Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Positionspapier

zur TKG-Novelle: Ergänzungsvorschläge für eine wirksame Betrugsprävention

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Kontakt:
Diana Campar
Associate Director
Telefon: +49 30 1663-1546
E-Mail: diana.campar@bdb.de

Berlin, 29. August 2025

Federführer:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin
Telefon: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de

Rechtliche Grundlagen für eine wirksame Betrugsprävention schaffen

Die Deutsche Kreditwirtschaft (DK) begrüßt die vom Bundesministerium für Digitales und Staatsmodernisierung (BMDS) vorgelegten Eckpunkte zur Novellierung des Telekommunikationsgesetzes[1], die in erster Linie den dringend notwendigen Netzausbau adressieren. Gleichzeitig möchten wir auf eine weitere ebenso dringende Herausforderung aufmerksam machen, die im aktuellen Gesetzgebungsprozess mitbehandelt werden muss: den Schutz von Verbraucherinnen und Verbrauchern sowie von Unternehmen vor den immer raffinierter werdenden Betrugsformen des Social Engineerings und Manipulation im Online-Kontext.

Social Engineering ist mittlerweile die am weitesten verbreitete Form des digitalen Betrugs. Kriminelle geben sich als vertrauenswürdige Institutionen aus, manipulieren Bankkundinnen und Bankkunden und verschaffen sich so Zugang zu sensiblen Daten oder veranlassen betrügerische Transaktionen.

Bei Social Engineering werden besonders häufig Telekommunikationskanäle genutzt – sei es durch manipulierte Anruferkennungen („Call-ID-Spoofing“) oder durch täuschend echt wirkende Phishing-SMS. Diese Täuschungsversuche sind oft der Beginn komplexer Betrugsketten. In der Folge verursachen sie gravierende Schäden für die Betroffenen, das Bankensystem und letztlich die gesamte Volkswirtschaft.

Telekommunikationsunternehmen verfügen über technische Möglichkeiten, um Spoofing-Anrufe und Phishing-SMS wirksam zu erkennen und vor der Weiterleitung an Kunden zu blockieren oder mit Warnungen zu versehen. Damit diese wirksamen Maßnahmen zur Eindämmung von Social Engineering konsequent eingesetzt werden können, ist die notwendige rechtliche Grundlage zu schaffen. Denn das derzeitige Verbot des sogenannten Call-ID-Spoofings greift zu kurz, da es weiterhin möglich ist, gespoofte Anrufe über deutsche Telekommunikationsanlagen durchzustellen. Ein effektiver Schutz kann erst dann gewährleistet werden, wenn auch solche Anrufe erfasst und, mit Ausnahme berechtigter Nutzer wie seriöser Call-Center, blockiert werden dürfen. Eine bloße Anonymisierung reicht nicht aus.

Ebenso dringend erforderlich ist die Möglichkeit für Telekommunikationsunternehmen, sogenannte SMS-Content-Firewalls einzusetzen. Nur so können massenhaft versendete Phishing-SMS automatisiert gefiltert, blockiert oder mit klaren Warnhinweisen versehen werden.

Darüber hinaus muss es erlaubt sein, dass Telekommunikationsanbieter mit Banken und anderen relevanten Akteuren betrugsrelevante Daten, auch auf Basis von Verkehrsdaten, austauschen, um verdächtige Muster schneller zu erkennen und betrügerische Transaktionen

[1] https://bmds.bund.de/aktuelles/pressemitteilungen/17072025-bmds-legt-eckpunkte-mit-aenderungsvorschlaegen-fuer-tk-gesetz-vor

zu verhindern. Derartige Mechanismen sind bereits in dem Entwurf der EU-Zahlungsdiensteverordnung[2] vorgesehen. Ohne die notwendigen Anpassungen im nationalen Recht – konkret im TKG und im TDDDG – können diese Maßnahmen in Deutschland nicht umgesetzt werden.

Die Kriminalität im Bereich des Social Engineerings entwickelt sich dynamisch, ist hochprofessionell und international vernetzt. Präventionsmaßnahmen müssen mit dieser Entwicklung Schritt halten und dürfen nicht durch fehlende gesetzliche Grundlagen ausgebremst werden. Daher appelliert die Deutsche Kreditwirtschaft eindringlich an den Gesetzgeber, die aktuellen Änderungen des Telekommunikationsgesetzes und des Telekommunikationsdienste-Datenschutzgesetzes zu nutzen, um klare Befugnisse für Telekommunikationsunternehmen zur Betrugsprävention zu ergänzen. Jede Verzögerung führt dazu, dass Kriminelle weiterhin ungehindert ihre Methoden perfektionieren und noch mehr Bürgerinnen und Bürger Opfer von Betrug werden sowie betrügerisch erlangte Gelder in internationale kriminelle Strukturen sowie ggf. sogar Terrorismusfinanzierung abfließen.

Die Chance, im Zuge der aktuellen TKG-Novelle jetzt die erforderlichen rechtlichen Grundlagen zu schaffen, darf nicht ungenutzt bleiben. Nur durch ein entschlossenes Handeln können wir die Kommunikationswege sicherer machen, das Vertrauen der Verbraucherinnen und Verbraucher stärken und die Integrität unseres Finanzsystems nachhaltig schützen.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0367