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

# Position paper

## on the TKG amendments: proposed additions for effective fraud prevention

*Lobby Register No R001459*
*EU Transparency Register No 52646912360-95*

Contact:
Diana Campar
Associate Director
Telephone: +49 30 1663- 1546
E-mail: diana.campar@bdb.de

Berlin, 29 August 2025

Coordinator:
Bundesverband deutscher Banken e.V.
(Association of German Banks)
Burgstraße 28 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de

# Creating the legal basis for effective fraud prevention

The German Banking Industry Committee (GBIC) welcomes the proposals on the amendment of the German Telecommunications Act (Telekommunkationsgesetz (TKG))[1] presented by the Federal Ministry for Digital Transformation and Government Modernisation (BMDS), which primarily address the urgent need to expand fibre optical and cellular networks. However, we would like to draw attention to another challenge that is just as urgent and that must also be addressed during the current legislative process: protection of consumers and businesses from social engineering and manipulation online. These are forms of fraud that are becoming more and more sophisticated as time goes on.

Social engineering is now one of the most widespread types of digital fraud. Criminals impersonate trustworthy institutions, manipulating bank clients in order to gain access to sensitive data or make fraudulent transactions.

Telecommunication channels are often the medium of choice for social engineering. Common methods include caller ID spoofing or highly realistic phishing text messages. These attempts to deceive are often just the beginning of a highly complex chain of fraudulent activity that results in serious harm to victims, the banking system and ultimately the entire economy.

Telecommunications firms have the technical expertise to effectively identify spoofed calls or phishing texts and block them or add a warning to them before they are forwarded to clients. Now is the time to create the proper legal basis for ensuring that these effective countermeasures against social engineering attacks are implemented consistently. It’s become very clear that the current ban on caller ID spoofing is inadequate, as spoofed calls continue to reach users of the German telecommunications networks. Effective protection can only be guaranteed if these calls are caught and can be blocked (with the exception of those from legitimate users, such as reputable call centres). Simple anonymisation is clearly inadequate.

It is also extremely urgent that telecommunications businesses be granted the right to implement SMS content firewalls. This is the only way to ensure that phishing SMSs, which are usually sent en masse, can be filtered, blocked or furnished with clear warnings.

In addition, telecommunications providers must be able to exchange data (including call details) pertaining to fraud with banks and other relevant institutions, allowing them to identify suspicious patterns faster, thus preventing fraudulent transactions. These types of mechanisms are currently already included in the draft EU payment services regulation[2]. If no changes are made to national law – specifically the TKG and the TDDDG (Data Protection for

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

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

Telecommunications and Digital Services Act) – it will be impossible to implement these measures in Germany.

Criminal social engineering is dynamic, and the perpetrators are part of a highly professional, international network. Preventative measures must keep pace with these developments and should not be impeded by inadequate legal conditions. The German Banking Industry Committee is therefore urgently calling for legislators to take the opportunity, while amending the Telecommunications Act and the Data Protection Telecommunications Act, to add clear fraud prevention rights for telecommunications' businesses to the laws. Any delay in doing so will allow criminals to continue to perfect their methods unimpeded, so that even more people will become victims of fraud. Not only that, the money gained through this fraud can then be pumped into international, criminal structures, up to and including financing terrorism.

It is essential that we do not waste this opportunity, and act immediately and as part of the TKG amendments to create the necessary legal basis. Now is the time to take decisive action to protect our communication networks, improve consumer confidence and protect the integrity of our financial system over the long term.