit zu einer anderen Organisation, das Anbieten von Leistungen, die nicht erbracht werden können oder für die die erforderlichen Lizenzen fehlen, oder durch Phishing und die missbräuchliche Nutzung fremder Identitäten. Ein Recovery-Scam, der eine tatsächlich nicht erbrachte Rückholleistung verspricht, verstößt damit bereits gegen diese allgemeine Richtlinie.

Der entscheidende Unterschied zu den Kategorien aus 6.1 liegt jedoch im Durchsetzungsmechanismus: Verstöße gegen die Kategorien aus 6.1 werden – soweit zertifizierungspflichtig – bereits vor der ersten Anzeigenschaltung geprüft. Verstöße gegen die „Unacceptable business practices“-Richtlinie werden dagegen laut Richtlinien text „bei Entdeckung“ geahndet – also reaktiv, nach Anzeigenschaltung, in aller Regel nach einer Meldung oder einem automatisierten Abgleichtreffer.

6.3 Die Lücke im Wortlaut

Bemerkenswert ist, was in der Aufzählung aus 6.1 nicht vorkommt: Weder „Vermögensermittlung“ noch „Asset Recovery“ noch eine vergleichbare Bezeichnung erscheint als eigene, benannte Unterkategorie der Google-Ads-Finanzrichtlinien. Anbieter von Recovery-Dienstleistungen fallen damit – jedenfalls nach dem öffentlich einsehbaren Richtlinienwortlaut – standardmäßig nicht in eine der zertifizier-

rungspflichtigen Kategorien, sondern lediglich unter die allgemeine, reaktive Missbrauchsaufsicht aus 6.2. Diese textliche Lücke ist der unmittelbare Beleg für die in diesem Whitepaper als „Kategorisierungslücke“ bezeichnete These.

07 Die Kategorisierungslücke: Nachweis und Matrix

7.1 Kategorisierungsmatrix

Die folgende Übersicht fasst den in Kapitel 6 dargestellten Befund tabellarisch zusammen:

KATEGORIE	EIGENE GOOGLE-ADS-KATEGORIE?	VORAB-ZERTIFIZIERUNG / PRÜFUNG?
Privatkredite	Ja (Personal loans)	Ja – Offenlegungspflichten
Schuldnerberatung	Ja (Debt services)	Ja – Zertifizierung erforderlich
Kreditreparatur	Ja (Credit repair services)	Anzeigen generell untersagt
Kryptowährungen	Ja (Cryptocurrencies)	Ja – Zertifizierung, regionsabhängig
Komplexe Spekulationsprodukte (CFD/Forex)	Ja	Ja – nur lizenzierte Anbieter
Vermögensermittlung / Recovery-Dienstleistungen	Nein – keine eigene Kategorie	Nein – nur allgemeine, reaktive Missbrauchsaufsicht

Kategorisierungsmatrix. Die Tabelle beruht auf dem öffentlich zugänglichen Wortlaut der Google-Ads-Richtlinien zu Finanzprodukten und -dienstleistungen (Stand der Recherche: Juli 2026) und stellt keine Aussage über nicht-öffentliche interne Klassifizierungsprozesse dar, die über den veröffentlichten Richtlinienkontext hinausgehen könnten.

7.2 Qualitative Beobachtung aus der forensischen Fallarbeit

In der von finanz-forensik.de begleiteten Fallarbeit berichten Betroffene wiederholt, dass sie den Kontakt zu einem sich später als betrügerisch herausstellenden „Vermögensermittler“ über eine gesponserte Google-Anzeige hergestellt hatten, nachdem sie aktiv nach Hilfe im Zusammenhang mit einem vorherigen Anlagebetrug gesucht hatten. Diese Beobachtung beruht auf einer begrenzten Zahl individueller Fallschilderungen und erhebt ausdrücklich keinen Anspruch auf Repräsentativität; sie deckt sich jedoch der Tendenz nach mit den in Kapitel 5.1 dargestellten, extern erhobenen Befunden von BEUC und vzbv.

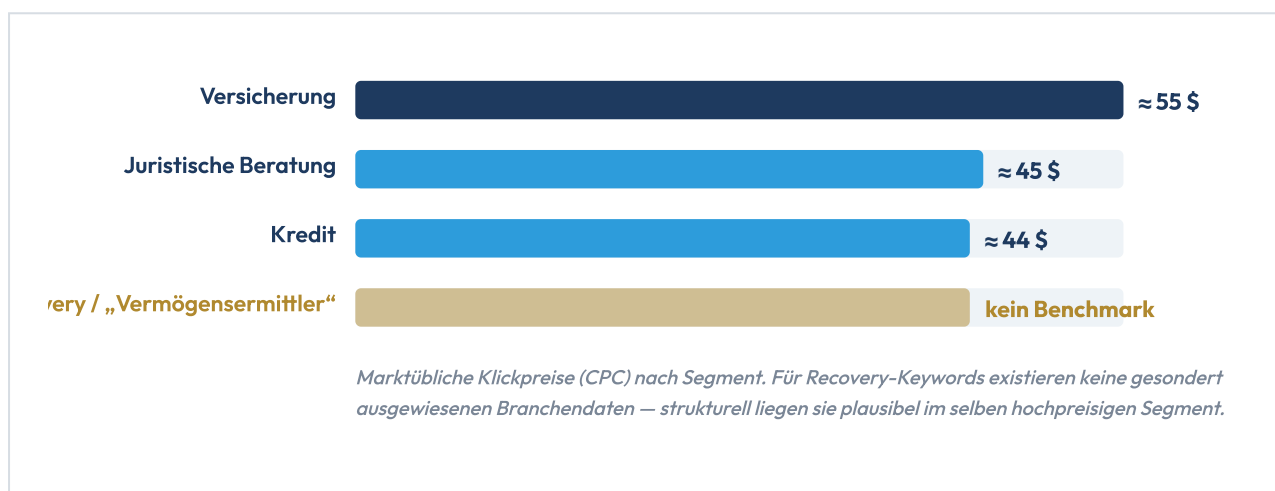
7.3 Warum klassische, rein reaktive Aufsicht strukturell zu spät kommt

Ein rein reaktives Melde-Modell – melden, prüfen, im Erfolgsfall entfernen – trifft bei anzeigenbasierten Recovery-Scams auf ein strukturelles Zeitproblem: Eine gemeldete Anzeige kann, wie Kapitel 5.1 zeigt, über Wochen aktiv bleiben, bevor über ihre Entfernung entschieden wird; in dieser Zeit generiert sie für die Plattform weiterhin Werbeeinnahmen. Da Werbekonten zudem vergleichsweise schnell neu angelegt werden können, ersetzt ein entferntes Konto im Zweifel rasch ein neues – ein Muster, das strukturell dem in der Blockchain-Forensik bekannten „Whack-a-Mole“-Effekt bei Wallet-Adressen ähnelt.

08 Die Ökonomie der Recovery-Scam-Werbung

Kapitel 3 bis 7 haben gezeigt, dass die Kategorisierungslücke rechtlich und regulatorisch besteht. Sie besteht jedoch nicht in einem wirtschaftlichen Vakuum: Anzeigenplattformen verdienen an jedem Klick – unabhängig davon, ob die beworbene Dienstleistung real oder betrügerisch ist.

Branchenbenchmarks von WordStream (2025/2026) zeigen, dass Finanz- und Rechtsdienstleistungs-Keywords zu den teuersten Segmenten im Google-Ads-Auktionssystem zählen: Versicherungs-Keywords erreichen marktübliche Klickpreise (CPC) von rund 55 US-Dollar, Kredit-Keywords rund 44 US-Dollar, juristische Beratungs-Keywords im Schnitt rund 45 US-Dollar – bei spezialisierten Long-Tail-Begriffen mit dokumentierten Ausreißern von mehreren Hundert US-Dollar pro Klick. Für „Vermögensermittler“- bzw. Recovery-Keywords existieren keine gesondert ausgewiesenen Branchen-CPC-Daten – strukturell bewegen sich diese Anzeigen jedoch in unmittelbarer thematischer Nähe zu Recht und Finanzberatung und damit plausibel im selben hochpreisigen Auktionssegment.



Finanz- und Rechts-Keywords zählen zu den teuersten CPC-Segmenten. Quelle: WordStream Google Ads Benchmarks 2025/2026; Recovery-Werte modelliert nach thematischer Nähe, kein ausgewiesener Branchen-CPC.

Dass Werbeplattformen an rechtswidrigen Finanzanzeigen tatsächlich in erheblichem Umfang verdienen können, ist – jedenfalls für Meta – kein bloßer Verdacht, sondern durch die in Kapitel 4.1 zitierte Reuters-Recherche anhand interner Konzerndokumente belegt: rund 15 Milliarden „höheres Risiko“-Anzeigen pro Tag, ein interner Umsatz-Richtwert von 7 bis 16 Milliarden US-Dollar jährlich. Für Google selbst liegen keine vergleichbaren geleakten internen Zahlen vor; die strukturelle Logik eines klickbasierten Auktionsmodells – Einnahmen entstehen unabhängig von der Rechtmäßigkeit der erworbenen Leistung – gilt jedoch systemunabhängig für jede Plattform, die Anzeigen im Cost-per-Click-Modell versteigert.

Auf der Schadensseite steht dem der bereits in Kapitel 4.1 zitierte IC3-Befund gegenüber: rund 1,4 Milliarden US-Dollar Schaden allein durch gemeldete Recovery-Scams in den USA im Jahr 2025 – eine Zahl, die ausschließlich die USA und ausschließlich gemeldete Fälle abbildet und daher eher eine untere Grenze der tatsächlichen globalen Schadenssumme markieren dürfte. Die Schlussfolgerung dieses Kapitels: Die Kategorisierungslücke aus Kapitel 6 und 7 besteht nicht trotz, sondern auch wegen eines wirtschaftlichen Anreizes, sie nicht zu schließen. Das Problem ist damit nicht nur juristisch – es ist ökonomisch.

09 Haftungsszenarien im Überblick

Aus den in Kapitel 3 dargestellten Rechtsgrundlagen lässt sich ein Spektrum möglicher Haftungssituationen ableiten. Die folgende Matrix konkretisiert dieses Spektrum anhand der beiden für die forensische und juristische Praxis entscheidenden Variablen – nachweisbare Kenntnis der Plattform und Häufigkeit/Struktur der Meldungen:

KENNTNIS DER PLATTFORM	ANZEIGE WEITERHIN AKTIV?	MELDUNG(EN) ERHALTEN?	RECHTLICHE EINORDNUNG
Keine Kenntnis	Ja	Nein	Haftungsprivileg nach DSA Art. 6 bleibt bestehen
Kenntnis (Einzelfall)	Ja	Ja (einmalig)	Mögliche Störerhaftung bei Untätigkeit; DSA-Art.-16-Pflicht ausgelöst
Kenntnis (wiederholt)	Ja	Mehrfach, strukturell vergleichbar	Erhöhtes DSA-Risiko; Berufung auf Unkenntnis zunehmend unhaltbar
Kenntnis der Kampagnenstruktur	Ja, organisiert/skaliert	Viele, über mehrere Konten	Mögliches systemisches Risiko nach DSA Art. 34/35; Bußgeldrisiko bis 6 % Jahresumsatz

Haftungsmatrix. Welches dieser Szenarien im Einzelfall vorliegt, ist stets eine Frage der konkreten Tatsachenfeststellung – insbesondere zur nachweisbaren Kenntnis der Plattform und zum Zeitpunkt sowie Inhalt etwaiger Meldungen. Dieses Whitepaper ersetzt keine rechtliche Einzelfallprüfung.

10 Wie müsste eine Werbeplattform Recovery-Anbieter technisch prüfen?

Kapitel 5.3 hat gezeigt, dass Google die technische und organisatorische Fähigkeit zur Vorab-Verifizierung von Finanzwerbetreibenden bereits mehrfach unter Beweis gestellt hat. Die folgenden Prüfschritte übertragen dieses bereits bestehende Verifizierungs-Instrumentarium (Kapitel 6.1) konkret auf die Kategorie Recovery-/Vermögensermittlungs-Dienstleistungen und sind als Reformvorschlag, nicht als Beschreibung eines bestehenden Verfahrens zu verstehen:

- Handelsregistrauszug bzw. gleichwertiger Nachweis der Unternehmensexistenz und des wirtschaftlich Berechtigten.
- Nachweis einer einschlägigen behördlichen Zulassung, soweit im Zielmarkt erforderlich (z. B. Erlaubnis als Detektiv/Wirtschaftsdetektei nach § 34a GewO in Deutschland, vergleichbare Lizenzen in anderen Jurisdiktionen) oder Nachweis der Zulassung als Rechtsanwaltskanzlei, sofern rechtliche Schritte beworben werden.
- Nachweis einer AML-Registrierung, soweit die Dienstleistung Zahlungsflüsse oder Vermögenswerte Dritter berührt.
- Verifizierung einer realen Geschäftsadresse, analog der bereits für Finanzwerbung geltenden Offenlegungspflicht aus Kapitel 6.1.
- Identitätsprüfung der verantwortlichen natürlichen Personen (Liveness-Detection/KYC), wie sie Google bei der Krypto-Werbeverifizierung bereits einsetzt.
- Referenzprüfung anhand nachprüfbarer, nicht durch den Werbetreibenden selbst kuratierter Fallreferenzen.
- Nachweis einer tatsächlichen Kooperation mit einer zugelassenen Anwaltskanzlei oder Strafverfolgungsbehörde, sofern eine solche Kooperation in der Werbung behauptet wird.

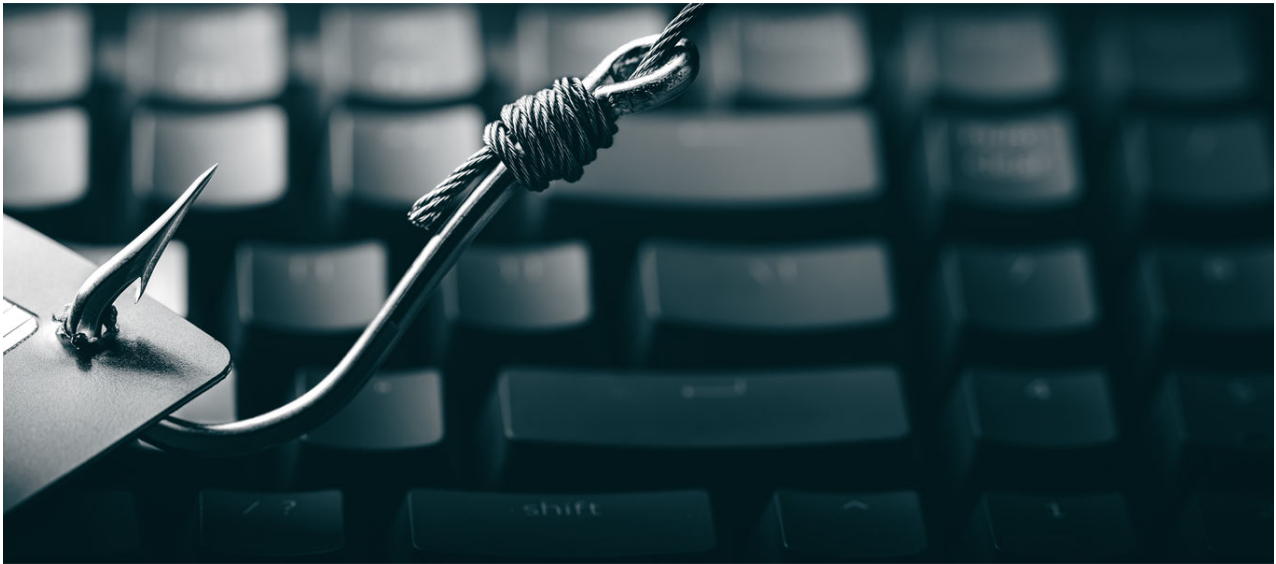
Keiner dieser Prüfschritte erfordert neue technische Fähigkeiten: Handelsregisterabfragen, Lizenzprüfungen und Identitätsverifizierung sind exakt die Bausteine, die Google im Rahmen der Kryptowährungs- und Schuldnerberatungs-Verifizierung (Kapitel 5.3, 6.1) bereits produktiv einsetzt. Die Kernthese dieses Kapitels lautet daher: Google könnte das Problem der Kategorisierungslücke technisch lösen – die offene Frage ist nicht Machbarkeit, sondern regulatorischer und kommerzieller Wille.

11 Forensische Beobachtungen: Muster hinter den Kulissen

Über die in Kapitel 2 beschriebene Anzeigen-Ebene hinaus lassen sich in der forensischen Nachverfolgung von Recovery-Scam-Fällen wiederkehrende technische und organisatorische Muster beobachten, die – soweit unten mit externer Quelle gekennzeichnet – auch unabhängig von finanz-forensik.de dokumentiert sind. Ohne externe Quellenangabe handelt es sich um qualitative, nicht-repräsentative Beobachtungen aus eigener Fallarbeit:

- **Domain-Rotation:** Zielseiten hinter Anzeigen werden häufig innerhalb kurzer Zeiträume auf neue Domains umgestellt, sodass eine bereits gemeldete und gesperrte Domain durch eine strukturell identische neue Seite ersetzt wird.
- **Wiederverwendung von Rufnummern** und Kontaktkanälen über mehrere, nominell unabhängige „Vermögensermittler“-Marken hinweg.
- **Wiederkehrende Zahlungsendpunkte:** Bereits aus anderen Fällen bekannte Wallet-Adressen oder Zahlungsdienstleister-Konten tauchen bei nachfolgenden Recovery-Scam-Fällen erneut auf.
- **Wiederverwendung bzw. Weiterverkauf von Opferlisten** zwischen Tätergruppen (extern dokumentiert durch die CFTC, siehe Kapitel 2.1) – ein Muster, das sich in der forensischen Fallarbeit von finanz-forensik.de mit der Beobachtung deckt, dass mehrfach kontaktierte Opfer auffällig häufig von strukturell ähnlich auftretenden Akteuren angesprochen werden.
- **Callcenter-ähnliche Gesprächsführung** mit standardisierten Skripten, die sich über verschiedene vermeintliche „Vermögensermittler“-Marken hinweg auffällig ähneln.

Diese Beobachtungen sind – wie in Kapitel 7.1 zur Kategorisierungslücke – ein zusätzliches Argument dafür, dass eine rein anzeigenbezogene, konto-individuelle Reaktion auf einzelne Meldungen strukturell zu kurz greift: Die tatsächliche Organisationsebene liegt häufig oberhalb der einzelnen Anzeige oder des einzelnen Werbekontos.



Die Suche nach Hilfe wird zum zweiten Einfallstor. Wer nach einem Verlust nach Rückhol-Hilfe sucht, trifft in den bezahlten Anzeigenplätzen erneut auf organisierte Täterstrukturen — die Kontrolle über diesen Kanal liegt bei der Plattform.

12 Handlungsoptionen für Geschädigte

Die CFTC nennt in ihrer Verbraucherwarnung eine Reihe von Warnsignalen, die sich mit den forensischen Beobachtungen aus Kapitel 2 und 11 decken: fehlende oder nicht verifizierbare physische Geschäftsadresse, Zahlungsaufforderung vor Erbringung jeglicher Leistung, Kommunikation ausschließlich über Messenger-Dienste, sowie die Bitte um Bankdaten zur angeblichen Auszahlung „wiederbeschaffter“ Gelder.

- Screenshots der Anzeige, der Ziel-Webseite und des gesamten Kommunikationsverlaufs zeitnah sichern – Anzeigen werden häufig kurzfristig deaktiviert oder verändert.
- Meldung sowohl bei der Werbeplattform selbst (Notice-and-Action nach DSA Art. 16) als auch bei der Verbraucherzentrale oder einer vergleichbaren Trusted-Flagger-fähigen Organisation einreichen.
- Anzeige bei der örtlichen Polizei bzw. Staatsanwaltschaft erstatten – unabhängig von der plattformrechtlichen Aufarbeitung.
- Bei erheblichem Schaden und dokumentierter Kenntnisnahme der Plattform anwaltliche Prüfung möglicher zivilrechtlicher Ansprüche gegen die Plattform in Betracht ziehen.
- Zeitnahe forensische Sicherung und Nachverfolgung etwaiger Zahlungsflüsse, insbesondere bei Kryptowährungs-Zahlungen an den vermeintlichen Vermögensermittler.

13 Empfehlungen

AN WERBEPLATTFORMEN

- Ausweitung der bestehenden Verifizierungspflicht für Finanzwerbung (Kapitel 6.1) um eine eigene Kategorie „Recovery- und Vermögensermittlungs-Dienstleistungen“ mit den in Kapitel 10 vorgeschlagenen Prüfschritten.
- Verkürzung der Bearbeitungsfristen für Trusted-Flagger-Meldungen nach DSA Art. 22 auf einen verbindlichen, veröffentlichten Zeitrahmen.
- Verpflichtende Cross-Referenzierung neu angelegter Werbekonten gegen zuvor gesperrte Konten mit strukturell vergleichbaren Anzeigeninhalten, Zielseiten-Mustern oder Zahlungsendpunkten (vgl. Kapitel 11).

AN REGULIERUNGSBEHÖRDEN

- Klarstellung durch die EU-Kommission bzw. die zuständigen Digital Services Coordinators, dass Recovery-Scam-Anzeigen unter die systemische Risikobewertungspflicht aus DSA Art. 34/35 fallen.
- Prüfung, ob der in Großbritannien entstehende Ofcom-„Fraudulent Advertising Code of Practice“ (Kapitel 4.2) als Vorlage für eine vergleichbare, EU-weit koordinierte Verwaltungspraxis dienen kann.
- Regelmäßige, öffentlich zugängliche Auswertung der DSA-Anzeigendatenbank (Art. 39) speziell im Hinblick auf Finanzbetrugs- und Recovery-Scam-Muster.

AN VERBRAUCHERSCHUTZ & MEDIEN

- Fortsetzung und Ausweitung systematischer Meldeaktionen nach dem Vorbild von „Sponsored by Scammers“, um eine belastbare Datengrundlage für aufsichtsrechtliches Handeln zu schaffen.

14 Fazit

Der rechtliche Rahmen für die Haftung digitaler Werbeplattformen hat sich mit dem Digital Services Act – und, wie Kapitel 4 zeigt, parallel auch in den USA, im Vereinigten Königreich und in Australien – spürbar in Richtung Systemverantwortung verschoben. Die in Kapitel 5 dargestellte Beschwerdelage zeigt jedoch, dass zwischen dieser regulatorischen Verschiebung und ihrer tatsächlichen Durchsetzung in der Praxis eine erhebliche Lücke klafft – eine Lücke, die bei anzeigenbasierten Recovery-Scams durch die in Kapitel 6 und 7 anhand des Richtlinienwortlauts nachgewiesene Kategorisierungslücke zusätzlich verschärft und, wie Kapitel 8 zeigt, durch ein reales wirtschaftliches Anreizproblem verstärkt wird. ■

„Eine Werbeplattform, die genau weiß, wie sie einen Kreditvermittler verifiziert, kann nicht plausibel behaupten, sie wisse nicht, wie sie einen ‚Vermögensermittler‘ verifizieren würde. Die Frage ist nicht technische Machbarkeit – die Frage ist regulatorischer und kommerzieller Wille.“

Recovery-Scam — Nachfassbetrug, bei dem bereits geschädigte Opfer unter dem Vorwand der Vermögensrückholung erneut zu Vorabzahlungen bewegt werden.

Advance-Fee-Fraud — Vorschussbetrug: Zahlung eines kleineren Betrags im Voraus im Austausch für das Versprechen einer deutlich größeren, tatsächlich nie erfolgenden Rückzahlung.

VLOP / VLOSE — Very Large Online Platform / Very Large Online Search Engine – DSA-Bezeichnung für Dienste mit mehr als 45 Mio. monatlichen Nutzern in der EU, die verschärften Pflichten unterliegen.

Notice-and-Action — Melde- und Abhilfeverfahren nach Art. 16 DSA, über das rechtswidrige Inhalte gemeldet und von Plattformen geprüft werden müssen.

Trusted Flagger — Nach Art. 22 DSA anerkannte Stelle (z. B. Verbraucherschutzorganisation), deren Meldungen vorrangig bearbeitet werden müssen.

Systemische Risikobewertung — Pflicht aus Art. 34/35 DSA für VLOPs/VLOSEs, strukturelle Risiken ihres Dienstes proaktiv zu identifizieren und zu mindern.

„Aktive Rolle“-Doktrin — EuGH-Rechtsprechung, wonach das Haftungsprivileg entfällt, sobald ein Anbieter durch aktive Kuratierung Kenntnis von oder Kontrolle über fremde Inhalte erlangt.

Störerhaftung — Deutsches Rechtsinstitut zur Haftung eines Nicht-Täters, der willentlich und adäquat kausal zu einer Rechtsverletzung Dritter beigetragen hat; im TMG/DDG-Kontext seit 2024 stark zurückgebaut.

Section 230 — US-amerikanische Haftungsimmunität für Plattformen bei nutzergenerierten Inhalten (Communications Decency Act); durch neuere Rechtsprechung bei vertraglichen Ansprüchen eingeschränkt.

Kategorisierungslücke — In diesem Whitepaper anhand des Google-Ads-Richtlinienwortlauts nachgewiesene Beobachtung, dass „Vermögensermittler“-Anzeigen keiner eigenen, zertifizierungspflichtigen Kategorie unterliegen.

CPC (Cost per Click) — Preis, den ein Werbetreibender einer Auktionsplattform pro Anzeigenklick zahlt; zentrale Erlösgröße im Google-Ads-Geschäftsmodell.

Victim Recycling — Wiederverwendung oder Weiterverkauf von Kontaktdaten bereits Geschädigter zwischen Tätergruppen zur gezielten Wiederansprache.

STUDIEN, BEHÖRDEN & BERICHTERSTATTUNG

BEUC / vzbv u. a.: „Sponsored by Scammers“ – Bericht und Beschwerden gegen Google, Meta und TikTok, Mai 2026 (beuc.eu, vzbv.de) · Europäische Kommission: Auskunftersuchen (Request for Information) nach Art. 67 DSA an Google u. a. zu Finanzbetrugs-Werbung, September 2025 · Federal Bureau of Investigation, Internet Crime Complaint Center (IC3): 2025 Internet Crime Report, insbesondere Kennzahlen zu Recovery-Scams und Recovery Asset Team (ic3.gov) · Commodity Futures Trading Commission (CFTC): „Don't be Re-Victimized by Recovery Frauds“, Verbraucherwarnung (cftc.gov) · Reuters: Investigativ-Recherche zu internen Meta-Dokumenten über Umsätze aus Betrugs- und Regolverstoß-Anzeigen, November 2025 / Januar 2026 (Sekundärberichterstattung u. a. Marketing Brew, Marketing Dive, SiliconANGLE, 80,000 Hours) · Australian Competition and Consumer Commission (ACCC): laufendes Verfahren ACCC v. Meta Platforms, Feststellungen zu Krypto-Werbeanzeigen · Ofcom: Consultation on the Fraudulent Advertising Code of Practice, 10. Juli 2026 (ofcom.org.uk); Online Safety Act 2023 (legislation.gov.uk) · UK Financial Conduct Authority (FCA): Maßnahmen gegen irreführende Finanzwerbung und „Finfluencer“, 2023 · WordStream: Google Ads Benchmarks 2025/2026 – branchenübliche CPC-Richtwerte nach Sektor.

RECHTSPRECHUNG & RECHTSGRUNDLAGEN

Consumer Federation of America v. Meta Platforms; Ninth Circuit Court of Appeals, Entscheidung zur Section-230-Reichweite bei vertraglichen Ansprüchen · Santa Clara County v. Meta Platforms, Kalifornien, laufendes Verfahren · BGH, Urteil vom 14.05.2013, Az. VI ZR 269/12 („Autocomplete“-Entscheidung) · OLG Frankfurt am Main, Beschluss vom 27.02.2020, Az. 6 U 240/19 (AdWords-Störerhaftung) · EuGH, Rechtsprechungslinie Google France/Louis Vuitton (verb. Rs. C-236/08 bis C-238/08) sowie L'Oréal/eBay (Rs. C-324/09) zur „aktiven Rolle“ von Vermittlern · Verordnung (EU) 2022/2065 (Digital Services Act), insbesondere Art. 6, 16, 22, 34, 35, 39 · Richtlinie 2000/31/EG (E-Commerce-Richtlinie), Art. 14 · Telemediengesetz (TMG) a. F. sowie Digitale-Dienste-Gesetz (DDG), Deutschland · Google: Advertising Policies Help – „Financial products and services“ und „Unacceptable business practices“ (support.google.com/adspolicy), Stand der Recherche Juli 2026; Richtlinienankündigungen zur Verifizierungspflicht für Finanzwerbung (UK 2021, Durchsetzung ab Januar 2023; Deutschland Juni 2025; EU/EWR-weite Ausweitung 23. Juli 2026).

KRIMINOLOGISCHE GRUNDLAGEN & EIGENE FALLARBEIT

Titus, Richard M., und Angela R. Gover: „Personal Fraud: The Victims and the Scams“, Crime Prevention Studies 12 (2001), S. 133–152 (zit. nach CFTC-Verbraucherwarnung) · AARP Fraud Watch Network: „Investment Fraud Vulnerability Study“, AARP Research, 2017 (zit. nach CFTC-Verbraucherwarnung) · finanz-forensik.de: Qualitative, anonymisierte Beobachtungen aus der forensischen Fallarbeit zu anzeigenbasierten Recovery-Scams, 2026 (siehe methodischen Hinweis).

Hinweis: Dieses Whitepaper kombiniert öffentlich zugängliche Rechtsprechung und Studienergebnisse Dritter mit qualitativen, anonymisierten Beobachtungen aus eigener forensischer Fallarbeit (Stand Juli 2026) und dient der allgemeinen Einordnung. Es stellt keine Rechtsberatung im Einzelfall dar und ersetzt keine anwaltliche Prüfung des konkreten Sachverhalts. Die in Kapitel 2.2 dargestellten Fallmuster sind illustrative, anonymisierte Komposit-Szenarien ohne Bezug zu realen Einzelfallbeträgen. Alle schematischen Abbildungen sind illustrativ. Die in Kapitel 6 und 7 dargestellte Analyse der Google-Ads-Richtlinien beruht auf dem öffentlich zugänglichen Richtlinienwortlaut zum Zeitpunkt der Recherche und kann sich durch spätere Richtlinienänderungen überholen.

ÜBER FINANZ-FORENSIK.DE



David Lüdtké

Geschäftsführer · OSINT-Analyst & Krypto-Forensiker · Finanz Forensik GmbH

finanz-forensik.de unterstützt Geschädigte, Kanzleien und Behörden bei der forensischen Nachverfolgung betrügerisch erlangter Vermögenswerte, insbesondere im Bereich Kryptowährungen und digitaler Zahlungsverkehr. Die in diesem Whitepaper zusammengefassten Beobachtungen zur Rolle anzeigenbasierter Kontaktaufnahme bei Recovery-Scams (Kapitel 7.2 und 11) basieren auf Mustern, die sich in unserer laufenden Fallarbeit wiederholt beobachten lassen. **Kontakt:** postfach@finanz-forensik.de · +49 6057 9189145 · www.finanz-forensik.de

Herausgeber: Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtké, David Lüdtké. Dieses Whitepaper dient der allgemeinen Information und gibt den Rechts- und Diskussionsstand Juli 2026 wieder; es stellt keine Rechts-, Steuer- oder Anlageberatung dar und begründet kein Mandatsverhältnis. © 2026 Finanz Forensik GmbH — alle Rechte vorbehalten.