

## **Antwort**

### **der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Marcel Emmerich, Lukas Benner, Schahina Gambir, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/ DIE GRÜNEN**  
**– Drucksache 21/3052 –**

### **Love Scamming – Milliardenbetrug durch Organisierte Kriminalität**

#### Vorbemerkung der Fragesteller

Love Scamming – auch unter anderen Begriffen wie „Romance Scamming“ oder „Pig Butchering“ bekannt – ist eine perfide Form des Internetbetrugs, bei dem die organisierten Täter eine romantische Beziehung vortäuschen, um das Vertrauen ihrer Opfer zu gewinnen und sie anschließend finanziell auszubeuten. Betrügerinnen und Betrüger treten meist in Datingplattformen oder sozialen Netzwerken auf, wo sie sich falsche Identitäten schaffen, oft mit gefälschten KI (künstliche Intelligenz)-generierten Fotos und einer emotionalen Ansprache, um Sympathie zu erlangen. Nachdem eine scheinbar enge Beziehung aufgebaut wurde, fordern die Betrügerinnen und Betrüger das Opfer dazu auf, Geld zu schicken. Die erfundenen Geschichten sind vielfältig. Mal werden angebliche Notlagen wie eine Krankheit, ein Unfall oder ein dringender Umzug vorgetäuscht. Mal wollen sie Flugtickets für einen Besuch besorgen oder überzeugen die Opfer davon, Investitionen in vermeintlich lukrative Geschäfte zu tätigen. In manchen Fällen werden die Opfer auch mit Screenshots erpresst, nachdem per Videocall intime Aufnahmen von ihnen gemacht wurden. Die Opfer werden so lange erpresst und betrogen, bis das Vertrauen und das Geld erschöpft sind. Dann bricht der Kontakt ab.

Gerade Organisierte Kriminelle stecken hinter diesem perfiden Geschäftsmodell, das an betrügerische Telefonanrufe erinnert. Allerdings können die Betrügerinnen und Betrüger mithilfe künstlicher Intelligenz ihre Betrugsmasche noch authentischer gestalten. Automatisierte Chats, Deepfakes und synthetische Stimmen helfen den Tätern dabei, weltweit und rund um die Uhr potenzielle Opfer immer effektiver zu täuschen.

Bekanntheit erlangen die Fälle bisher vor allem über Erzählungen der Betroffenen – wie der Anfang 2025 bekannt gewordene Betrug einer Frau, die einhalb Jahre lang dachte, eine heimliche Liebesbeziehung mit einem Prominenten zu führen und im Laufe dessen 830 000 Euro an die Kriminellen überwies ([www.stern.de/lifestyle/leute/brad-pitt-aeussert-sich-zum-love-scam-in-s-einem-namen-35388728.html](http://www.stern.de/lifestyle/leute/brad-pitt-aeussert-sich-zum-love-scam-in-s-einem-namen-35388728.html)).

Love Scamming ist inzwischen ein weltweites Milliardengeschäft für die Organisierte Kriminalität. Kriminelle agieren dabei transnational und über Konti-

nente hinweg. Allein bei der Zentralstelle Cybercrime in Bamberg wurden im Jahr 2024 mehr als 18 000 Fälle erfasst und bearbeitet. Der dadurch entstandene Gesamtschaden lag alleine bei dieser Zentralstelle bei 49 Mio. Euro (<https://www1.wdr.de/nachrichten/nah-dran-cybermafia-doku-100.html>). Laut Vereinten Nationen (VN) liegt der jährliche Umsatz allein der von Südostasien aus agierenden Betrügerinnen und Betrüger bei rund 40 Mrd. US-Dollar. Die Dunkelziffer dürfte noch sehr viel höher liegen, da viele Betroffene sich aus Scham nicht bei der Polizei melden.

Die Betrugsmaschen werden vor allem durch Gruppen der Organisierten Kriminalität durchgeführt, die Betrugszentren kontrollieren. Mit falschen Jobangeboten locken sie Menschen an, halten sie in Zentren fest und zwingen sie unter Gewaltandrohung zum Betrug. Sie werden erst dann wieder freigelassen, wenn ihre Familien Lösegeld zahlen. Wenn sie versuchen, zu fliehen, oder sie nicht die von den Banden vorgegebenen Planzahlen einhalten, droht ihnen Folter oder Mord ([www.ardmediathek.de/video/story/im-inneren-der-cybermafia-love-like-lost/ndr/Y3JpZDovL2Rhc2Vyc3RlLmRlL2FyZC1zdG9yeV8yMDI1LTA2LTEwLTlyLTUw](http://www.ardmediathek.de/video/story/im-inneren-der-cybermafia-love-like-lost/ndr/Y3JpZDovL2Rhc2Vyc3RlLmRlL2FyZC1zdG9yeV8yMDI1LTA2LTEwLTlyLTUw)). Die VN sprechen von moderner Sklaverei und schätzen, dass weltweit über 100 000 Menschen in solchen Zentren festgehalten werden (<https://news.un.org/en/story/2025/05/1163521>). Insbesondere in Myanmar befinden sich zahlreiche dieser Betrugszentren in Gebieten, die von bewaffneten Gruppen, Milizen oder kriminellen Netzwerken kontrolliert werden. Internationale Organisationen dokumentieren, dass dort systematisch Menschenrechte verletzt werden: Menschen werden entführt, eingesperrt, zur Begehung von Betrugshandlungen, einschließlich Love Scamming, gezwungen und bei Fluchtversuchen gefoltert. In Myanmar sind Teile der Scam-Zentren in Konflikt- und Grenzregionen angesiedelt, wo die Gewinne durch Schutzgelderpressung, Besteuerung oder direkte Kontrolle zur Finanzierung bewaffneter Akteure beitragen ([www.theguardian.com/global-development/2025/sep/08/myanmar-military-junta-scam-centres-trafficking-crime-syndicates-kk-park](http://www.theguardian.com/global-development/2025/sep/08/myanmar-military-junta-scam-centres-trafficking-crime-syndicates-kk-park)). Auch in Kambodscha bestehen enge Verbindungen zwischen staatlich geduldeten Machtstrukturen, Organisierter Kriminalität und schweren Menschenrechtsverletzungen in diesen Zentren ([www.amnesty.org/en/latest/news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds](http://www.amnesty.org/en/latest/news/2025/06/cambodia-government-allows-slavery-torture-flourish-inside-scamming-compounds)). Das Auswärtige Amt hat auch aufgrund dieser falschen Jobangebote Teilreisewarnungen für Kambodscha und Thailand ausgesprochen ([www.auswaertiges-amt.de/de/service/laender/kambodscha-node/kambodschasicherheit-220008](http://www.auswaertiges-amt.de/de/service/laender/kambodscha-node/kambodschasicherheit-220008); [www.auswaertiges-amt.de/de/service/laender/thailand-node/thailandsicherheit-201558](http://www.auswaertiges-amt.de/de/service/laender/thailand-node/thailandsicherheit-201558)). Für das Bürgerkriegsland Myanmar hat das Auswärtige Amt eine Reisewarnung ausgesprochen, vor sogenannten Scam Compounds wird explizit gewarnt ([www.auswaertiges-amt.de/de/reise/ndsicherheit/myanmarsicherheit-212100#content\\_1](http://www.auswaertiges-amt.de/de/reise/ndsicherheit/myanmarsicherheit-212100#content_1)).

Ähnliche Dynamiken zeigen sich auch bei weiteren Online-Scams. Auf Onlinemarktplätzen beispielsweise nimmt die Anzahl betrügerischer Aktivitäten, irreführender Versprechen und gefälschter Produkte, die künstlich sichtbar gemacht werden, zu. Neben den Onlinemarktplätzen gibt es täuschend echt aussehende Fakeshops, die Käufer und Käuferinnen immer wieder um ihr Geld bringen. Nahezu jede und jeder achte (12 Prozent) Online-Shopper ist in den vergangenen zwei Jahren auf einen Fakeshop reingefallen, zeigt eine Forsa-Befragung im Auftrag des Verbraucherzentrale Bundesverbands. Besonders ärgerlich: Die Hälfte (50 Prozent) der von der Verbraucherzentrale untersuchten Fakeshops schalten Werbung auf Plattformen von Google oder Meta (Verbraucherreport 2025, Ergebnisse einer repräsentativen Bevölkerungsbefragung, erhoben durch Forsa vom 3. November 2025 [www.vzbv.de/sites/default/files/2025-10/25-11-03\\_Verbraucherreport%202025\\_Chartbericht\\_0.pdf](http://www.vzbv.de/sites/default/files/2025-10/25-11-03_Verbraucherreport%202025_Chartbericht_0.pdf)).

Eine weitere betrügerische Methode sind Financial Scams, bei denen angebliche Handelsplattformen Verbraucherinnen mit Traumrenditen locken ([www.bafin.de/DE/Verbraucher/Finanzbetrug/Anlagebetrug/BetrugHandelsplattformen/handelsplattformen\\_node.html](http://www.bafin.de/DE/Verbraucher/Finanzbetrug/Anlagebetrug/BetrugHandelsplattformen/handelsplattformen_node.html)). Allein in den vergangenen zwölf Monaten erreichten die Marktbeobachtung der Verbraucherzentralen und des Verbraucherzentrale Bundesverbandes (vzbv) Beschwerden zu weit über 100 verschiedenen Plattformen ([www.verbraucherzentrale.de/wissen/geld-versicherungen/](http://www.verbraucherzentrale.de/wissen/geld-versicherungen/)

sparen-und-anlegen/vorsicht-betruegerisches-onlinetrading-54699). Daher ist es zu begrüßen, dass die Europäische Kommission eine koordinierte Initiative gegen Online-Scams und Betrug angekündigt hat (<https://digital-strategy.ec.europa.eu/en/news/press-statement-european-board-digital-services-following-its-16th-meeting>).

Angesichts dieser milliarden schweren Betrugsmaschinen Organisierter Krimineller weltweit stellen sich nach Ansicht der Fragestellenden zahlreiche sicherheits- und verbraucherpolitische Fragen und Herausforderungen mit Blick auf die Arbeit der Bundesregierung beim sogenannten Love Scamming und anderen Online-Scams. Darüber hinaus stellt sich die Frage, wie Bürgerinnen und Bürger davor geschützt werden können und der Kampf gegen die organisierte Kriminalität in diesem Bereich verbessert werden kann.

1. Welche Erkenntnisse hat die Bundesregierung zu den Strukturen Organisierter Kriminalität hinter dem Phänomenbereich des Love Scammings?

Im Bereich des klassischen Love Scammings sind insbesondere Bezüge in westafrikanische Länder festzustellen. Hierbei sind nigerianische Strukturen organisierter Kriminalität (OK) hervorzuheben, denen auch teilweise sogenannte nigerianische Bruderschaften zuzuordnen sind. Diese haben sich auf eine Vielzahl von Betrugsdelikten spezialisiert, darunter vor allem Love Scamming und CEO-Fraud/BEC-Fraud (Business Email Compromise).

2. Welche Betrugsmaschinen sind der Bundesregierung im Bereich des Love Scammings – gegebenenfalls auch unter Verwendung anderer Begriffe – bekannt?

Beim klassischen Love Scam werden über Dating-Webseiten oder soziale Netzwerke Opfern Liebesbeziehungen vorgespiegelt. Häufig täuschen die Täter vor, englischsprachige, westliche Geschäftsmänner oder Militärangehörige zu sein. Aufgrund von Auslandseinsätzen/Dienstreisen wird den Opfern zunächst eine Fernbeziehung suggeriert. Bei den Gesprächen geht es zu Beginn keineswegs um Geld, sondern um den Beruf, die Familie sowie um Liebe und eine gemeinsame Zukunft. Oft werden Geschichten über verstorbene Ehepartner und Kinder dargestellt. Nach einiger Zeit werden Notlagen, beispielsweise ein kostenintensiver Krankenhausaufenthalt oder Probleme mit Kreditkarten, vorgegaukelt und die Opfer dazu gebracht, immer höhere Summen zu überweisen. Mitunter werden die Opfer in einer späteren Phase des Betrugs wesentlich oder unwissentlich als sogenannte Finanzagenten oder „money mules“ zur Geldwäsche eingesetzt.

Beim Betrugsphänomen des sog. „Romance Baiting“ hingegen handelt es sich um eine Form des organisiert begangenen Anlagebetruges unter Verwendung von Elementen des Love Scamming: Hierbei werden attraktive Fake-Profile zur Kontaktabbahnung zu Geschädigten genutzt und diese dann zu angeblichen Investitionen verleitet, überwiegend in Kryptowährungen. Zu einer tatsächlichen Geldanlage kommt es allerdings nicht, der Kontakt wird täterseitig irgendwann abgebrochen und die vermeintlich investierten Gelder werden einbehalten.

Derartige Straftaten werden vornehmlich aus sog. Scam-Centern im südostasiatischen Raum dort vor allem in Myanmar, Laos und Kambodscha (aber auch auf den Philippinen und in Thailand) begangen. Die Organisatoren der Scam-Center und Initiatoren der OK-Strukturen sind oftmals chinesische Staatsangehörige. Es liegen zudem Hinweise vor, die darauf hindeuten, dass ähnliche Strukturen auch in Westafrika und Mittelamerika existieren. Ergänzend wird auf die Antworten zu den Fragen 5 und 6 verwiesen.

3. Was macht nach Ansicht der Bundesregierung Personen in Deutschland zu einem Angriffsziel der Betrügerinnen und Betrüger?
  - a) Wie steht Deutschland als Angriffsziel im europäischen Vergleich?
  - b) Wie steht Deutschland als Angriffsziel im weltweiten Vergleich?

Die Fragen 3 bis 3b werden gemeinsam beantwortet.

Grundsätzlich ist das Vorgehen der Täterstrukturen auf maximale Gewinnerzielung ausgerichtet. Opfer derartiger Betrugsstraftaten werden daher vornehmlich in vergleichsweise wohlhabend geltenden Industrienationen gesucht. Täter zielen weltweit vorrangig auf vermögende Personen ab und nutzen dabei Englisch oder andere weit verbreitete Sprachen. Dies macht auch Deutschland zu einem Ziel für Betrugsversuche. Vergleichende Statistiken liegen nicht vor. Aus dem internationalen kriminalpolizeilichen Informationsaustausch ist jedoch bekannt, dass es auch in anderen europäischen Staaten Geschädigte gleichgelagerter Straftaten gibt.

4. Welche Erkenntnisse hat die Bundesregierung über Ausmaß und Betroffene von Love Scamming in Deutschland seit dem 1. Januar 2020 (bitte nach Herkunftsland, Alter, Geschlecht, Form von Betrug und Bundesland, indem die Betroffenen ermittelt wurden aufschlüsseln)?

Der Bundesregierung liegen keine statistischen Informationen im Sinne der Fragestellung vor. Für die geschätzten Ausmaße der Gewinnerzielung durch südostasiatische Betrugszentren wird auf die Antworten zu den Fragen 5 und 6 verwiesen.

5. Welche Erkenntnisse hat die Bundesregierung über die Betrugszentren?
6. Welche Erkenntnisse hat die Bundesregierung über Menschenhandel, Zwangsarbeit, Freiheitsberaubung und andere Menschenrechtsverletzungen über die Betrugszentren in Myanmar und Kambodscha, insbesondere im Zusammenhang mit Love Scamming?

Die Fragen 5 und 6 werden gemeinsam beantwortet.

In Südostasien, vor allem in Myanmar, Laos und Kambodscha (aber auch auf den Philippinen und in Thailand) werden in professionell organisierten Strukturen, sog. Scam-Centern, über hunderttausend Menschen zum Begehen verschiedener Formen des Online-Betrugs beschäftigt. In sog. „Scam Compounds“ generieren organisierten Gruppen hohe Beträge durch Online-Betrug, laut Schätzungen von UNODC in Höhe von 40 bis 60 Mrd. US-Dollar jährlich. Zum Teil arbeiten die betroffenen Personen freiwillig in den Centern, zum Teil werden diese gegen ihren Willen – auch unter Einsatz von Zwangsmaßnahmen – zur Begehung von Straftaten gezwungen. Der größte Teil der Mitarbeiter kommt aus Ländern der Region. Bei den Betreibern handelt es sich in der Regel um lokale oder regionale Gruppierungen, die weitgehend eigenverantwortlich agieren.

Die Handelnden sind häufig Opfer von Menschenhandel und werden unter Androhung von Gewalt zur Tatbegehung gezwungen. Überwiegend südostasiatische Staatsangehörige werden mittels lukrativer Jobangebote dazu verleitet, ihre Heimatländer zu verlassen, um einer Beschäftigung in anderen südostasiatischen Ländern – hauptsächlich Kambodscha, Laos oder Myanmar – nachzugehen. Vor Ort folgt häufig eine Abnahme von Pässen, unfreiwillige Festhaltung sowie Anwendung von Zwang, um die Betroffenen Personen zur Bege-

hung verschiedener Betrugsdelikte aus Callcentern zu bewegen. Europäische und deutsche Staatsbürger sind kein primäres Ziel, aber grundsätzlich gefährdet und können Opfer von Betrugsdelikten werden.

7. Gibt es nach Kenntnis der Bundesregierung deutsche und europäische Staatsangehörige, die zur Arbeit in die Betrugszentren festgehalten wurden?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor.

8. Ist der Bundesregierung bekannt, ob es Betrugszentren in Deutschland oder Europa gibt, und wenn ja, in welchen Ländern?

Der Bundesregierung liegen keine Erkenntnisse im Sinne der Fragestellung vor. Zum Vorkommen von Betrugszentren im südostasiatischen Raum wird auf die Antwort zu Frage 5 der hiesigen Anfragen verwiesen.

9. Gibt es deutsche und europäischen Staatsangehörige, die an den Betrugszentren beteiligt sind, und wenn ja, wie viele?

Der Bundesregierung liegen keine statistischen Informationen im Sinne der Fragestellung vor.

10. Welche Maßnahmen unternimmt oder plant die Bundesregierung auf nationaler Ebene, um gegen Love Scamming vorzugehen?

Soweit es sich um in Deutschland verfolgbare Straftaten handelt, gehen die deutschen Strafverfolgungsbehörden dagegen im Rahmen strafrechtlicher Ermittlungsverfahren vor, die wenn möglich in gerichtliche Strafverfahren münden. Darüber hinaus erfolgen Präventions- und Aufklärungsmaßnahmen zu dem Phänomen Love Scamming. Für weitergehende Informationen wird auf die Antworten zu den Fragen 10a bis 10d verwiesen.

- a) Welche Aufklärungskampagnen oder Informationsangebote gibt es, um die Bevölkerung vor Love Scamming zu schützen?
- b) Wie werden Plattformbetreiber (z. B. Dating-Apps, soziale Netzwerke) in die Präventionsarbeit einbezogen?
- c) Hält die Bundesregierung die Kooperation der Plattformbetreiber für ausreichend?
- d) Wenn nein, inwiefern plant die Bundesregierung, gesetzliche Vorgaben hierzu anzupassen?

Die Fragen 10a bis 10d werden gemeinsam beantwortet.

Die Bearbeitung präventiver Themenstellungen wird unter anderem durch die gemeinschaftliche Gremienarbeit der Polizeien der Länder und des Bundes sichergestellt. So werden im Bund-Länder-finanzierten Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) Konzepte, Medien und Initiativen entwickelt, die über Kriminalität aufklären und Schutzempfehlungen vermitteln. Das Internetportal [www.polizei-beratung.de](http://www.polizei-beratung.de) ist die zentrale virtuelle Plattform der Polizeilichen Kriminalprävention. Dort finden sich auch Informationsangebote für das Phänomen „Love Scamming“.

Insbesondere wird auf folgende Angebote verwiesen:

- Online-Dating: So schützen Sie sich vor Love Scamming [www.polizei-beratung.de/aktuelles/detailansicht/romance-scamming/](http://www.polizei-beratung.de/aktuelles/detailansicht/romance-scamming/),
- Das Medienpaket – Love Scamming – das sollte man tun [www.polizei-beratung.de/medienangebot/detail/29806-love-scamming-tipps/](http://www.polizei-beratung.de/medienangebot/detail/29806-love-scamming-tipps/),
- Social Media Paket zu Love Scamming: Was ist das eigentlich? [www.polizei-beratung.de/medienangebot/detail/29806-love-scamming-definition/](http://www.polizei-beratung.de/medienangebot/detail/29806-love-scamming-definition/),
- Social Media Paket Love Scamming: Schutz beim Online-Dating [www.polizei-beratung.de/medienangebot/detail/29806-love-scamming-schutz-beim-online-dating/](http://www.polizei-beratung.de/medienangebot/detail/29806-love-scamming-schutz-beim-online-dating/),
- TrueCyberCrime Podcast über Love-Scamming u. a. [www.polizei-beratung.de/aktuelles/detailansicht/truecybercrime-podcast-love-scamming/](http://www.polizei-beratung.de/aktuelles/detailansicht/truecybercrime-podcast-love-scamming/),
- Tipps für Opfer von Romance Scamming [www.polizei-beratung.de/aktuelles/detailansicht/sendungshinweis-traummann-gesucht-albtraum-gefunden/](http://www.polizei-beratung.de/aktuelles/detailansicht/sendungshinweis-traummann-gesucht-albtraum-gefunden/).

Zudem hat das ProPK (Account „Zivile Helden“) in Kooperation mit der Dating-Plattform Tinder am 10. Dezember 2024 eine Informationskampagne zum Phänomen Love Scams auf Social-Media geschaltet.

Der Rechtsrahmen für in der EU tätige Online-Plattformen ist durch den Digital Services Act (DSA – Verordnung (EU) 2022/2065) vollharmonisiert geregelt:

Im Februar 2024 sind mit dem DSA neue Pflichten für Online-Plattformen vollumfänglich in Kraft getreten, die einen Beitrag auch bei der Bekämpfung rechtswidrigen betrügerischen Handelns und illegaler – hierunter gefälschter – Produkten leisten. So sind Hostingdiensteanbieter (hierunter Online-Plattformen) verpflichtet, ein Verfahren einzurichten, mithilfe dessen Nutzer vermutete rechtswidrige Inhalte melden können. Nutzer können auf diesem Weg sowohl Werbeanzeigen für vermuteten Online-Betrug als auch vermutete rechtswidrige Produkte melden. Online-Plattformen sind zusätzlich verpflichtet, ein Beschwerdeverfahren einzurichten, ebenso wie Meldungen von zertifizierten „Trusted Flagger“ priorisiert zu behandeln und mit zertifizierten außergerichtlichen Streitbeilegungsstellen zusammenzuarbeiten. Online-Marktplätze haben zudem zusätzliche Pflichten, hierunter Informationen zur Nachverfolgbarkeit von Händlern zu veröffentlichen und nach bestem Bemühen zu überprüfen. Darüber hinaus müssen sehr große Online-Plattformen bewerten, welche systemischen Risiken (wie etwa die Verbreitung illegaler Produkte, für den Verbraucherschutz, durch vorsätzliche Manipulation des Dienstes oder unauthentische Accounts) auf ihren Diensten bestehen und entsprechende risikominimierende Maßnahmen ergreifen. Sehr große Online-Plattformen müssen darüber hinaus Werbeanzeigen in einem Archiv öffentlich zugänglich und durchsuchbar machen.

Artikel 91 DSA verpflichtet die EU-Kommission erstmals bis zum 17. November 2027 die Verordnung zu evaluieren. Das Ergebnis dieser Evaluierung bleibt abzuwarten, bevor über weitere gesetzliche Vorgaben im Rahmen der Plattformregulierung entschieden werden kann.

- e) Gibt es beim Bundeskriminalamt spezielle Einheiten oder Ermittlungsgruppen innerhalb der Polizei, die auf Love Scamming spezialisiert sind, und wenn nein, ist dies noch geplant?

Das Bundeskriminalamt ist im Bereich des Love Scamming als Zentralstelle der deutschen Polizei tätig. Ermittlungsverfahren zu dem Phänomen Love Scamming werden von den jeweils zuständigen Landespolizeibehörden geführt.



- f) Welche Hilfsangebote (z. B. Hotlines, Beratungsstellen) werden von der Bundesregierung oder in Kooperation mit Nichtregierungsorganisationen (NGOs) bereitgestellt oder unterstützt?

Das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend fördert den Bundesverband der Frauenberatungsstellen und Frauennotrufe (bff) sowie dessen Projekt „Aktiv gegen digitale Gewalt“. Love Scamming wird als Form von digitaler Gewalt gesehen. Ziel der Förderung ist die Weiterentwicklung und Qualifizierung des Frauenunterstützungssystems (Fokus ambulantes Frauenunterstützungssystem) und damit mittelbar eine bessere Unterstützung von gewaltbetroffenen Frauen.

Außerdem wurde im Jahr 2013 per Gesetz das bundesweite Hilfetelefon „Gewalt gegen Frauen“ (HilfetelefonG) beim Bundesamt für Familie und zivilgesellschaftliche Aufgaben eingerichtet.

Das Hilfetelefon „Gewalt gegen Frauen“ richtet sich an Frauen, die Gewalt erleben oder erlebt haben. Unter der Nummer 116 016 können Frauen rund um die Uhr und kostenlos Kontakt zu Beraterinnen aufnehmen – vertraulich und anonym. Es wird zu allen Gewaltformen beraten, neben Häuslicher Gewalt, psychischer, physischer und sexualisierter Gewalt auch zu Mobbing, Digitaler Gewalt und weiteren Gewaltformen (siehe hilfetelefon.de).

Mithilfe von Dolmetscherinnen ist die Beratung beim Hilfetelefon in 18 Fremdsprachen möglich. Auf Wunsch können die Hilfesuchenden einen Kontakt zu geeigneten Beratungsstellen und Hilfsorganisationen in ihrem Umfeld erhalten. Das Angebot richtet sich auch ausdrücklich an Betroffene mit einer Beeinträchtigung oder Behinderung. Sie können eine Beratung in Leichter Sprache oder in Deutscher Gebärdensprache erhalten.

11. Welche Maßnahmen unternimmt die Bundesregierung auf internationaler Ebene, um gegen Love Scamming vorzugehen?

Auf die Antworten zu den Fragen 11a bis 11g wird verwiesen.

- a) Welche Maßnahmen unternimmt die Europäische Union (EU) auch im Rahmen von Europol, und wie beteiligt sich Deutschland hieran?

Europol stellt eine Vielzahl an Maßnahmen zur Verfügung, um Love Scamming zu bekämpfen. Dies umfasst beispielsweise strategische und operative Analysen, Möglichkeiten für den sicheren Informationsaustausch, die Koordinierung von internationalen Verfahren sowie die Bereitstellung von finanziellen Förderungsmöglichkeiten.

- b) Welche Maßnahmen unternimmt die Bundesregierung in ihren diplomatischen Beziehungen zu südostasiatischen Ländern?

Die Bundesregierung verfolgt das Geschehen sorgfältig, stimmt sich mit anderen Staaten ab und spricht das Thema mit betroffenen Staaten an. Zur Eindämmung der regional destabilisierenden Wirkung der Betrugszentren fördert die Bundesregierung die grenzüberschreitende Kooperation bei der Bekämpfung der organisierten Kriminalität.

- c) Welche Maßnahmen unternehmen die VN, und wie beteiligt sich Deutschland hieran?

Die Bundesregierung unterstützt den Trust Fund der Vereinten Nationen für die Opfer von Menschenhandel (UN Trust Funds for Victims of Human Traffick-

ing), der auch die Projektarbeit durch Nichtregierungsorganisationen unterstützt.

- d) Welche Maßnahmen unternimmt Interpol, und wie beteiligt sich Deutschland hieran?

Interpol stellt verschiedene Unterstützungsmaßnahmen zur Verfügung und vernetzt die nationalen Polizeibehörden der Mitgliedstaaten. Zu diesen Unterstützungsleistungen gehören u. a. die Bereitstellung einer sicheren Plattform für den Datenaustausch, Datenbanken sowie Fahndungsausschreibungen auf internationaler Ebene.

Weiterhin unterstützt Interpol die Mitgliedstaaten mit der Koordinierung von internationalen Verfahren im Rahmen von Operations oder Action Days, mit strategischer sowie operativer Auswertung oder auch mittels Ausrichtung von Tagungen. Die Beteiligung deutscher Polizeibehörden an Operations zu Love Scamming von Interpol findet anlassbezogen statt, sofern Bezüge nach Deutschland vorliegen.

- e) Welche Erkenntnisse hat die Bundesregierung über Menschenhandel, Zwangsarbeit, Freiheitsberaubung und andere Menschenrechtsverletzungen über die Betrugszentren in Myanmar und Kambodscha, insbesondere im Zusammenhang mit Love Scamming?

Auf die Antwort zu Frage 6 der hiesigen Anfrage wird verwiesen.

- f) Welche Maßnahmen unternimmt die Bundesregierung zur Unterstützung von NGOs, die sich für Opfer von Menschenhandel – insbesondere in Thailand und Kambodscha – einsetzen?

Auf die Antwort zu Frage 11c wird verwiesen.

- g) Welche Erkenntnisse hat die Bundesregierung über die Organisierte Kriminalität bei Love Scamming durch ihre europäische und internationale Zusammenarbeit?

Die Bundesregierung befindet sich im stetigen Austausch mit ihren europäischen und internationalen Partnern zu diversen OK-Phänomenen. Auf EU-Ebene wird in regelmäßigen Zyklen eine Risikoanalyse zu derzeit relevanten OK-Phänomenen und Schwerpunkten veröffentlicht, das sogenannte „Serious and Organised Crime Threat Assessment“ (EU-SOCTA). Zu Online Scamming allgemein weist das EU-SOCTA für das Kriminalitätsfeld „Online-Fraud/Online fraud schemes“ eine wachsende Bedeutung aus. Zudem finden internationale Konferenzen und Austauschformate statt, um die Bekämpfung von Betrugsphänomenen ganzheitlich durch die Staatengemeinschaft anzugehen, so z. B. der Global Fraud Summit, welcher von Interpol und UNODC ausgetragen wird. Auch in diesem Rahmen werden Erkenntnisse zum Phänomenbereich Betrug ausgetauscht.



- h) Wie bewertet die Bundesregierung die Wirksamkeit der EU-Sanktionen vom 29. Oktober 2024 gegen Personen und Organisationen, die für Scam-Operationen und schwerwiegende Menschenrechtsverletzungen in Myanmar verantwortlich sind?
- i) Wie bewertet die Bundesregierung die Notwendigkeit weiterer EU-Sanktionen im Zusammenhang mit Scam-Zentren in Myanmar, einschließlich möglicher Maßnahmen gegen zusätzliche verantwortliche Akteure oder unterstützende Strukturen?

Die Fragen 11h und 11i werden gemeinsam beantwortet.

Die EU hat am 29. Oktober 2024 die Chit Linn Myaing Group (CLM) und ihren Gründer und ehemaligen Vorsitzenden sowie zwei weitere in Betrugscenter verwickelte myanmarische Personen gelistet. Die Sanktionen wurden wegen massiver Menschenrechtsverletzungen, einschließlich Zwangsarbeit und Folter verhängt. Neben der wirtschaftlichen Sanktionswirkung kommt den Sanktionen auch ein wichtiger politischer Signalcharakter zu.

- 12. Wie viele Fälle von Love Scamming haben die Sicherheitsbehörden in Deutschland in den Jahren 2023, 2024 und 2025 registriert?
  - a) Wie viele der erfassten Fälle führten zu Ermittlungsverfahren?
  - b) Wie viele der erfassten Fälle führten zu Anklagen?
  - c) Wie viele der erfassten Fälle führten zu Verurteilungen?

Die Fragen 12 bis 12c werden gemeinsam beantwortet.

Der Bundesregierung liegen keine statistischen Informationen im Sinne der Fragestellung vor. Die Verantwortung für die Verfolgung von Straftaten in Bezug auf Love Scamming liegt in der Zuständigkeit der Länder.

- 13. Ist der Bundesregierung bekannt, wie viele Betroffene in den Jahren 2023, 2024 und 2025 jeweils Beratungsangebote und Hotlines zu Love Scamming in Anspruch genommen haben?

Der Bundesregierung liegen keine statistischen Informationen im Sinne der Fragestellung vor.

- 14. Wie viele Suizide und Suizidversuche von Betroffenen von Love Scamming sind der Bundesregierung in den Jahren 2023, 2024 und 2025 bekannt?

Die schweren Folgen und die tragische Dimension, die Love Scamming für die Opfer mit sich bringt, sind der Bundesregierung bewusst. Gerade deshalb fördert die Bundesregierung die oben genannten Präventionskampagnen und Hilfsangebote und setzt sich auf internationaler Ebene für die Bekämpfung von Organisierter Kriminalität und damit auch der Ausprägung durch Love Scamming ein. Statistische Informationen zur Anzahl von Suiziden oder Suizidversuchen liegen der Bundesregierung nicht vor.

- 15. In welcher Höhe belief sich in den Jahren 2023, 2024 und 2025 jeweils der Betrugsschaden durch Love Scamming?
  - a) Wie hoch ist der durchschnittliche finanzielle Schaden pro Fall?

- b) Wie viele Betroffene meldeten Verluste über 10 000 Euro, 50 000 Euro oder 100 000 Euro?
- c) Welche Schadenssumme konnte den Betroffenen zurückerstattet werden?

Die Fragen 15 bis 15c werden gemeinsam beantwortet.

Der Bundesregierung liegen keine statistischen Informationen im Sinne der Fragestellung vor. Auf die Antworten zu den Fragen 5. und 6 wird verwiesen.

- 16. Wie schützt die Bundesregierung Verbraucher und Verbraucherinnen vor betrügerischem Handeln, gefälschten oder illegalen Produkten auf Onlinemarktplätzen und durch Fake Shops?

Sowohl die Verbraucherzentrale als auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bieten ein vielfältiges Informationsangebot, um Verbraucherinnen und Verbraucher vor betrügerischem Handeln, gefälschten oder illegalen Produkten auf Online-Marktplätzen zu schützen.

Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) fördert u. a. mit dem Projekt Wirtschaftlicher Verbraucherschutz diverse Informationsangebote der Verbraucherzentralen, die Verbraucherinnen und Verbraucher über betrügerische Angebote im Internet informieren. Diese sind neben vielen Angeboten auf dem Online-Gemeinschaftsauftritt der Verbraucherzentralen unter [www.verbraucherzentrale.de](http://www.verbraucherzentrale.de) zu finden (dort z. B. auch mittels Podcasts [www.verbraucherzentrale.de/podcast/podcast-wie-kaufe-ich-sicher-im-internet-75929](http://www.verbraucherzentrale.de/podcast/podcast-wie-kaufe-ich-sicher-im-internet-75929) oder Infografiken [www.verbraucherzentrale.de/wissen/digitale-welt/onlinehandel/abzocke-online-wie-erkenne-ich-fakeshops-im-internet-13166](http://www.verbraucherzentrale.de/wissen/digitale-welt/onlinehandel/abzocke-online-wie-erkenne-ich-fakeshops-im-internet-13166)).

Zudem fördert das BMJV den Verbraucherzentrale Bundesverband e. V. (vzbv) institutionell zur Wahrnehmung seiner satzungsgemäßen Aufgaben. Im Zuge der Marktbeobachtung wertet der vzbv unter anderem eingegangene Beschwerden der Verbraucherinnen und Verbraucher aus und deckt Probleme und Missstände in Märkten auf. Auch das Europäische Verbraucherzentrum (EVZ) Deutschland, welches ebenfalls u. a. vom BMJV gefördert wird, informiert über betrügerische Aktivitäten im Internet.

Im Rahmen des Digitalen Verbraucherschutzes des BSI wurde zudem eine Reihe von Maßnahmen zur Sensibilisierung entwickelt und den Bürgerinnen und Bürgern zur Verfügung gestellt, dazu zählen u. a.

- Diverse Informationsangebote auf der Website des BSI, u. a.; [www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Shopping/Worauf-beim-Online-Einkauf-zu-achten-ist/worauf-beim-online-einkauf-zu-achten-ist.html](http://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Shopping/Worauf-beim-Online-Einkauf-zu-achten-ist/worauf-beim-online-einkauf-zu-achten-ist.html),
- Pressemitteilungen zur Sensibilisierung, z. B. anlässlich des Black Friday; [www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251125\\_Black-Friday-Deals\\_Betrugsmaschen.html](http://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/251125_Black-Friday-Deals_Betrugsmaschen.html),
- Checklisten in Kooperation mit ProPK, z. B. Betrug beim Onlinebanking; [www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschuren/Wegweiser\\_Checklisten\\_Flyer/Checkliste\\_BSI\\_ProPK\\_Onlinebanking.pdf?\\_\\_blob=publicationFile&v=3](http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschuren/Wegweiser_Checklisten_Flyer/Checkliste_BSI_ProPK_Onlinebanking.pdf?__blob=publicationFile&v=3),
- Checklisten in Kooperation mit Verbraucherzentralen zum Thema Online-shopping; [www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kampagne/Online-shopping\\_SOS\\_Karte.pdf?\\_\\_blob=publicationFile&v=5](http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kampagne/Online-shopping_SOS_Karte.pdf?__blob=publicationFile&v=5).

Zudem wird das Thema durch das BSI sowie durch die Verbraucherzentralen und Verbraucherzentrale Bundesverband e. V. (vzbv) auch regelmäßig auf Social Media und auf Veranstaltungen aufgegriffen.

Des Weiteren wird im Digitalen Verbraucherschutz des BSI die Transparenz von Produkten durch Maßnahmen wie das IT-Sicherheitskennzeichen gefördert, um Verbraucherinnen und Verbrauchern eine Möglichkeit der Auswahl sicherer Produkte an die Hand zu geben.

Insgesamt wird das Sicherheitsniveau von Produkten durch Anforderungen im Rahmen der Standardisierung und Regelung zu Produkten angehoben. Für digitale Produkte wird im Rahmen des Cyber Resilience Acts ab dem Jahr 2027 eine weitere Grundlage für Produktsicherheit gesetzt.

- a) Inwieweit hat sich dieser Ansatz im Zuge des Gesetzes über Digitale Dienste verändert?

Die Bundesregierung setzt sich gegenüber der Europäischen Kommission dafür ein, dass der Digital Services Act („DSA“, europäisches Gesetz über Digitale Dienste) konsequent umgesetzt wird. Dieser legt Plattformbetreibern umfassende Sorgfaltspflichten im Internet auf. Sehr große Plattformen müssen eine Risikoanalyse und Risikominderungsmaßnahmen durchführen und spätestens, wenn sie von Angeboten für Fälschungen oder illegale Produkte Kenntnis erlangen, diese entfernen.

Der DSA umfasst lediglich die Rechte und Pflichten von Vermittlungsdiensten, wozu insbesondere Online-Plattformen zählen. Er ist daher insbesondere nicht anwendbar für Fake-Shop-Webseiten. Zu den grundsätzlichen Inhalten des DSA wird auf die Antworten zu den Fragen 10a bis 10d verwiesen.

Für die Durchsetzung der DSA-Vorschriften über systemische Risiken gegenüber Vermittlungsdiensten ist die EU-Kommission zuständig. Diese hat bereits Verfahren gegen die sehr große Online-Marktplätze AliExpress und Temu eröffnet, dies insbesondere mit Blick auf die Verbreitung illegaler Produkte. AliExpress hat Verpflichtungszusagen abgegeben.

Der Digital Services Coordinator (DSC) in der Bundesnetzagentur (BNetzA) hat seit Sommer 2025 Kontakt zu verschiedenen Behörden in Deutschland aufgenommen, die sich seit geraumer Zeit mit dem Thema Online-Betrug beschäftigen. Auf der europäischen Ebene hat der DSC in Arbeitsgruppe 5 „Verbraucherschutz und Online-Marktplätze“ des Europäischen Gremiums für digitale Dienste den stellvertretenden Vorsitz inne. In dieser Arbeitsgruppe wurde zuletzt ein eigener Workstream zu Online-Betrug eingerichtet.

- b) Wie viele Verstöße liegen dem Digital Service Coordinator (DSC) bereits vor, und wie viele gehen regelmäßig ein?

Die Frage wird dahingehend verstanden, dass sie sich auf dem DSC vorliegenden Ermittlungen des DSC zu Online-Marktplätzen handelt. Der DSC nimmt ausschließlich Beschwerden aufgrund von DSA-Verstößen entgegen. Der DSC ist nicht zuständig für die Bearbeitung von Meldungen zu illegalen Produkten oder Betrugsfällen. Er übernimmt in keinem Fall eine Bewertung oder Kontrolle von Inhalten oder Produkten. Er prüft, ob die Plattformen die Rechte und Pflichten aus dem DSA erfüllen, also z. B. eine geeignete Möglichkeit zur Meldung rechtswidriger Inhalte bereitstellen und Beschwerde- und Streitbeilegungsmechanismen eingerichtet haben.

In eigener Zuständigkeit ermittelt der Digital Services Coordinator in sechs Fällen gegen Online Marktplätze und prüft, ob diese die Vorschriften des DSA einhalten, hierunter die Vorschriften über das Melde- und Abhilfeverfahren so-

wie die Nachverfolgbarkeit von Händlern. Da es sich hierbei um Online-Plattformen unterhalb der Schwelle sehr großer Online-Plattformen handelt, sind nur die allgemeinen DSA-Vorschriften (Artikel 11 bis 32 DSA) einschlägig, nicht jedoch die Vorschriften über systemische Risiken. In einigen Fällen haben die Anbieter von Online-Marktplätzen ihren Dienst nach Intervention des DSC DSA-konform ausgestaltet. In anderen Fällen sind die Ermittlungen noch nicht abgeschlossen. Entsprechend ist noch in keinem Fall ein Verstoß gegen den DSA durch einen Online-Marktplatz mit Sitz oder gesetzlichem Vertreter in Deutschland festgestellt worden.

- c) Wie plant die Bundesregierung, bei wachsendem Aufkommen von Online-Scams nachzusteuern und die Aufsichtsbehörden zu stärken?

Die Bundesregierung setzt sich aktiv für fairen Wettbewerb im Onlinehandel sowie den Schutz von Verbraucherinnen und Verbrauchern ein. Im Januar hat die Bundesregierung einen Aktionsplan E-Commerce veröffentlicht, der darauf abzielt, dem zunehmenden Import nichtkonformer Produkte aus Drittstaaten entgegenzuwirken. Dabei liegt ein Fokus auf der Stärkung der Marktüberwachung im Onlinehandel. Im Rahmen des Praxischecks „Marktüberwachung im Onlinehandel“ entwickelt das Bundesministerium für Wirtschaft und Energie (BMWE) derzeit gemeinsam mit Marktüberwachungsbehörden und anderen relevanten Stakeholdern konkrete Vorschläge, wie die Marktüberwachungsbehörden effizienter und wirkungsstärker im Onlinehandel vorgehen können. Das BMWE wird sich zudem aktiv bei dem von der Europäischen Kommission geplanten „Product Act“ u. a. zur Überarbeitung der Marktüberwachungs-Verordnung und des New Legislative Frameworks einbringen. Darüber hinaus unterstützt das BMWE die von der Europäischen Kommission vorgeschlagene Marktüberwachungsbehörde auf EU-Ebene in einigen Prioritätsbereichen wie E-Commerce Importe aus Drittstaaten.

- d) An welche (Beschwerde-)Stellen können sich betrogene Verbraucher und Verbraucherinnen wenden, und wie machen diese Anlaufstellen auf sich und die Betrugsmaschen aufmerksam?

Für Verbraucherinnen und Verbraucher besteht immer die Möglichkeit, sich an eine Verbraucherzentrale zu wenden. Diese können auch in Einzelfällen beratend tätig werden. Sofern es sich jedoch um eine Straftat handelt, sind vorrangig die Strafverfolgungsbehörden zuständig. Strafanzeigen können in Präsenz auf der zuständigen Polizeiwache oder auch online in sogenannten „Online-wachen“ gestellt werden.

Das BSI verweist auf seiner Webseite über das Format Cyber-Sicherheitslotse auf die relevanten Akteure und Anlaufstellen zum Thema Fakeshops: [www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Shopping/Worauf-beim-Online-Einkauf-zu-achten-ist/worauf-beim-online-einkauf-zu-achten-ist.html](http://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-Banking-Online-Shopping-und-mobil-bezahlen/Online-Shopping/Worauf-beim-Online-Einkauf-zu-achten-ist/worauf-beim-online-einkauf-zu-achten-ist.html).

- e) Sind aus Sicht der Bundesregierung die Beschwerdestellen, wie zum Beispiel der Digital Service Coordinator ausreichend bekannt, und wenn nein, was unternimmt die Bundesregierung, um die Bekanntheit für Verbraucher und Verbraucherinnen zu erhöhen, um ihre Fälle zu melden und sichtbar zu machen?

Der DSC beteiligt sich an einer Informationskampagne zu Betrug, der beispielsweise über Online-Plattformen oder Online-Marktplätzen angebahnt wird. In diesem Zusammenhang veröffentlichte der DSC am 28. November 2025 eine Pressemitteilung sowie einen Hinweisartikel auf seiner Website, um Ver-

braucherinnen und Verbrauchern Hilfestellungen zum Umgang mit betrügerischen Inhalten auf Vermittlungsdiensten bereitzustellen. Zudem flankiert der DSC eine Informationskampagne der EU-Kommission zu Online Scams über Social Media Post auf den Kanälen der BNetzA.

Darüber hinaus steht der DSC im Austausch mit den Marktüberwachungsbehörden und den Verbraucherschutzzentralen. Zudem führt der DSC unter dem Titel „Online-Marktplätze @DSC“ in regelmäßigen Abständen Online-Veranstaltungen mit unterschiedlichen Stakeholdern, u. a. auch zu den genannten Themen, durch.

17. Welche Maßnahmen unternimmt oder plant die Bundesregierung, um gegen Financial Scamming und unseriöse Trading-Angebote vorzugehen?

Auf die Antwort der Bundesregierung zu Frage 9 der Kleinen Anfrage der Fraktion Die Linke auf Bundestagsdrucksache 21/2145 sowie zu den Fragen 17b bis 17d der hiesigen Anfrage wird verwiesen.

- a) Welche Aufklärungskampagnen oder Informationsangebote gibt es, um die Bevölkerung vor Financial Scamming zu schützen?

Auf die Antwort der Bundesregierung zu Frage 9 der Kleinen Anfrage der Fraktion Die Linke auf Bundestagsdrucksache 21/2145 wird verwiesen.

- b) Wie werden Plattformbetreiber (z. B. ETF (Exchange Trades Fund)- und Trading-Plattformen) in die Präventionsarbeit einbezogen?

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bezieht bei Verbraucheraufklärungen zu Financial Scamming Plattformbetreiber nicht ein, sondern wendet sich über ihre Webseite direkt an die Verbraucher.

- c) Gibt es beim Bundeskriminalamt spezielle Einheiten oder Ermittlungsgruppen innerhalb der Polizei, die auf Financial Scamming spezialisiert sind, und wenn nein, ist dies noch geplant?

Das Bundeskriminalamt ist im Bereich des Financial Scammings als Zentralstelle der deutschen Polizei tätig. Ermittlungsverfahren zu dem Phänomen Love Scamming werden grundsätzlich von den jeweils zuständigen Strafverfolgungs- und Polizeibehörden der Länder geführt.

- d) Welche Hilfsangebote (z. B. Hotlines, Beratungsstellen) werden von der Bundesregierung oder in Kooperation mit Nichtregierungsorganisationen bereitgestellt oder unterstützt?

Auf die Antwort der Bundesregierung zu Frage 9 der Kleinen Anfrage der Fraktion Die Linke auf Bundestagsdrucksache 21/2145 wird verwiesen.

- e) Sind aus Sicht der Bundesregierung die Überwachung von Kontoaktivitäten und technischen Systemen, wie Onlinebanking oder Banking-Apps, gegen Angriffe ausreichend geschützt, und wenn nein, warum verpflichtet die Bundesregierung die Anbieter nicht, nachzujustieren?
- f) Sind aus Sicht der Bundesregierung zum Schutz von Verbrauchern und Verbraucherinnen Sorgfaltspflichten für Zahlungsdienstleister ausreichend konkret gesetzlich definiert, und wenn nein, warum nicht?

- g) Wie plant die Bundesregierung, bei wachsendem Aufkommen von Financial Scams nachzusteuern und die Aufsichtsbehörden zu stärken?

Die Fragen 17e bis 17g werden gemeinsam beantwortet.

In Bezug auf die Zahlungsdienstleister bestehen seit der Umsetzung sicherheitstechnischer Anforderungen der Richtlinie (EU) 2015/2366 (Payment Services Directive, kurz PSD 2) zum 14. September 2019 aufsichtsrechtliche Pflichten der Zahlungsdienstleister, die Betrugsfälle im Zahlungsverkehr bekämpfen sollen (insbesondere Starke Kundenauthentifizierung und Transaktionsüberwachung). Diese Pflichten sind in Deutschland insbesondere im Zahlungsdiensteaufsichtsgesetz konkret gesetzlich definiert. Die BaFin beaufsichtigt die Zahlungsdienstleister hinsichtlich der Einhaltung der aufsichtlichen Anforderungen. Da es sich bei der PSD 2 um eine europäische Vollharmonisierungsrichtlinie handelt, können auf nationaler Ebene weder strengere noch weniger strenge Anforderungen umgesetzt werden. Auf EU-Ebene werden derzeit Verhandlungen zum Vorschlag für eine Payment Services Regulation (PSR) sowie eine Payment Services Directive 3 (PSD 3) geführt, die die Regelungen der PSD 2 weiterentwickeln werden. Dabei enthält insbesondere die PSR nach aktuellem Stand zusätzliche Pflichten für Zahlungsdienstleister, um Zahlungsbetrug weiter einzugrenzen (etwa deutlichere Anforderungen an die Transaktionsüberwachung sowie die Pflicht, Zahlungen bei Betrugsverdacht künftig noch effektiver zu stoppen). Die Verhandlungen werden voraussichtlich Anfang nächsten Jahres abgeschlossen werden.



*Vorabfassung - wird durch die lektorierte Version ersetzt.*

*Vorabfassung - wird durch die lektorierte Version ersetzt.*