

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. 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 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 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 bewusst getrennt gehaltene Ebenen: den europäischen und deutschen Rechtsrahmen (E-Commerce-Richtlinie, DSA, Störerhaftungs-Rechtsprechung), einen internationalen Vergleich (USA, Vereinigtes Königreich, Australien), eine ökonomische Analyse des anzeigenfinanzierten Geschäftsmodells und qualitative Beobachtungen aus der forensischen Fallarbeit von finanz-forensik.de.

METHODISCHER HINWEIS

Dieses Whitepaper unterscheidet strikt zwischen extern erhobenen, mit Quellenangabe zitierten Rechtsprechungs- und Studienergebnissen (insbesondere Kapitel 3–6) 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 US-Aufsichtsbehörde 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: 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 Betrugsopfer mehrfach viktimisiert wird.

2.2 Illustrative Fallmuster

Die folgenden drei Szenarien sind anonymisierte, illustrative Komposit-Darstellungen wiederkehrender Muster — keine Wiedergabe realer Einzelfälle mit realen Beträgen.

MUSTER A · DIREKTER ANZEIGENKLICK

Ausgangspunkt ist ein vorangegangener Krypto-Anlagebetrug. Das Opfer sucht gezielt nach Rückhol-Möglichkeiten, klickt auf eine gesponserte „Vermögensermittler“-Anzeige mit professioneller Website. Nach einem Erstgespräch wird eine Vorabgebühr für „Ermittlungs- und Rechtskosten“ verlangt; die Rückholung bleibt aus, der Kontakt bricht ab.

MUSTER B · „FAKED-NEWS“-VARIANTE

Vor dem Anzeigenkontakt stößt das Opfer auf einen scheinbar redaktionellen Artikel über einen „erfolgreichen Vermögensermittler“ — ein von der CFTC beschriebenes Muster, bei dem Täter Presseartikel über Presseverteiler platzieren. Der Artikel erhöht die Glaubwürdigkeit der anschließend geklickten Anzeige. Weiterer Ablauf wie Muster A.

MUSTER C · RECYCELTE KONTAKTDATEN

Das Opfer hatte bei einem ersten — nicht notwendig anzeigenbasierten — Betrugsversuch Kontaktdaten hinterlassen. Wochen oder Monate später wird es erneut kontaktiert, diesmal unter dem Vorwand eines „Ermittlungserfolgs“. Die CFTC beschreibt dies 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.

3.1 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: 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 Privileg um; es wurde 2024 durch das Digitale-Dienste-Gesetz (DDG) abgelöst, das den DSA in nationales Recht einbettet. Eine rechtswidrige Anzeige begründet damit im Ausgangspunkt nicht automatisch eine Haftung der Plattform — diese Privilegierung ist jedoch an Bedingungen geknüpft, die im Fall organisierter Recovery-Scams zunehmend infrage stehen.

3.2 Deutsche Rechtsprechung: von der Störerhaftung zur Kenntnis-Schwelle

Der Bundesgerichtshof hat die Grundlinie im 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. Spezifisch zu AdWords hat das OLG Frankfurt am Main entschieden (Beschluss vom 27.02.2020, Az. 6 U 240/19), dass die markenrechtliche Störerhaftung in erster Linie den werbenden Kunden trifft, nicht den Suchmaschinenbetreiber — solange dieser keine aktive Rolle einnimmt. Beide Entscheidungen etablieren ein Kenntnis-Modell. 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 den Rahmen zweifach. Erstens konkretisiert er das reaktive Melde-Modell: Art. 16 DSA verpflichtet zu einem funktionierenden „Notice-and-Action“-Verfahren, Art. 22 DSA führt einen privilegierten Meldeweg für Trusted Flagger ein. Zweitens verpflichten Art. 34 und 35 DSA sehr große Online-Plattformen und Suchmaschinen (VLOP/VLOSE, über 45 Millionen monatliche EU-Nutzer) zu einer systemischen Risikobewertung und -minderung; Google Search und Google Ads erfüllen diese Schwellenwerte. Art. 39 DSA verpflichtet zu umfassender Werbetransparenz in einer öffentlichen Anzeigendatenbank — für die forensische Nachverfolgung von Recovery-Scam-Kampagnen von unmittelbarer Bedeutung. Bei Verstößen gegen Art. 34/35 DSA drohen Bußgelder von bis zu 6 % des weltweiten Jahresumsatzes.

3.4 Die „aktive Rolle“-Doktrin des EuGH

Der EuGH hat in seiner Rechtsprechung zu Online-Marktplätzen und Suchmaschinenwerbung (Google-France/Louis-Vuitton sowie L'Oréal/eBay) 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 Daten verschafft. Für Google Ads ist dies keine akademische Frage: Anzeigen-Ranking, algorithmisches Targeting und qualitätsbasierte Gebotsmechanismen sind gerade keine neutrale, rein technische Weiterleitung, sondern eine aktive redaktionelle und kommerzielle Gestaltungsleistung.

04 Internationaler Vergleich

Die europäische Entwicklung steht nicht isoliert. In den USA, im Vereinigten Königreich und in Australien lässt sich unabhängig voneinander ein vergleichbarer Trend beobachten: eine wachsende 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-Meldestelle IC3 registrierte 2025 mehr als 10.500 Beschwerden speziell zu Recovery-Scams mit einem geschätzten Gesamtschaden von rund 1,4 Milliarden US-Dollar. Das FBI-„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 bereits eingetreten ist, bevor überhaupt eingegriffen werden kann. Rechtlich bemerkenswert ist die Section-230-Entwicklung: Der Ninth Circuit Court of Appeals entschied, dass Section 230 Meta nicht vor Ansprüchen schützt, die sich auf gebrochene vertragliche Zusagen in den eigenen Nutzungsbedingungen stützen — ein Präzedenzfall, der die klassische Plattformimmunität spürbar einschränkt. Parallel verklagte Santa Clara County Meta mit der Begründung, der Konzern profitiere systematisch von betrügerischen Anzeigen.

Wie groß der wirtschaftliche Anreiz sein kann, legte eine Reuters-Recherche 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 rund 7 Milliarden US-Dollar Umsatz aus solchen Anzeigen, mit einer Projektion von bis zu 16 Milliarden US-Dollar. Diese Zahlen betreffen ausdrücklich Meta, nicht Google; sie belegen, dass das strukturelle ökonomische Anreizproblem anzeigenfinanzierter Plattformen real und dokumentiert ist.

4.2 Vereinigtes Königreich: vom Kulanz-Modell zur bindenden Aufsichtspflicht

Der britische Online Safety Act 2023 führt erstmals eine gesetzliche Pflicht zum Schutz vor betrügerischer Werbung ein und beauftragt Ofcom mit deren Durchsetzung. Am 10. Juli 2026 eröffnete Ofcom eine Konsultation zu knapp 40 Maßnahmen eines „Fraudulent Advertising Code of Practice“ mit erstmals verbindlichen Pflichten bei bezahlter Werbung. Verstöße können mit bis zu 18 Millionen Pfund oder 10 % des weltweiten Konzernumsatzes geahndet werden. Nach Ofcom-Schätzungen verlieren britische Verbraucher jährlich rund 200 Millionen Pfund allein durch betrügerische Werbeanzeigen. Die FCA erwirkte bereits 2023 die Rücknahme oder Änderung von mehr als 10.000 irreführenden Finanzwerbe-Anzeigen — genau dieser Druck bewog Google 2021 zur Einführung seiner ersten Finanzwerbe-Verifizierung im Vereinigten Königreich.

4.3 Australien: ACCC gegen Meta als Vergleichsfall

Die ACCC führt ein Verfahren gegen Meta, in dessen Rahmen eigene Untersuchungen ergaben, dass rund 58 % der überprüften, gemeldeten Krypto-Werbeanzeigen gegen Plattformrichtlinien verstießen oder betrügerischer Natur waren. Dieser Befund stützt die These, dass das Muster keine Besonderheit einer einzelnen Plattform ist, sondern ein strukturelles Problem des anzeigenbasierten Geschäftsmodells.

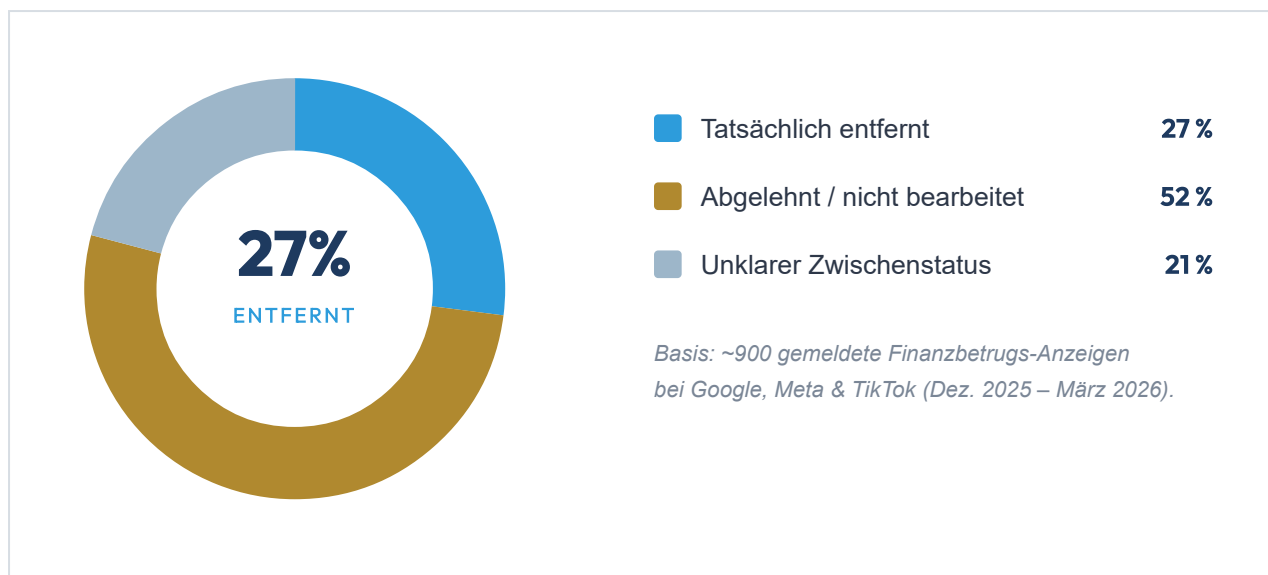
„Weg von einer rein reaktiven Kenntnis-Schwelle, hin zu einer proaktiven Systemverantwortung — EU, UK, USA und Australien bewegen sich unabhängig voneinander in dieselbe Richtung.“

ZWISCHENFAZIT KAPITEL 4

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 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 ausgewertet.



Plattformreaktion auf gemeldete Betrugsanzeigen. Nur gut ein Viertel der gemeldeten Anzeigen wurde tatsächlich entfernt. Quelle: BEUC/vzbv, „Sponsored by Scammers“, Mai 2026. Die Verbraucherorganisationen reichten auf dieser Grundlage formelle DSA-Beschwerden gegen alle drei Plattformen ein.

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 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 Pflicht in Deutschland auf 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 Argumentation, eine lückenlose Vorab-Prüfung sei technisch unmöglich.

06 Die Google-Ads-Richtlinien im Detail

6.1 Was Google bereits reguliert

Die offizielle Richtlinie „Financial products and services“ definiert Finanzprodukte als Produkte und Dienstleistungen im Zusammenhang mit der Verwaltung oder Anlage von Geld und Kryptowährungen und listet u. a. auf: Privatkredite (mit Pflichtangaben zu Zins und Gesamtkosten), Umschuldung/Loan Modification (Verbot von Erfolgsgarantien und Vorabgebühren), Kreditreparatur (generell untersagt), Schuldnerdienstleistungen (nur nach Zertifizierung), Binäre Optionen (untersagt), komplexe Spekulationsprodukte wie CFDs/Forex (nur lizenzierte Anbieter nach Zertifizierung), Kryptowährungen (mit/ohne Zertifizierung je Region) sowie Prediction Markets. Für alle zertifizierungspflichtigen Kategorien gilt eine Offenlegungspflicht für physische Geschäftsadresse, sämtliche Gebühren und behauptete Dritt-Akkreditierungen.

6.2 Was Google verbietet, aber nur reaktiv durchsetzt

Die Richtlinie „Unacceptable business practices“ untersagt allgemein, Nutzer durch Verschleierung oder Falschdarstellung zu täuschen — etwa durch Vortäuschen einer Zugehörigkeit oder das Anbieten nicht erbringbarer Leistungen. Ein Recovery-Scam verstößt damit bereits gegen diese Richtlinie. Der entscheidende Unterschied liegt jedoch im Durchsetzungsmechanismus: Verstöße gegen die zertifizierungspflichtigen Kategorien aus 6.1 werden vor der ersten Anzeigenschaltung geprüft; Verstöße gegen „Unacceptable business practices“ dagegen laut Richtlinien text erst „bei Entdeckung“ — also reaktiv, nach Anzeigenschaltung.

6.3 Die Lücke im Wortlaut

Bemerkenswert ist, was in der Aufzählung aus 6.1 nicht vorkommt: Weder „Vermögensermittlung“ noch „Asset Recovery“ erscheint als eigene, benannte Unterkategorie. Anbieter von Recovery-Dienstleistungen fallen damit — jedenfalls nach dem öffentlich einsehbaren Richtlinienwortlaut — nicht in eine zertifizierungspflichtige Kategorie, sondern lediglich unter die allgemeine, reaktive Missbrauchsaufsicht aus 6.2. Diese textliche Lücke ist der unmittelbare Beleg für die „Kategorisierungslücke“.

07 Die Kategorisierungslücke: Nachweis und Matrix

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)	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 Aufsicht

Kategorisierungsmatrix. Grundlage ist der öffentlich zugängliche Wortlaut der Google-Ads-Finanzrichtlinien (Stand Juli 2026). Die Tabelle trifft keine Aussage über nicht-öffentliche interne Klassifizierungsprozesse.

7.2 Qualitative Beobachtung aus der forensischen Fallarbeit

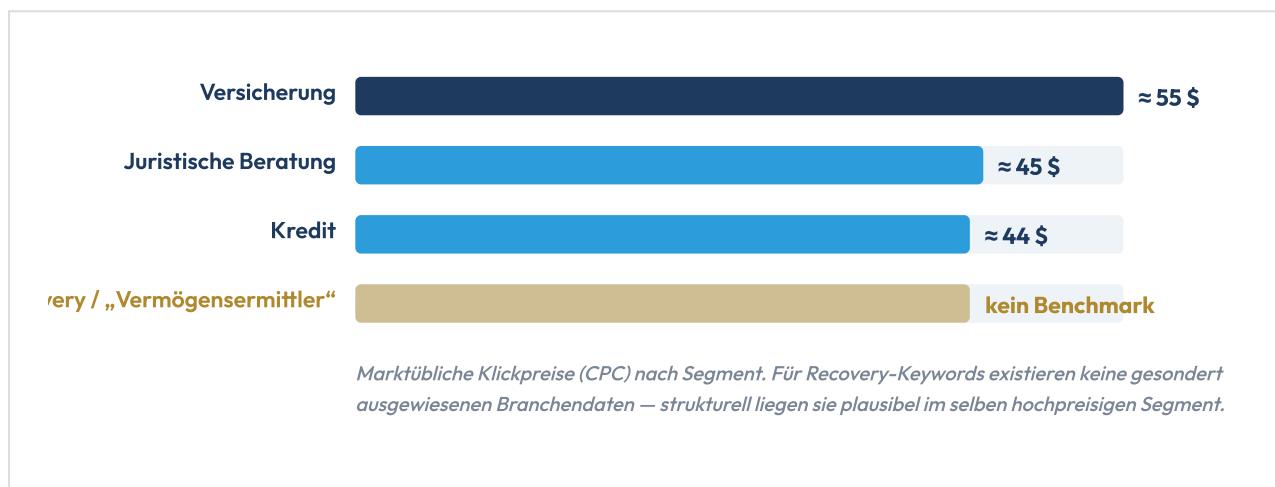
In der von finanz-forensik.de begleiteten Fallarbeit berichten Betroffene wiederholt, dass sie den Kontakt zu einem sich später als betrügerisch herausstellenden „Vermögensermittler“ über eine gesponserte Google-Anzeige hergestellt hatten, nachdem sie aktiv nach Hilfe gesucht hatten. Diese Beobachtung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

7.3 Warum rein reaktive Aufsicht strukturell zu spät kommt

Ein rein reaktives Melde-Modell trifft bei anzeigenbasierten Recovery-Scams auf ein strukturelles Zeitproblem: Eine gemeldete Anzeige kann über Wochen aktiv bleiben, bevor über ihre Entfernung entschieden wird; in dieser Zeit generiert sie weiterhin Werbeeinnahmen. Da Werbekonten zudem schnell neu angelegt werden, ersetzt ein entferntes Konto rasch ein neues — ein Muster, das dem in der Blockchain-Forensik bekannten „Whack-a-Mole“-Effekt bei Wallet-Adressen ähnelt.

08 Die Ökonomie der Recovery-Scam-Werbung

Die Kategorisierungslücke besteht 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.



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 in erheblichem Umfang verdienen können, ist — jedenfalls für Meta — durch die Reuters-Recherche belegt: rund 15 Milliarden „höheres Risiko“-Anzeigen pro Tag, ein interner Umsatz-Richtwert von 7 bis 16 Milliarden US-Dollar jährlich. Für Google liegen keine vergleichbaren geleakten Zahlen vor; die strukturelle Logik eines klickbasierten Auktionsmodells gilt jedoch systemunabhängig. Dem gegenüber steht der IC3-Befund von rund 1,4 Milliarden US-Dollar Recovery-Scam-Schaden allein in den USA 2025 — eher eine untere Grenze. Die Schlussfolgerung: Die Kategorisierungslücke besteht nicht trotz, sondern auch wegen eines wirtschaftlichen Anreizes, sie nicht zu schließen.

09 Haftungsszenarien im Überblick

Aus den Rechtsgrundlagen aus Kapitel 3 lässt sich ein Spektrum möglicher Haftungssituationen ableiten, konkretisiert anhand der beiden entscheidenden Variablen — nachweisbare Kenntnis der Plattform und Häufigkeit/Struktur der Meldungen:

KENNTNIS DER PLATTFORM	ANZEIGE 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; Bußgeld bis 6 % Jahresumsatz

Haftungsmatrix. Welches Szenario im Einzelfall vorliegt, ist stets eine Frage der konkreten Tatsachenfeststellung. Dieses Whitepaper ersetzt keine rechtliche Einzelfallprüfung.

10 Wie müsste eine Werbeplattform Recovery-Anbieter prüfen?

Google hat die technische und organisatorische Fähigkeit zur Vorab-Verifizierung bereits mehrfach unter Beweis gestellt. Die folgenden Prüfschritte übertragen dieses bestehende Instrumentarium auf die Kategorie Recovery-/Vermögensermittlungs-Dienstleistungen — als Reformvorschlag, nicht als Beschreibung eines bestehenden Verfahrens:

- Handelsregistrauszug bzw. gleichwertiger Nachweis der Unternehmensexistenz und des wirtschaftlich Berechtigten.
- Nachweis einer einschlägigen behördlichen Zulassung (z. B. Erlaubnis als Wirtschaftsdetektei nach § 34a GewO in Deutschland) 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 geltenden Offenlegungspflicht.
- Identitätsprüfung der verantwortlichen natürlichen Personen (Liveness-Detection/KYC), wie bei der Krypto-Werbeverifizierung bereits eingesetzt.
- Referenzprüfung anhand nachprüfbarer, nicht selbst kuratierter Fallreferenzen.
- Nachweis einer tatsächlichen Kooperation mit einer zugelassenen Kanzlei oder Strafverfolgungsbehörde, sofern in der Werbung behauptet.

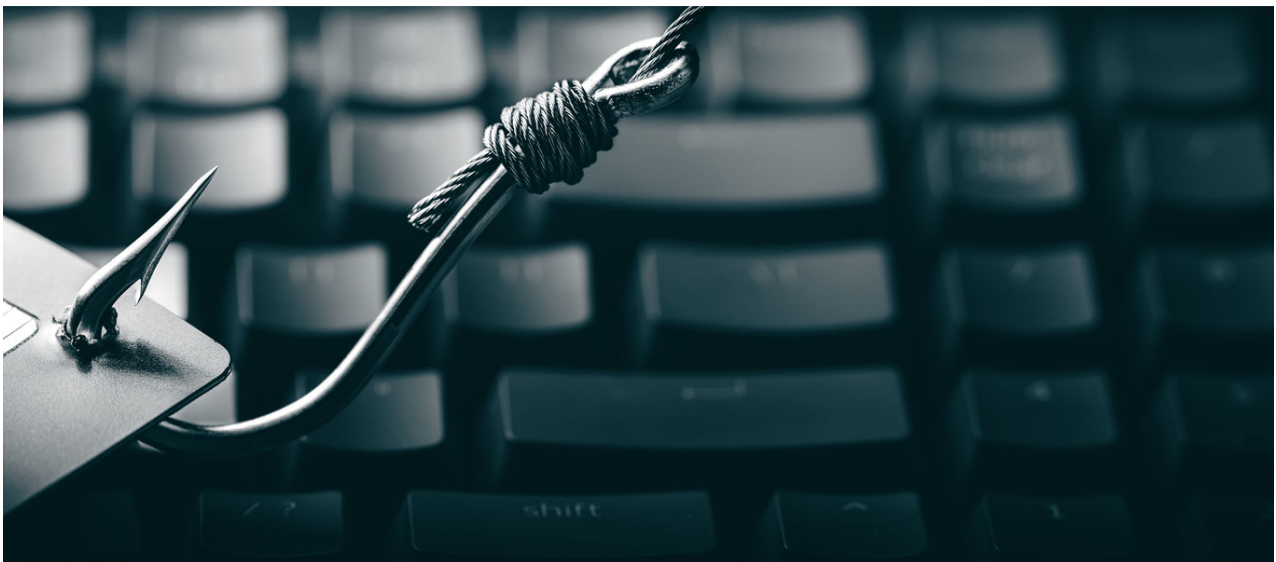
Keiner dieser Prüfschritte erfordert neue technische Fähigkeiten: Handelsregisterabfragen, Lizenzprüfungen und Identitätsverifizierung sind exakt die Bausteine, die Google bei der Krypto- und Schuldnerberatungs-Verifizierung bereits produktiv einsetzt. Die offene Frage ist nicht Machbarkeit, sondern regulatorischer und kommerzieller Wille.

11 Forensische Beobachtungen: Muster hinter den Kulissen

Über die Anzeigen-Ebene hinaus lassen sich in der forensischen Nachverfolgung wiederkehrende technische und organisatorische Muster beobachten (ohne externe Quellenangabe: qualitative, nicht-repräsentative Beobachtungen aus eigener Fallarbeit):

- **Domain-Rotation:** Zielseiten hinter Anzeigen werden innerhalb kurzer Zeiträume auf neue Domains umgestellt, sodass eine 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 erneut auf.
- **Wiederverwendung von Opferlisten** zwischen Tätergruppen (extern dokumentiert durch die CFTC) — mehrfach kontaktierte Opfer werden auffällig häufig von strukturell ähnlichen Akteuren angesprochen.
- **Callcenter-ähnliche Gesprächsführung** mit standardisierten Skripten, die sich über verschiedene „Vermögensermittler“-Marken hinweg auffällig ähneln.

Diese Beobachtungen sind ein zusätzliches Argument dafür, dass eine rein anzeigenbezogene, konto-individuelle Reaktion 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 Warnsignale, die sich mit den forensischen Beobachtungen decken: fehlende verifizierbare Geschäftsadresse, Zahlungsaufforderung vor jeglicher Leistung, Kommunikation ausschließlich über Messenger, 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 (Notice-and-Action nach DSA Art. 16) als auch bei der Verbraucherzentrale oder einer Trusted-Flagger-fähigen Organisation.
- Anzeige bei der örtlichen Polizei bzw. Staatsanwaltschaft — unabhängig von der plattformrechtlichen Aufarbeitung.
- Bei erheblichem Schaden und dokumentierter Kenntnisnahme der Plattform anwaltliche Prüfung möglicher zivilrechtlicher Ansprüche gegen die Plattform.

- Zeitnahe forensische Sicherung und Nachverfolgung etwaiger Zahlungsflüsse, insbesondere bei Krypto-Zahlungen an den vermeintlichen Vermögensermittler.

13 Empfehlungen

AN WERBEPLATTFORMEN

Eigene Verifizierungskategorie „Recovery- und Vermögensermittlungs-Dienstleistungen“ mit den Prüfschritten aus Kapitel 10. Verbindliche, veröffentlichte Bearbeitungsfristen für Trusted-Flagger-Meldungen (Art. 22 DSA). Verpflichtende Cross-Referenzierung neu angelegter gegen zuvor gesperrte Werbekonten.

AN REGULIERUNGSBEHÖRDEN

Klarstellung, dass Recovery-Scam-Anzeigen unter die systemische Risikobewertung (Art. 34/35 DSA) fallen. Prüfung des Ofcom-„Fraudulent Advertising Code“ als EU-Vorlage. Regelmäßige öffentliche Auswertung der DSA-Anzeigendatenbank (Art. 39) auf Betrugsmuster.

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 parallel in den USA, im Vereinigten Königreich und in Australien — spürbar in Richtung Systemverantwortung verschoben. Die Beschwerdelage zeigt jedoch, dass zwischen dieser regulatorischen Verschiebung und ihrer tatsächlichen Durchsetzung eine erhebliche Lücke klafft — verschärft durch die am Richtlinienwortlaut nachgewiesene Kategorisierungslücke und verstärkt durch ein reales wirtschaftliches Anreizproblem. ■

„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.“

FINANZ-FORENSIK.DE, JULI 2026

GLOSSAR

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 für das Versprechen einer nie erfolgenden größeren Rückzahlung. · **VLOP / VLOSE** — Very Large Online Platform / Search Engine; DSA-Dienste mit über 45 Mio. monatlichen EU-Nutzern und verschärften Pflichten. · **Notice-and-Action** — Melde- und Abhilfeverfahren nach Art. 16 DSA. · **Trusted Flagger** — nach Art. 22 DSA anerkannte Stelle, deren Meldungen vorrangig bearbeitet werden. · **Systemische Risikobewertung** — Pflicht aus Art. 34/35 DSA, strukturelle Risiken proaktiv zu mindern. · **„Aktive Rolle“-Doktrin** — EuGH-Rechtsprechung: Haftungsprivileg entfällt bei aktiver Kuratierung. · **Störerhaftung** — deutsches Rechtsinstitut, im TMG/DDG-Kontext seit 2024 stark zurückgebaut. · **Section 230** — US-Haftungsimmunität; durch neuere Rechtsprechung bei vertraglichen Ansprüchen eingeschränkt. · **Kategorisierungslücke** — Beobachtung, dass „Vermögensermittler“-Anzeigen keiner zertifizierungspflichtigen Kategorie unterliegen. · **CPC** — Cost per Click; zentrale Erlösgröße im Google-Ads-Geschäftsmodell. · **Victim Recycling** — Wiederverwendung von Kontaktdaten bereits Geschädigter zwischen Tätergruppen.

QUELLEN (AUSWAHL)

STUDIEN & BEHÖRDEN

BEUC / vzbv: „Sponsored by Scammers“, Mai 2026 · Europäische Kommission: Auskunftersuchen (Art. 67 DSA) an Google, Sept. 2025 · FBI IC3: 2025 Internet Crime Report (Recovery-Scams, Recovery Asset Team) · CFTC: „Don't be Re-Victimized by Recovery Frauds“ · Reuters: interne Meta-Dokumente zu Umsätzen aus Betrugs-Anzeigen, Nov. 2025 / Jan. 2026 · ACCC v. Meta Platforms · Ofcom: Fraudulent Advertising Code of Practice, 10.07.2026; Online Safety Act 2023 · UK FCA: Maßnahmen gegen irreführende Finanzwerbung, 2023 · WordStream: Google Ads Benchmarks 2025/2026.

RECHTSPRECHUNG & RECHT

BGH, Urteil v. 14.05.2013, Az. VI ZR 269/12 („Autocomplete“) · OLG Frankfurt a. M., Beschluss v. 27.02.2020, Az. 6 U 240/19 · EuGH, Google France/Louis Vuitton (verb. Rs. C-236/08–C-238/08) sowie L'Oréal/eBay (Rs. C-324/09) · Consumer Federation of America v. Meta (Ninth Circuit); Santa Clara County v. Meta · VO (EU) 2022/2065 (DSA), Art. 6, 16, 22, 34, 35, 39 · RL 2000/31/EG (E-Commerce-RL), Art. 14 · TMG a. F. / DDG · Google Advertising Policies: „Financial products and services“, „Unacceptable business practices“ (Stand Juli 2026).

Kombiniert öffentlich zugängliche Rechtsprechung und Studienergebnisse Dritter mit qualitativen, anonymisierten Beobachtungen aus eigener forensischer Fallarbeit (Stand Juli 2026). Keine Rechtsberatung im Einzelfall.

ÜBER DEN AUTOR



David Lüdtke

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

Gerichtsfeste Kryptotransaktionsanalysen, OSINT-gestützte Vermögensermittlung und gutachterliche Aufbereitung für Strafverteidiger, Insolvenzverwalter und Unternehmen. Zertifiziert als Crystal Expert (CECF · CEEI · CEUI). **Kontakt:** postfach@finanz-forensik.de · +49 6057 772 994 86 · www.finanz-forensik.de

Herausgeber: Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtke, David Lüdtke. 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.