Victim Support Europe

Victim Support Europe (VSE) Submission to the European Commission Consultation on the Action Plan to Fight Online Fraud

1. Problem Definition and Rationale

Fraud is among one of the most pervasive and rapidly evolving threats to global security, economic stability and public trust. As a significant transnational threat, fraudsters operate across borders, exploiting digital platforms, financial systems and jurisdictional gaps – making isolated national efforts insufficient. A strong coordinated EU response is urgently needed to build collective resilience, disrupt and dismantle organized criminal groups involved in fraud and strengthen EU and international cooperation. Let's not forget that according to the EU Fundamental Rights Agency (FRA), about 1 in 4 Europeans report being victims of consumer fraud[1].

Online fraud represents a swiftly growing and increasingly complex form of crime in the European Union, enabled by digitalisation, artificial intelligence, international financial systems, and cross-border anonymity. UNODC categorises online fraud (6 categories including identity fraud, relationship and trust fraud, consumer fraud) and highlights its dynamic, continuous and adapting nature[2].

Despite existing EU and national measures, the incidence and impact of online fraud continue to increase, indicating persistent implementation gaps and insufficient coordination across sectors and Member States (Europol, 2023[3]). For instance, there is an average of 56% of adults who have experienced fraud in the past years, with the emotional suffering[4] being immense due to the **manipulation**; and nearly 1 in 2 people in the EU have been targeted by online or phone scams[5].

While current policy responses focus primarily on prevention, detection, and enforcement, the **human impact of fraud remains systematically underestimated**. Victims experience not only financial losses but also psychological trauma (i.e. love, loss, shame), loss of trust, social stigma, and long-term disengagement from digital and institutional systems (FRA, 2023)[6]. The impact of online fraud on victims relates, then, to huge financial loss and serious psychological harm, (self-)shaming, manipulation, and isolation (i.e. the psychological harm is comparable to any harm inflicted by domestic violence). Hence there is need for more specialised support services and peer support groups[7].

[1] https://fra.europa.eu/en/news/2021/consumer-fraud-affects-1-4-europeans
[2] https://www.unodc.org/documents/organized-crime/Publications/IssuePaperFraud-eBook.pdf
[3] https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023
[4] https://commission.europa.eu/system/files/2020-01/factsheet_fraud_survey.final_.pdf
[5] https://www.consilium.europa.eu/en/policies/top-cyber-threats/
[6] https://fra.europa.eu/en/publication/2023/victims-rights
[7] https://www.researchgate.net/publication/396117587_Poster_ROMANCE_SCAM_VICTIMS_RECOVERING_TOGETHER_-_Peer_Support_Group_Model_for_Recovery

Under-reporting remains significant (e.g. victims have no way to easily retrieve data on the fraud), reducing the effectiveness of enforcement and distorting evidence bases for policymaking; this is important as according to FRA research[8], two-thirds of victims do not report being harmed.

Several types of fraud that are prevalent in cross-border e-commerce. These include fraudulent websites, phishing scams, identity theft, and online dating fraud; fake websites fail to deliver products, and investment scams refer to traders outside the EU who are not authorized to sell their products within the EU, leading to substantial financial losses[9].

For example, with **online shopping scams** on the rise, campaigning should aim to inform the public about these deceptive schemes and how they can be reported under the Digital Services Act (DSA) Notice and Action mechanism. This reporting tool provides key advantages for users, including transparency: platforms must notify users of their decision (i.e. whether the reported scam was removed or not) and allow users to appeal if necessary. Additionally, the DSA ensures platforms are legally accountable for illegal content reported to them, potentially facing liability if they fail to act.

Due to the nature of the crime, online fraud is one of the key threats for the EU and stressed that the victims are attacked in their safe environment at home, making them more vulnerable.

From a better Regulation perspective, this constitutes a **structural policy failure**: without adequately addressing victim needs, current systems fail to achieve their intended outcomes, namely effective crime prevention, trust in digital markets, and respect for fundamental rights. Reporting fraud is not enough: **victims need emotional support, clarity on rights, guidance on recovery, and help navigating justice systems. Understanding the nature of crime is only the first step to respond to victims' needs.**

A victim-centred, trauma-informed approach is therefore not an additional policy layer but a **necessary condition for effectiveness, coherence, and EU added value**. This submission aims to strengthen efforts regarding advancing policy, developing and implementing solutions for cooperation at the EU level, researching, supporting victims of online fraud and communicating with them, and related activities. **The coming EC Action plan on online fraud** has to be based not only on whole-society-approach (i.e. stressing the need for coordination between the law enforcement, consumer bodies, financial institutions, private partners and civil society), pro-active actions related to investigation, prosecution, assistance to victims and recovery of funds, **but mostly on a victim-centred approach responding to victims' needs.**

Every day, cybercrime and online fraud leave millions of Europeans feeling alone, scared, and uncertain. At VSE, we know that behind every statistic is a real person; a victim who needs more than advice and is in need of a lifeline. That's why in VSE we put **victims at the heart** of everything we do: we listen to their voices, co-design solutions with them, and ensure they can **report crime safely, be fully informed, participate meaningfully, feel secure, and achieve true restoration**. Technology changes fast, but support must move faster. By empowering victims and embedding their insights into every policy and service, we can build **safer, more just, and more resilient societies**; online, offline, and across borders.

Beyond online fraud, victims face the impacts of **cybercrime, AI-driven fraud, digital exploitation, and trafficking**. Criminal networks are increasingly sophisticated, agile, and cross-border, leveraging

[8] https://fra.europa.eu/en/news/2021/violence-and-harassment-across-europe-much-higher-official-records
[9] https://www.eccnet.eu/publication/online-fraud

technology to expand operations rapidly while evading detection. Victims of cross-border crime often encounter fragmented services, unclear responsibilities, and limited access to justice. The need for cross-border cooperation comes from the cross-border character of the crime. As discussed at the 2nd Eurojust Symposium on victims' rights[10], online fraud typically concerns a large number of victims from different countries while the 80 % of all online investment fraud starts with advertisements on social media platforms – hence the need to cooperate with private actors.

Overall, **challenges relate to the investigation of online fraud** such as the global scale, the hugenumber of victims in different countries, and the large quantity of data to investigate. Thus, there is a need for specialised law enforcement teams using cross-border cooperation and modern IT tools. Additional **difficulties relate to restitution and compensation**; in this context the limits of the 2018 Regulation on freezing and confiscation[11] has to be taken into account.

This is why **victim-centred approaches** are crucial: listening to victims, protecting them first, and designing services:

- **National Victim Support Frameworks:** ensuring coordinated, high-quality, and harmonised services across Member States.
- **Access to Safe Justice:** trauma-informed processes, protection, and minimising secondary victimisation.
- **Victim-Centric Approaches:** recognition, empowerment, dignity, and meaningful participation.
- **Effective Communication with Victims:** ensuring clear, respectful, and trauma-informed guidance.
- **Sustainable Funding** and **116 006 Helplines** for universal and accessible support.
- **Strong Data Protection Standards** safeguarding privacy and accessibility.

2. Policy Objectives: Practical steps and requirements for success

The Action Plan should pursue the following interlinked objectives which describe positioning for action, partnerships, support and resources:

- **Reduce the incidence and impact of online fraud**, including telephone-enabled fraud, across the EU.
- **Improve effectiveness of reporting, detection, and enforcement** through increased victim trust and engagement. There is a clear need to enhance trust in law enforcement and set up alternative reporting options (e.g. systematic use of third-party reporting).
- **Ensure compliance with EU victims' rights standards**, notably Directive 2012/29/EU.
- **Strengthen resilience and trust** in digital environments, financial systems, and public institutions.

[10] https://www.eurojust.europa.eu/sites/default/files/assets/files/second-symposium-on-victims-rights-23-april-2025.pdf
[11] https://eur-lex.europa.eu/eli/reg/2018/1805/oj/eng

- **Deliver EU added value** by addressing cross-border challenges that cannot be effectively tackled by Member States acting alone. Embed **victim-centred standards** into national and international responses, ensuring trauma-informed, safe, and accessible reporting and support.
- **Enhance cross-border responses:** fully implement 116 006 helplines, coordinated referral pathways, interpretation/translation, and remote participation in justice proceedings. To achieve all these, there is a need to emphasise the need for cross-border referral systems, so victims in different countries can access support and justice.
- **Address tech-enabled crime (incl. online fraud):** integrate AI and cybersecurity foresight, expand specialised support for cybercrime, online fraud, and digital exploitation, and implement preventive strategies.
- **Evidence-informed approaches:** combine desk research and interviews with victims, law enforcement, judicial authorities, defence lawyers, companies, and victim support services across eight Member States to identify practical solutions and promising practices.
- **Empower children, youth,** and the elderly to resist online organized crime by embedding early prevention, resilience, and victim support into education and community programs.
- Equip non-governmental stakeholders with practical skills to prevent and combat organised crime, for instance by **training local NGOs** on identifying early signs of exploitation in schools and by supporting responsible authorities and civil society actors to develop cross-border referral pathways for victims.
- **Ensure sustained funding** for general and specialised victim services, including online fraud, cybercrime, domestic violence, and terrorism-related cases.
- **Multi-sector partnerships** among governments, NGOs, UN agencies, and networks like VSE to enable coordinated, evidence-based, and cross-border responses. For instance, law enforcement partnerships and multi-agency investigations (police, prosecutors, Europol / Eurojust) when supporting victims, both criminally and in referral, can be foreseen.
- **Robust IT and data systems** to safeguard sensitive victim information, enhance cybersecurity, and enable safe referrals.
- **Research and foresight capacity** to anticipate emerging risks from technology, AI, and organised crime adaptation.

3. Intervention Logic: Integrating Victim-Centred Approaches Across the Policy Cycle

3.1 Victim-Centred Prevention and Early Intervention

Evidence shows that policies which fail to address the psychological and social dimensions of crime generate low reporting rates and limited deterrence (FRA, 2023)[12]. The Action Plan should therefore

[12] https://fra.europa.eu/sites/default/files/fra_uploads/pr-2023-underpinning-victims-rights_en.pdf

integrate trauma-informed, victim-sensitive approaches from the first point of contact. Member States should mandate reporting mechanisms and helplines (e.g. 116 006), especially designed for fraud victims, following EU policies, legislation provisions and frameworks.

Key measures should:

- Recognise online fraud victims as **rights-holders**, entitled to information, support, and protection under EU law. Being scammed can happen to anyone – scammers are skilled and target people of all ages and backgrounds. Acting quickly can help minimise damage and protect others.
- Embed dignity, empathy, and validation in reporting mechanisms, law enforcement responses, and public communication.
- Ensure **early access to support services**, including psychosocial support and legal information, immediately after fraud is suspected or identified. EU countries need to ensure victim support organisations offer sufficient support. These organisations should follow clearly defined performance standards which should be monitored. EU countries should also offer comprehensive victim support services tailored to the needs of different groups of victims.
- Raising awareness (e.g. diverse campaigns) on the risks/threats, among stakeholders and not only victims, and educating the public on worrisome signs, how to recognise fraud, and on building empathetic approaches to victims of online fraud (e.g. adding curricula at schools to enhance prevention and work with families/employees on how to recognise fraud etc.). Adding to this, a good practice has been the EC DG CNECT Christmas 2025 main social media tools[13] campaign (endorsed and supported by VSE) on **raising awareness of the existence of the DSA notice and action mechanism to report financial frauds, especially shopping scams, to platforms.**
- Dissemination of stay safe tip sheets to spot illegal content or a suspected scam, report it directly to appropriate platforms[14].

These measures directly contribute to **effectiveness** by increasing reporting and cooperation, and to **efficiency** by reducing repeated victimisation and long-term harm.

3.2 Prevention Through Empowerment and Digital Literacy

Digital literacy and informed skepticism are critical preventive tools, particularly in light of AI-enabled fraud and behavioural manipulation techniques. However, prevention strategies must avoid victim-blaming and recognise systemic responsibilities.

The Action Plan should:

[13] https://digital-strategy.ec.europa.eu/en/policies/dsa-notice-and-action-mechanism. The landing page provides detailed information on the DSA notice and action mechanism, explaining its purpose, functionality, and importance. It also offers guidance on identifying shopping scams and staying safe online, along with resources for victims seeking support. This page is available in all EU languages through automatic translation and can serve as a hub for national campaigns.

[14] https://digital-strategy.ec.europa.eu/en/policies/dsa-notice-and-action-mechanism

- Support EU-wide awareness campaigns on emerging fraud typologies (Europol, 2023)[15].
- Invest in inclusive digital literacy programmes that promote critical thinking, identity verification, and recognition of manipulative tactics (i.e. the seriousness of consequences of online fraud for victims is often underestimated; crimes involving psychological manipulation – such as romance, investment fraud, sextortion, grooming – leave victims devastated and in a need of targeted support).
- Protect victims better from secondary victimisation. Victims are often further traumatised by having to repeatedly talk about their experiences, insensitive comments or seeing their abuser. EU countries need to ensure that police officers receive practical guidance on protecting victims from repeat and secondary victimisation.
- Provide accessible self-protection tools and guidance in all EU languages.

This approach enhances **proportionality and social acceptance**, while contributing to long-term prevention outcomes.

3.3 Cross-Sector and Cross-Border Coordination

Online fraud is a cross-border phenomenon requiring coordinated EU action to ensure added value. Fragmented reporting channels, siloed data, and inconsistent cooperation undermine enforcement outcomes. Services should be coordinated through the inclusion of referrals, national frameworks or support (with cross-border provisions), individual needs assessment, funding programmes, access to safe justice, and compensation for the lost assets.

VSE recommends:

- Structured cooperation frameworks between law enforcement, financial institutions, platforms, consumer authorities, and victim support organisations.
- Secure, real-time information-sharing mechanisms, with appropriate safeguards under the GDPR.
- Establishment of protocols to identify the situation, map referrals and support services, and assist in writing the police report.
- Streamlined, victim-friendly reporting systems with clear feedback loops and reporting pathways that are safe for victims (e.g. 116 006 helplines, specialised helplines, online support schemes, third-party reporting etc.).

Improved coordination enhances **coherence** across EU policies and strengthens **operational effectiveness**. Platforms have a major responsibility to protect users, but the report can make a real difference; that is the reason why victim-oriented reporting is crucial; reporting illegal content online, including scams, fake or unsafe products, and illegal goods are good practices embedded into the DSA reporting tool.

3.4 Access to Justice, Remedies, and Recovery

[15] https://www.europol.europa.eu/how-we-work/public-awareness-and-prevention-guides

Impact assessments consistently show that lack of access to justice reduces the deterrent effect of criminal law and undermines public trust. For fraud victims, procedural complexity and lack of information are major barriers (FRA, 2023).

The Action Plan should ensure:

- Access to specialised legal assistance for online fraud victims.
- Integrated support models combining psychosocial assistance and procedural guidance.
- Clear pathways to restitution, compensation, and asset recovery where feasible.
- Setting up an after-care plan on the basis of crisis intervention, recovery/support, checking-in upon 6 weeks, calling victims regularly. Long-term support is crucial for victims; it has to be guaranteed both emotionally and legally long after the crime (not just at the reporting phase).

These measures support the victim's empowerment in a tailored approach and a long-term manner, enhance **fundamental rights compliance** and improve **outcome sustainability and the chances for no repeat vicitmisation instances**.

4. Expected Impacts

A victim-centred Action Plan is expected to deliver:

- Increased reporting rates and improved data quality.
- Enhanced enforcement outcomes through victim cooperation.
- Reduced long-term psychological and financial harm.
- Improved trust in digital markets and institutions.
- Greater coherence between fraud prevention, victims' rights, and digital policy frameworks.

5. Monitoring, Evaluation, and Indicators

To ensure accountability and learning, the Action Plan should include:

- Indicators measuring not only fraud reduction but also victim confidence, access to support, and satisfaction with responses.
- Disaggregated data collection where appropriate. Collecting **qualitative data from victims** to inform better support mechanisms can help feed into EU-level policy and law enforcement practice.
- Regular evaluation involving civil society and victim organisations.

Monitoring victim outcomes is essential to assess **effectiveness and EU added value and integrate victim-centric and trauma-informed approaches**.

6. Main take-away messages

- **Prevention is key**. More awareness is needed about the nature, the forms, and consequences of online fraud to avoid victimisation, to acknowledge it and take appropriate steps when it is happening. **Specialised training is necessary** for law enforcement and judiciary to facilitate crime reporting and improve victims' journey through the justice schemes (EJTN and CEPOL to take actions). There is a need to reinforce the protection against **online fraud from the consumer perspective** as flagged in the newly adopted 2030 Consumer Agenda.
- **Shame is a powerful feeling** - common to victims of online fraud, often amplified by victim-blaming by law enforcement, the offenders, and the society. It leads to underreporting, secondary victimisation, re-victimisation and empowers the offenders.
- **Promotion of a whole-society-approach** – By speaking common languages and showcasing real time examples we can make a difference (e.g. an example of a shop assistant who made the victim realise that she was subject to fraud and stopped sending the coupons etc.).
- Developing a **strong public–private partnership** with telecom companies, social media platforms and banks is essential for crime prevention and identification of victims. Consumer platforms, education, and support services should be also part of the coordination and cooperation structures.

7. Conclusions

Online fraud poses a systemic risk to individuals, markets, and democratic trust. Addressing it effectively requires an integrated policy response that combines prevention, enforcement, and victim support.

From a better regulation perspective, **victim-centred and trauma-informed approaches are not optional**; they are critical to policy effectiveness, coherence, and legitimacy. Victim Support Europe therefore calls on the European Commission to ensure that the Action Plan to Fight Online Fraud (as well as the upcoming EU Victims' Rights Strategy) fully integrates victims' rights, access to justice, and recovery as core components of its intervention logic.

VSE stands ready to contribute to implementation, monitoring, and evaluation, ensuring that EU action delivers tangible benefits for people affected by online fraud across the Union. VSE plays a **bridging role** between frontline service providers, policymakers, and EU institutions. We have supported EU-wide standards on victims' rights, advocated for trauma-informed justice systems, and trained authorities to understand victims' complex needs.

If we want to improve **evidence quality**, especially in digital contexts, we must **protect first and prosecute second**. Support and protection are essential. Without legal and psychosocial support, they are unlikely to come forward. Studies across Europe show that **trauma-informed, comprehensive support increases victim cooperation and the quality of evidence**.

At VSE, we say: *"Protection is not an incentive for cooperation; it is a prerequisite for it."* Evidence follows trust. Trust follows safety. Safety begins with unconditional, trauma-informed support.

Where referral pathways work, law enforcement is trauma-informed, and services are accessible regardless of status or nationality, cooperation rises. Without these measures, victims may remain silent — and justice cannot be achieved. **Investing in victims' protection is investing in justice.** Only by

ensuring safety, dignity, and long-term support can victims like Sofia participate meaningfully, help bring criminals to account, and rebuild their lives.

Annex I

Good practices

- Hackshield, an educational programme aimed at preventing cybercrime for children,
- EMPACT (European Multidisciplinary Platform Against Criminal Threats) security initiative

Annex II

Proposed Action Plan Measure	Relevant EU Legal / Policy Framework	Problem Addressed	Expected Outcome / Added Value	Implementation & Monitoring Considerations
Embed victim-centred and trauma-informed approaches across prevention, reporting, investigation and support	Victims' Rights Directive (2012/29/EU), and the revised one; Charter of Fundamental Rights; EU Strategy on Victims' Rights (2020–2025), and the new one to cover 2026-2030	Under-reporting; secondary victimisation; lack of trust in institutions	Increased reporting; improved victim cooperation; reduced long-term harm	Indicators on victim satisfaction, reporting rates, access to support; qualitative victim feedback
Guarantee early access to information, psychosocial support and referral services for online fraud victims	Victims' Rights Directive; European Pillar of Social Rights	Fragmented or delayed support; psychological harm	Faster recovery; reduced retraumatisation; improved system effectiveness	Monitoring of referral timelines; availability of services; accessibility standards
Develop streamlined, accessible, and victim-friendly reporting mechanisms with feedback loops	Victims' Rights Directive; Digital Europe Programme; Better Regulation principles	Complex reporting; lack of follow-up; disengagement	Higher reporting rates; better data quality; stronger enforcement	Track completion rates; user experience metrics; reporting-to-response time
Strengthen cross-sector cooperation between law enforcement, financial	Europol mandate; EU Cybersecurity Strategy	Fragmented responses; slow detection; cross-border barriers	Faster detection; improved asset tracing; deterrence	Data-sharing protocols; governance structures; evaluation of

Proposed Action Plan Measure	Relevant EU Legal / Policy Framework	Problem Addressed	Expected Outcome / Added Value	Implementation & Monitoring Considerations
institutions, platforms and victim support services				cooperation outcomes
Enhance EU-wide information sharing on emerging fraud typologies	Europol; ENISA; Digital Services Act	Rapidly evolving fraud techniques	Improved prevention; anticipatory responses	Regular risk assessments; early-warning indicators
Invest in inclusive digital literacy and self-protection programmes	DSA, EACEA frameworks	Countering lack of knowledge on how to spot signs and what to do in the crisis period	Better prevention	Early warning signs; campaigns; tip sheets

Annex III

About Victim Support Europe (VSE)

Victim Support Europe (VSE) is the leading European umbrella organisation which represents all victims of all crime, no matter who the victim is and what the crime is, representing 80 member organisations and providing support and information to more than 2 million people affected by crime every year in 35 countries. VSE actively engages and influences the development of European public and victims' policy to highlight the needs of victims and those affected by crime, as well as to strengthen victims' rights and support in the aftermath of a crime.