



Eidg. Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundeshaus Nord
CH-3003 Bern

Eingereicht via: <https://www.gate.bag.admin.ch/consultations/ui/home>
(wie gewünscht in PDF und Word)

Zürich, 17. September 2026

Teilrevision des Fernmeldegesetzes (FMG) im Bereich Sicherheit sowie Teilrevision der Verordnungen im Fernmeldebereich – Stellungnahme von SwissDebitPay

Sehr geehrter Herr Bundesrat,
Sehr geehrte Damen und Herren

SwissDebitPay, der Branchenverband der Schweizer Herausgeber von Debit-Zahlungsmitteln, bedankt sich für die Einladung, zu den Vernehmlassungsunterlagen zur Teilrevision des Fernmeldegesetzes im Bereich Sicherheit sowie zur Teilrevision der entsprechenden Verordnungen Stellung zu nehmen. SwissDebitPay beschränkt sich bei der Stellungnahme auf die für ihre Mitglieder wesentlichen Fragestellungen im Zusammenhang mit der Verhinderung von betrügerischen Zahlungen mit Debit-Zahlungsmitteln.

1. Bekämpfung des Missbrauchs von schweizerischen Telefonnummern

SwissDebitPay begrüsst die Absicht, mit den vorliegenden Teilrevisionen des Fernmeldegesetzes (FMG), der Verordnung über Fernmeldedienste (FDV) sowie der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV) den Konsumentenschutz zu stärken und insbesondere den Missbrauch von schweizerischen Telefonnummern für betrügerische Zwecke («Spoofing») zu bekämpfen. Die mit der Teilrevision eingeführten Massnahmen erscheinen jedoch für eine wirksame Bekämpfung ungenügend und bleiben hinter den Massnahmen anderer europäischer Länder zurück.

Spoofing, insbesondere das Fälschen der Rufnummern, begünstigt Finanzbetrug und führt zu erheblichen wirtschaftlichen und gesellschaftlichen Schäden. Telefonanrufe und SMS entwickelten sich zu einem der zentralen Angriffsvektoren für Finanzbetrug, bei welchen den Opfern bekannte Telefonnummern erhebliches Vertrauen gegenüber der Täterschaft wecken. Trotz erheblicher Anstrengungen und Investitionen in die präventive Aufklärung von Kundinnen und Kunden darüber, dass Anrufer-IDs nicht vertraut werden kann bzw. diese leicht gefälscht werden können (z.B. mittels der durch die Zahlkartenindustrie zusammen mit der Polizei durchgeführten grossflächigen Kampagnen unter dem Dach des Vereins «Card Security»), besteht in der Bevölkerung weiterhin eine breite Wahrnehmung, dass Rufnummern verifiziert und vertrauenswürdig sind. Entsprechend sind griffige Massnahmen verhältnismässig und notwendig, um diesen wesentlichen Angriffsvektor mit technischen und organisatorischen Massnahmen zu verhindern.

1.1. Internationaler Vergleich – wirksame Massnahmen

Im Erläuterungsbericht zum Vorentwurf FMG wird im Bereich Konsumentenschutz auf die Möglichkeiten Rufnummern zu entziehen oder zu sperren fokussiert. Allerdings wäre insbesondere eine Würdigung der in mehreren europäischen Ländern etablierten regulatorischen Grundlagen zur Verhinderung von Anrufen mit gefälschten Anrufer-IDs angezeigt. Die fortschreitend implementierten Massnahmen in anderen Ländern werden den Angriffsdruck auf Länder mit wenig wirksamen Massnahmen erwartungsgemäss weiter verstärken. Erwähnenswert in diesem Zusammenhang sind die Länder Belgien, Tschechische Republik, Finnland, Irland, Italien, Spanien, Frankreich und England, welche alle die Voraussetzungen geschaffen haben, mindestens Festnetzanrufe aus dem Ausland mit inländischen Nummern gänzlich zu blockieren.¹

Insbesondere die in Finnland umgesetzten umfassenden Massnahmen zeigten eine hohe Wirksamkeit zur Bekämpfung von Finanzbetrug in Folge von «Spoofing». So konnte die Schadensumme innert nur einem Jahr nach Umsetzung von Massnahmen von über sieben Millionen Euro pro Jahr auf wenige tausend Euro pro Jahr gesenkt werden.²

Eine weitergehende Regelung zur gänzlichen Blockierung von internationalen Festnetzanrufen mit Schweizer Telefonnummern sowie von internationalen, nicht roamenden Mobilfunkanrufen mit Schweizer Telefonnummern ist vertieft zu prüfen.

1.2. Inländisches Spoofing gleichwertig erfassen

Die Vorlage und die heute geltenden Filterpflichten setzen dort an, wo Anrufe mit Schweizer Anrufer-IDs aus dem Ausland in die Schweiz eingespeist werden. Nach der Wahrnehmung unserer Mitglieder tritt daneben regelmässig auch der Fall auf, dass Schweizer Rufnummern innerhalb der Schweiz gefälscht und über inländische Netzübergabepunkte eingespeist werden. Für die geschädigten Kundinnen und Kunden ist das Ergebnis dasselbe; für die Täterschaft ist die inländische Einspeisung schlicht der Weg des geringeren Widerstands, sobald an der Landesgrenze wirksam gefiltert wird.

Massnahmen, die primär auf grenzüberschreitende Spoofing-Anrufen abzielen, könnten daher in Folge zu einer Verlagerung des Missbrauchs führen, statt ihn zu unterbinden. Es wird daher empfohlen, diese Entwicklung sorgfältig zu beobachten und mögliche Massnahmen weiter zu prüfen, die eine Überprüfung, ob die übermittelte Anrufer-ID der Anschlusskundin oder dem Anschlusskunden tatsächlich zugeteilt ist, sicherzustellen.

¹ <https://eu-etc.com/2025/11/20/anonymisation-or-blocking-of-calls-from-abroad-with-a-national-number-european-countries-are-divided/> (Zugriff 18.08.2026)

² <https://www.tieto.com/en/cases/telecom/global-anti-fraud-model/> (Zugriff 18.08.2026)

Die technischen, organisatorischen und regulatorischen Voraussetzungen dafür, dass Anbieterinnen von Fernmeldediensten die Berechtigung zur Verwendung der übermittelten Anrufer-ID zuverlässig validieren können, sind vertieft zu prüfen und vorzubereiten. Dabei ist insbesondere die schrittweise Einführung einer verbindlichen Validierung zu prüfen, soweit diese technisch zuverlässig umsetzbar und verhältnismässig ist.

1.3. Durchsetzung von Massnahmen

Im Vorentwurf FMG sowie den Verordnungen fehlen an verschiedenen Stellen verpflichtende Elemente, die den Behörden Möglichkeiten eröffnen würden, bei Nichteinhaltung der Gesetzesbestimmungen entsprechende Sanktionen (bspw. Einschränkungen von fernmelderechtlichen Dienstleistungen oder Bussen) auszusprechen. Die vorliegenden Gesetzesanpassungen dürften nur dann eine nachhaltige Wirkung versprechen, wenn auch entsprechende Sanktionen konsequent geprüft und im Gesetz umgesetzt werden können.

Die vorgesehenen Massnahmen auf Gesetzes- und Verordnungsstufe sind hinsichtlich Durchsetzbarkeit mit angemessenen Sanktionsmassnahmen zu ergänzen.

1.4. Widerruf von Nummernblöcken ausländischer Anbieter

In Art. 4 FMG ist ein neuer Absatz 6 einzufügen, damit die zuständige Behörde der ausländischen Anbieterin von Fernmeldediensten mit Schweizer Adressierungselementen bei Nichteinhaltung der gesetzlichen Bestimmungen deren Registration und Leistungserbringung widerrufen kann. Ohne diese Bestimmung erscheint weiterhin problematisch, dass Nummernblöcke, welche an ausländische Anbieter verkauft wurden, bei Nichteinhaltung der gesetzlichen Pflichten nicht mehr zurückgerufen werden können. Damit sollen dem BAKOM Möglichkeiten geschaffen werden, die Registration und Leistungserbringung bei wiederholtem Fehlverhalten zu widerrufen.

In Art. 4 FMG ist ein neuer Absatz 6 einzufügen, damit die zuständige Behörde der ausländischen Anbieterin von Fernmeldediensten mit Schweizer Adressierungselementen bei Nichteinhaltung der gesetzlichen Bestimmungen deren Registration und Leistungserbringung widerrufen kann.

1.5. Sperrung durch Schweizer Anbieter bei Untervergabe

In Art. 6a FMG ist ein neuer Absatz einzufügen, damit die Sperrung auch durch Schweizer Anbieter (bei Untervergabe) oder bei direktem Verkauf der Adressierungselemente ins Ausland durch die zuständige Behörde möglich ist. Ansonsten bestünden keine gesetzlichen Möglichkeiten bei der Vergabe an Anbieter von Fernmeldediensten ins Ausland, wirksame Sperrungen vorzunehmen. Bereits heute treten verschiedene

ausländische Provider auf, welche die Daten der Kunden nicht bekannt geben, wobei keine wirksame Möglichkeit zur Sperrung besteht.

In Art. 6a FMG ist ein neuer Absatz einzufügen, damit Sperrungen bei Untervergabe oder Verkauf von Adressierungselementen ins Ausland möglich sind.

1.6. Sperrung von Rufnummern bei missbräuchlicher Verwendung

In der aktuellen Fassung der Vernehmlassungsvorlage fehlt die Möglichkeit, den Zugang zur Telefonie auch dann sperren lassen zu können, wenn die Rufnummer zwar korrekt registriert wurde, jedoch nachweislich für missbräuchliche Handlungen verwendet wird. Diese Lücke gilt es zu schliessen.

Art. 6a FMG Absatz 1 ist um einen Buchstaben d wie folgt zu erweitern: «... wenn aufgrund konkreter und dokumentierter Anhaltspunkte der begründete Verdacht besteht, dass der Zugang oder die Rufnummer für missbräuchliche Handlungen verwendet wird.»

1.7. Sperrfrist

Die Sperrfrist von maximal fünf Tagen in Art. 6b Abs. 1 FMG ist zu kurz, um weitere Massnahmen prüfen zu können oder, wie im Bericht zur Vernehmlassung dargelegt, die Kriminalitätsstörung (Crime Disruption) über einen ausreichenden Zeitraum aufrechtzuerhalten. Die Frist ist daher gesetzlich auf mindestens 30 Tage zu verlängern, um eine wirksame und nachhaltige Wirkung zu erzielen.

Die maximale Dauer der vorläufigen Sperrung nach Art. 6b Abs. 1 FMG ist von fünf auf 30 Tage zu verlängern. Die Sperrung ist vor Ablauf dieser Frist aufzuheben, sobald die gesetzlichen Voraussetzungen nicht mehr erfüllt sind. Weitergehende Sperrungen im Rahmen eines Strafverfahrens bleiben vorbehalten.

2. Bekämpfung des Missbrauchs von schweizerischen Domain-Namen

Die derzeit in den eidgenössischen Räten hängige Motion Götte (24.4393) soll im Rahmen dieser Teilrevision vollständig umgesetzt werden. Sollte der Ständerat die Motion gemäss Empfehlung der ständerätlichen Kommission für Verkehr und Fernmeldewesen (KVF-S) in der ursprünglichen Fassung überweisen, ist die geforderte Identifikationspflicht bei der Registrierung Schweizer Domains aufzunehmen.

Heute können Betrüger einfach und anonym Schweizer Internetadressen registrieren, um damit das Vertrauen der Bevölkerung in bekannte Marken wie die Post, die SBB oder Banken auszunutzen. Wird der Betrug erkannt und die Webseite gesperrt, ist es meist zu spät. Solche Betrugswellen dauern oft nur wenige Stunden. Dann ist das Geld der Opfer bereits gestohlen. Der Schaden bleibt an den Konsumentinnen und



Konsumenten sowie an der Finanzindustrie hängen, während die Bereitsteller der digitalen Infrastruktur kaum Verantwortung oder Kosten tragen. Betrug muss deshalb verstärkt an der Wurzel bekämpft werden: Dort, wo sich die Betrüger ihre Werkzeuge beschaffen. Genau hier setzt eine Identifikationspflicht an, indem sie den Betrügern die Anonymität nimmt. Die .ch- und .swiss-Domains geniessen als digitales Gütesiegel besonderes Vertrauen. Gerade deshalb dürfen sie Betrügern nicht als erstklassiges Angriffsinstrument dienen. Die Identifikationspflicht bei der Vergabe von Schweizer Domains ist entsprechend im Rahmen der Teilrevision aufzunehmen.

Die Identifikationspflicht bei der Registrierung Schweizer Domains ist im Rahmen der Teilrevision aufzunehmen. Dabei ist eine angemessene Verifikation der Identität der Halterin oder des Halters vorzusehen. Ergänzend sind die im Entwurf vorgesehenen Melde-, Prüf- und Sperrprozesse so auszugestalten, dass qualifizierte Hinweise auf Phishing- und Betrugsseiten unverzüglich beurteilt und notwendige Sperrmassnahmen ohne vermeidbare Verzögerung eingeleitet werden können.

Wir bedanken uns für die Möglichkeit zur Stellungnahme und für die Kenntnisnahme unserer Anliegen.

Freundliche Grüsse

Für SwissDebitPay

Sig. Thomas Weber

Über SwissDebitPay

Der Branchenverband SwissDebitPay fördert die Zusammenarbeit zwischen den Herausgebern von Debit-Zahlungsmitteln in der Schweiz, engagiert sich in nicht wettbewerbsbezogenen Aspekten von gegenseitigem Interesse; bringt sich in den Gestaltungsprozess rechtlicher und regulatorischer Entwicklungen ein; entwickelt Best Practices für die Branche; schützt die Integrität der Debit-Zahlungen; entwickelt Branchenstandards und koordiniert andere branchenweite Initiativen (z.B. solche, die auf Innovation abzielen). Mitglieder von SwissDebitPay sind die grossen Schweizer Debitkarten-Herausgeber, namentlich: UBS Switzerland AG, PostFinance AG, Raiffeisen, Zürcher Kantonalbank, Entris Banking AG, Migros Bank AG, SIX BBS AG, Viseca Payment Services SA, Graubündner Kantonalbank, Luzerner Kantonalbank, Berner Kantonalbank Schwyzer Kantonalbank, Zuger Kantonalbank, Banque Cantonale Fribourg, Bank CIC (Schweiz) AG, Banca Popolare di Sondrio (SUISSE) SA, YAPEAL AG.

Kontakt

SwissDebitPay
Thomas Weber, Geschäftsführer
c/o Kellerhals Carrard KIG, Rämistrasse 5, 8024 Zürich
thomas.weber@swissdebitpay.ch
www.swissdebitpay.ch