Is the EU taking the right approach to APP fraud?

Zach Meyers, Assistant Director, Centre for European Reform[1]

12 November 2024

1. Introduction

The EU law-making institutions are currently discussing updates to the EU's current payment laws. One of the issues they want to tackle is the growing number of payment scams in Europe.

The EU's existing payments laws have helped greatly in reducing simple forms of fraud, such as where a fraudster steals a consumer's card details. As a result, fraudsters have turned to more sophisticated scams, such as social engineering attacks. In these attacks, a fraudster may impersonate a consumer's bank – for example, to persuade them their account has been compromised and they need to move their funds to a 'safe' account. Or the fraudster might pretend to develop a romantic relationship with the consumer before asking for money. Because the consumer actively initiates the transaction, these are commonly called 'authorised push payment' or 'APP' scams.

European policy-makers' reforms must recognise that APP scams are complex, and typically involve a scammer using a variety of services – from social media, telecoms services, and banks – so that no one player has the full picture of the fraud taking place. Tackling APP fraud effectively therefore requires two things: educational programmes to help consumers act vigilantly and identify fraud; and trust and close collaboration between banks, telecoms companies, online platforms and authorities.

The Commission[2] and Parliament's proposals include new rules that force banks to reimburse consumers affected by APP fraud. Parliament's proposal goes much further, however, with strict rules to share liability between banks, telecoms companies[3] and online platforms.[4] Parliament's approach would encourage firms to focus on shifting liability for fraud between them. That is unlikely to be a helpful approach to fight fraud for four reasons:

a) Banks, telecoms companies and online platforms **already have strong incentives** to keep users safe. These players also have **extensive regulatory commitments** requiring them to take action against fraud.
b) Measures that focus on shifting liability for APP fraud **undermine trust and co-operation**.
c) Liability rules would contribute to a **complex and incoherent legal framework**.
d) **Measures focused on liability undermine educational programmes**, because they encourage users to be less vigilant, and **create a 'honeypot' effect** encouraging even more fraud.

[1] The author acknowledges the financial support of the Computer & Communications Industry Association (CCIA Europe). The views expressed here have been independently reached, are solely the author's, and should not be taken to represent the views of CCIA or its members.

[2] Proposal for a regulation on payment services (PSR), 28 June 2023, COM(2023) 367, arts 83 and 84. These steps include requiring banks to improve fraud monitoring; share data among themselves about fraud; and educate and alert customers about fraud risks.

[3] PSR art 59(5).

[4] European Parliament legislative resolution on the PSR, 23 April 2024, recitals 79-82a, arts 2(9a) and 59.

Policy-makers could take more effective steps to tackle the problem. These include addressing where existing EU law prevents firms from co-operating, and helping promote voluntary cross-sectoral initiatives to stop fraud.

2. **Platforms have both incentives and existing obligations to tackle fraud**

A key characteristic of APP fraud is that it tends to span across different services and platforms, and no one player has full visibility of the fraudster's conduct and their interactions between the fraudster and their target. Take a romance scam: the fraudster might make contact with their target over social media, a dating app, or another legitimate website; move their communications onto email, instant messaging apps, or a traditional telephone call; and then the person affected will send money over a payment network. Criminals involved in this activity can quickly change their strategies, use of different platforms, and modi operandi to avoid detection.

In tackling fraud effectively, the right starting question is to ensure each type of firm has the right incentives – or is under regulatory obligations – to co-operate with other players in the fight against fraud.

Banks, telecoms firms and online platforms already have strong incentives and undertake action to ensure their services are safe, so that consumers continue to use them and businesses are comfortable advertising on them. This is illustrated from the extent of firms' unilateral efforts: Amazon, for example, invested USD 1.2bn in 2024 to protect users from fraud and counterfeits,[5] Meta removed over 19 million examples of spam from Facebook in the EU in the 6 months ending 31 March 2024;[6] and Google removed nearly 14 million examples of spam or fraud from its search engine results over the same period.[7] Even more importantly, all these types of firms are already working together on a voluntary basis to eliminate fraud – both firms of the same type and different types of platforms. These include, for example:

- The Tech Against Scams coalition,[8] which includes both tech and financial services firms and aims to protect and educate users about scams, and share knowledge and best practices.
- The Global Signal Exchange, a platform for sharing real-time insights into online scams by consolidating different data sources together supported by Google and the Global Anti-Scam Alliance. Google also offers Cross-Account Protection, which means it shares information about suspicious activity with third-party apps and services connected to a consumer's Google Account, and a Global Priority Flagger Program, where Google prioritises reports of fraud from nearly participating scams and fraud partners around the world.
- Scam Signal API – a tool offered by Vodafone to help banks identify impersonation fraud, and block scam payments, in real-time.[9]

Beyond voluntary actions, EU law already imposes significant obligations on banks, telecoms firms and platforms in tackling APP fraud. For example:

[5] Amazon, DSA EU Store Transparency Report, 24 October 2024.
[6] Facebook, DSA Transparency Report, 26 April 2024 (updated 13 June 2024).
[7] Google, Biannual VLOSE/VLOP Transparency Report, 26 April 2024.
[8] CoinBase, 'Announcing the Tech Against Scams Coalition', 21 May 2024.
[9] Vodafone, 'Vodafone Business launches scam signal to defend against impersonation fraud', 22 April 2024.

- Banks are already obliged to report on incidents of fraud,[10] and to check that the account name matches what the payer has provided (called 'confirmation of payee') when executing a euro-dominated instant payment. The proposed PSR will also require banks to undertake further reporting; adopt fraud monitoring systems; share information on bank accounts suspected of being used to commit fraud; and educate and alert their customers on fraud risks.[11]

- Online platforms are already subject to the EU's Digital Services Act (DSA).[12] The DSA requires these platforms to promptly remove illegal material once they become aware of it, for example when they are informed by law enforcement.[13] It requires platforms to have mechanisms for users to easily report illegal content, online marketplaces to make best efforts to verify a trader's identity; and users to see who any advertisement is presented for and who paid for it.[14] The largest platforms are also under obligations to identify and mitigate systemic risks stemming from their platforms.[15]

- Both banks and telecoms firms are subject to the NIS2 Directive,[16] a cybersecurity law which requires them to take steps like assessing security risks, implementing cybersecurity policies and appropriately managing cybersecurity incidents.

3. **Imposing liability shifts undermines trust and co-operation**

   Given that no one player in the ecosystem has a full view of fraud, two tools are essential to solving the problem. The first is educational programs to help consumers spot when they are being scammed, and which are proven to make a big difference.[17] The second is closer co-operation and information-sharing across the ecosystem, such as sharing of data, intelligence and best practices within and across the industries which are abused by scammers. This is reflected in the views of Euro Retail Payments Board (ERPB) working group on fraud, whose recent report recommends that "initiatives need to mobilize all relevant actors from the local, national and EU level in a collaborative way".[18]

   Proposals to make different firms across the ecosystem liable for covering the costs of reimbursing consumers would, however, seem likely to undermine trust and co-operation and instead create a culture of blame-shifting:

   - Banks would have incentives to 'over-report' fraud to online platforms without undertaking proper enquiries themselves, since this will maximise their chance of passing on liability to a telecoms firm or online platform.

   - Telecoms firms' and online platforms' would have fewer reasons to co-operate with banks by sharing information and intelligence about emerging threats – since banks could use that

[10] Directive 2015/2366 (Payment Services Directive) (PSD2) art 96(6).
[11] PSR arts 83 and 84.
[12] Regulation 2022/2065 (Digital Services Act) (DSA).
[13] DSA art 9.
[14] DSA arts 16, 30 and 26.
[15] DSA arts 34 and 35.
[16] Directive 2022/2555 (NIS2).
[17] Jeremy Burke et al, 'Can educational interventions reduce susceptibility to financial fraud?', Journal of Economic Behaviour & Organization, Vol 198, June 2022.
[18] ECB, 'Report of the ERPB Working Group on fraud related to retail payments', September 2024.

information to shift more liability to the telecom firms and online platforms who co-operate with them.

- Telecoms firms and online platforms would likely respond by reallocating resources towards assessing the (potentially large) influx of reports from banks who want to reduce their own liability, rather than focusing on proactive co-operation and on preventative steps which could have greater overall impact on stopping fraud in the first place.

4. **Liability rules would create an incoherent legal framework**

This game of liability 'hot potato' would also raise new contradictions and unresolved tensions with other EU policy objectives. In relation to telecoms firms, for example, the European Electronic Communications Code (EECC) and ePrivacy Directive (EPD) both oblige telecoms firms to protect confidentiality, manage security risks, and in particular protect encryption.[19] The ePrivacy Directive and the Net Neutrality Regulation[20] also limit the ability of telecoms firms to monitor and block calls and messages. Expectations about how telecoms firms can investigate and take action against fraud must take these existing policy priorities into account.

Online platforms, too, would be subject to competing policy objectives if new liability rules were to be introduced. In adopting the DSA, for example, EU policy-makers engaged in difficult discussions about how to ensure online platforms protect their users while preserving the benefits of digital ecosystems, innovation, and freedom of expression. As a result, the DSA reaffirmed that online platforms are not generally liable for users who abuse their platforms, and platforms should not be forced into general monitoring of content on their platforms, or mandatory removal of lawful content.[21] Parliament's proposal is hard to reconcile with the DSA, since it does not refer to the DSA's set of detailed safeguards for the removal of content.[22]

Liability rules would therefore contribute to existing concerns that the EU's regulatory framework risks becoming incoherent, with policy-makers refusing to acknowledge the tensions between different policy priorities, and putting unrealistic expectations on firms to manage inconsistencies between different EU laws. In turn, that creates a confusing and uncertain environment for consumers, for example where platforms are forced to take different approaches to different types of illegal content.

5. **Mandatory liability rules would undermine educational programmes and create a 'honeypot' effect**

Giving those affected by fraud a guarantee that they will be compensated will have perverse effects and creates a 'moral hazard'. It would encourage users to be less cautious and prudent, which would counteract initiatives to increase consumer awareness and vigilance about fraud. Worse, it would increase incentives to participate in fraud. Guaranteed reimbursement gives fraudsters incentives to pose as 'victims' in order to collect compensation – which can be as simple as falsely claiming that a product has not been delivered. In preparing the Instant Payments Regulation, for example, the Commission accepted that "more lenient refund

[19] Directive 2018/1972 (European Electronic Communications Code) (EECC) art 40; Directive 2002/58/EC (ePrivacy Directive) (EPD).
[20] Regulation 2015/2120 (Net Neutrality Directive).
[21] DSA art 8.
[22] For example, DSA art 9 provides that when a public authority orders a platform to remove illegal content, the order must contain clear reasons why the information is illegal and a URL setting out precisely where the content is located.

conditions may give rise to greater moral hazard in the form of unfounded refund claims (e.g. where the payer changed their mind, did not like the product, etc.)".[23] It also provides more incentives for consumers to allow their account to be used (wittingly or unwittingly) as a 'mule account' for fraudsters. A recent survey carried out by the UK's leading fraud prevention service illustrated that 20% of UK adults thought agreeing to act as a 'money mule' could be reasonable, and that the proportion of adults who admit to committing fraud – often at a small scale and with a view that it is a 'victimless crime' – has increased in the years since the UK introduced compulsory reimbursement.[24]

In countries where compulsory reimbursement of consumers have been introduced, banks have had to expend considerable resources identifying and weeding out 'first party fraud', or cases where fraudsters have posed as 'victims'. Compounding this moral hazard, banks spread the costs of reimbursing those affected to all their customers, which results in a redistribution from responsible and cautious consumers to more reckless ones.

This explains why – as Table 1 shows – very few jurisdictions require banks to automatically reimburse victims of fraud. The UK is the only jurisdiction which currently requires mandatory reimbursement of APP fraud by banks. This study has not identified any countries which impose reimbursement liability on telecoms firms or platforms for APP fraud.

Table 1. Which countries impose mandatory reimbursement obligations for APP fraud?

	Banks	**Telecoms firms**	**Online platforms**
Japan	☒	☒	☒
Korea	☒	☒	☒
Hong Kong	☒	☒	☒
Singapore	☒[25]	☒	☒
Netherlands	☒ But voluntary scheme for bank impersonation scams	☒	☒
Australia	☒ Under consideration	☒	☒
UK	☑	☒	☒[26]
Commission proposal	☑	☒[27]	☒
MEPs' proposal	☑	☑	☑

When certain countries such as the UK and the Netherlands have encouraged banks to do more to reimburse consumers impacted by APP fraud, they have tried to impose safeguards to avoid

[23] European Commission Staff Working Document, Impact assessment for the Instant Payments Regulation proposal, SWD(2022) 546.

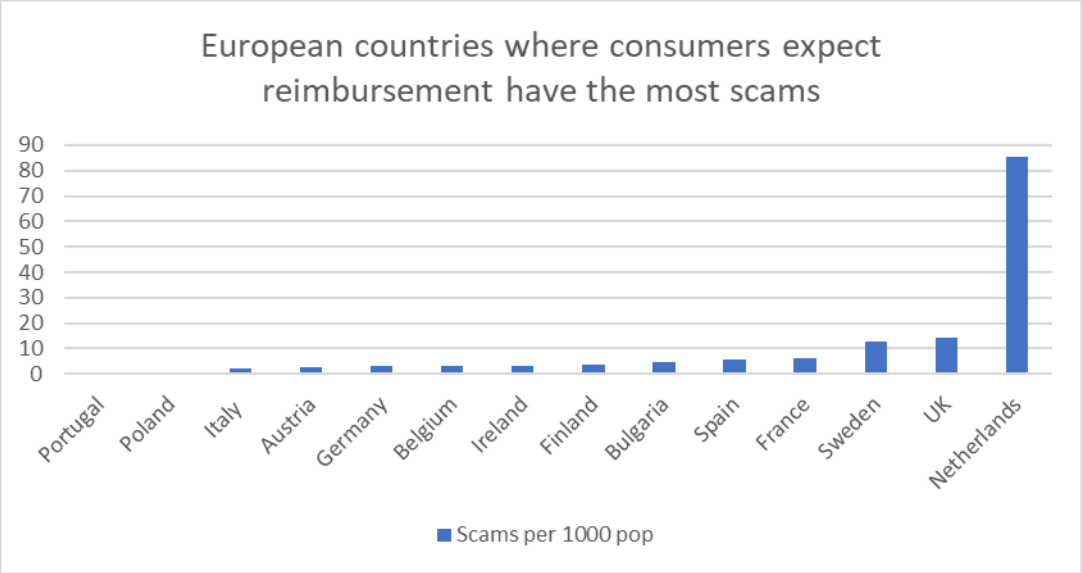
[24] CIFAS, '1 in 8 UK adults admit to committing fraud in the last 12 months', press release, 29 November 2023.

[25] Singapore is about to introduce mandatory reimbursement but only for unauthorised scams, not APP scams. In some cases telecoms firms may have liability, but only where telecoms firms breach specific enumerated duties. See Infocomm Media Development Authority, 'MAS and IMDA announce implementation of Shared Responsibility Framework from 16 December 2024', 24 October 2024.

[26] However, it has been reported that the government is considering imposing liability on online platforms: Tom Bleach, 'Financial Leaders Back Labour Plan to Force Tech Firms to Share APP Fraud Reimbursement Burden', Fintech Times, 3 July 2024.

[27] Specifically, the Commission's proposal does not introduce a new right of action, so recovery would be limited to where it is provided for under national law.

this 'honeypot' effect. However, these safeguards have been largely ineffective – as the below chart shows, with UK and the Netherlands having more scams than all other European countries where data was available.[28]



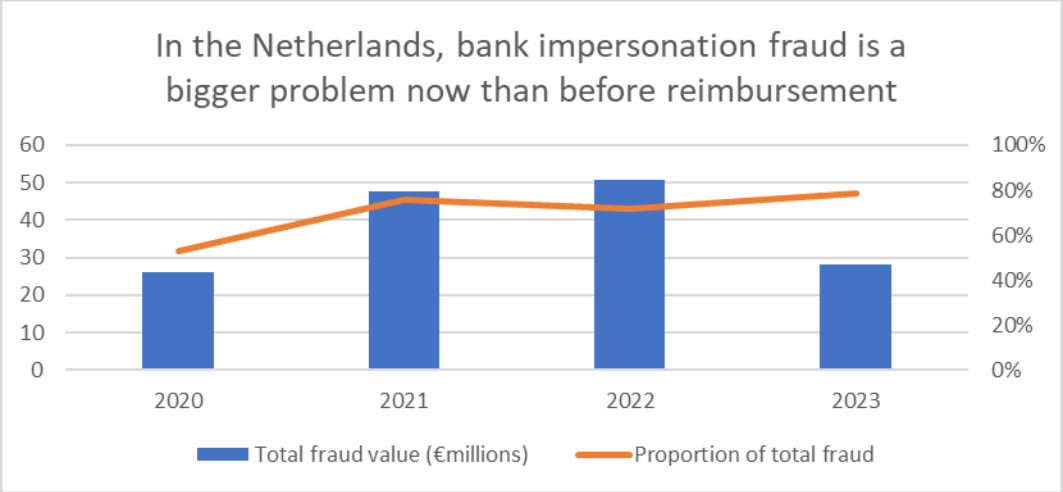
Take the Netherlands, where a voluntary reimbursement scheme for bank impersonation fraud was adopted by the country's four largest banks at the end of 2020. This is limited to bank impersonation, reflecting that banks have some degree of control over whether they are impersonated: they can explain to consumers how they will contact and communicate with them, for example, so the consumer can more easily spot an impersonation attempt. Furthermore, reimbursement in the Netherlands is not automatic and banks look at the specific facts and circumstances.[29]

Despite these safeguards and limitations, the 'honeypot effect' was pronounced. Over 2020 to 2021, the first year of widespread fraud reimbursement, losses from bank impersonation fraud nearly doubled from €26.2m to €47.6m, and bank impersonation fraud increased from 53% to over 75% of total fraud.[30] Even more noteworthy, the fraud problem seems correlated to the amount of reimbursement. In 2021, when fraud was the highest, 92% of bank impersonation fraud cases resulted in reimbursement. In 2023, a year in which total fraud dropped significantly, the four major Dutch banks only refunded 69% of losses from bank impersonation.

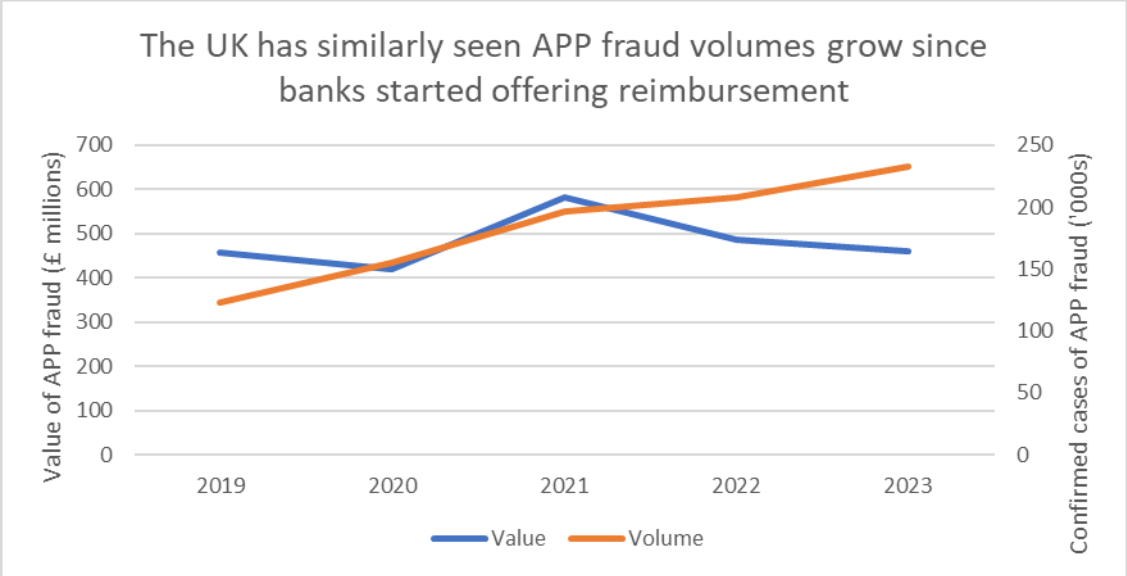
[28] Global Anti-Scam Alliance, 'The Global State of Scams Report', 2022.

[29] Nederlandse Vereniging van Banken, 'Toetsingscriteria voor coulance bij bankhelpdesk fraude (spoofing)', 4 June 2021.

[30] Nederlandse Vereniging van Banken, 'Online-oplichters richten zich steeds meer op de klant', 8 April 2022.



The UK provides a further example. Banks agreed to voluntarily reimburse consumers in 2019 and followed up with a mandatory approach (not yet in effect). However, since 2019 the volume of APP fraud in the UK has increased dramatically, and the total value of APP fraud remains higher than before the voluntary scheme was introduced despite the UK introducing a number of other significant anti-fraud measures, like educational campaigns and a confirmation of payee scheme, in recent years. This again illustrates that reimbursement of consumers is not a silver bullet and is likely counterproductive. The UK's mandatory approach has been coupled with new conditions which may help avoid a potential 'honeypot' effect – for example, compensation is generally subject to an 'excess' of up to £100 and there is a cap on the total amount of reimbursement to protect financial stability. However, it is yet to be seen whether these conditions will avoid creating more incentives for fraudsters.



An explicit desire to try to avoid the 'honeypot' effect explains Australia's proposed approach in its draft 'Scams Prevention Framework'. In Australia, those impacted by APP scams would have to seek recourse from an Ombudsman, without a default presumption of reimbursement.[31] Whether this model will be sufficient to avoid a 'honeypot' effect remains to be seen.

[31] Australian Treasury, 'Scams Prevention Framework – exposure draft legislation', 13 September 2024.

In comparison to countries which have focused on reimbursing consumers, others have achieved greater success through measures like educating consumers. For example, in Ireland the total losses suffered from APP fraud were the lowest in 2022 of any year since data on APP fraud began being recorded, with a reduction of 19% in 2022 compared to 2021.[32] One reason might be the proactive approach taken by banks in that country. For example, the Banking & Payments Federation Ireland launched FraudSMART, a highly regarded fraud awareness initiative. The Irish central bank has applauded the banking sector for being "proactive in informing consumers of these risks [and] the practical steps consumers can take to protect themselves."[33] Cross-sector co-operation plays a big role too, with telecoms operators and banks engaged in a joint project which has blocked about 10 million spam calls since September 2022.[34] The Irish banking federation has explained the much lower fraud rates in Ireland result from "the UK [becoming] a destination for fraudsters because it is known to be refunding".[35]

6. **What should European policy-makers do?**

Step 1: address existing constraints on voluntary co-operation on fraud

Given that players in the ecosystem already have good incentives to tackle APP fraud, policy-makers should firstly identify and address where existing EU laws prevents firms from collaborating to tackle APP fraud. Examples of issues might include the following:

- Enable cross-sector data sharing: Sharing information may require sharing personal data. National data protection authorities do not all have a coherent position on when and how the EU's General Data Protection Regulation allows sharing data for fraud prevention purposes.[36] The Commission proposes to specifically allow sharing of 'personal identifiers' between banks, but does not envisage more data sharing with telecoms firms and platforms.

- Ensure firms can use data for fraud analytics purposes: Europe's Digital Markets Act (DMA) imposes constraints on how some large platforms can combine different datasets, even if the purpose of doing so is to better detect fraud.[37]

- Ensuring telecoms firms can adopt 'anti-spoofing' solutions: the EU's ePrivacy Directive and Net Neutrality Directive limit the ability of telecoms firms to monitor and block calls and messages. To address this, in some countries the ePrivacy Directive was implemented with specific allowances, for example to allow telecoms firms to take "measures […] to prevent preparation of means of payment fraud".[38]

- Enable banks to delay execution of suspicious payments: EU law currently imposes strict time limits by which payments must be executed.[39] Fraudsters take advantage: the European Banking Authority (EBA) has observed that fraud for instant payments is about ten times

[32] FraudSMART, 'Payment Fraud Report: H2 2022'.

[33] Central Bank of Ireland, 'Consumer Protection Outlook Report 2023', March 2023, p 10.

[34] Niamh Davenport, evidence given to Houses of the Oireachtas, Joint Committee on Finance, Public Expenditure and Reform, and Taoiseach debate, 24 May 2023.

[35] Ibid.

[36] For example, GDPR recital 47 states that 'processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned', but the interests of the data subject still need to be taken into account. See also discussion in ECB, n 12 above.

[37] DMA art 5(2).

[38] See ECB, n 12 above.

[39] PSD2 art 83.

higher than for conventional credit transfers.[40] In exceptional cases, banks could have more time to investigate and share intelligence with other players in the ecosystem – an approach the UK is adopting and the EBA has suggested.[41]

Step 2: ensure existing regulatory tools are being used effectively, including to drive more voluntary co-operation

There is widespread concern – among businesses,[42] think-tanks,[43] and political leaders[44] – that the EU is no longer adopting basic principles of better regulation. A basic premise of better regulation is that policy-makers should assess whether existing regulatory instruments are working effectively before pushing ahead with new interventions. The concept of 'evaluate first' has been embedded in the EU's better regulation agenda since the early 2010s.[45]

Many anti-fraud measures have not had time to be fully effective so that they can be properly evaluated. While 'confirmation of payee' already applies to instant payments in euros, it will not be mandatory for all credit transfers in the single European payment area until October 2025. The rules in the DSA only began applying to most online platforms from February 2024. And most EU member-states have not yet transposed the NIS2 into national law despite the deadline of 17 October 2024 to do so.[46] So policy-makers cannot yet determine whether these laws have been effective or whether there are still gaps which need addressing. Imposing new laws before existing ones have been bedded in risks creating duplicative and incoherent obligations: a problem which already characterises the EU's digital regulatory landscape.[47]

A better alternative to imposing new interventions would be to ensure that the tools in these regulations have been fully implemented. The DSA provides a good model here, because it allows the Commission to encourage the creation of voluntary codes of conduct to tackle systemic risks.[48] The DSA points specifically to how codes could help address "the use of bots or fake accounts for the creation of intentionally inaccurate or misleading information, sometimes with a purpose of obtaining economic gain".[49] This type of self-regulation is likely to be the best model of regulation for tackling APP fraud: fraudsters' techniques change and adapt, so prescriptive laws will be unlikely to permanently address the problem.

Any code would need to foster co-operation with banks and telecoms firms, and encourage each of them to each take steps (such as set out in Table 2 below) which help mitigate APP fraud,

[40] European Banking Authority (EBA), 'EBA Opinion on new types of payment fraud and possible mitigants', EBA-Op/2024/01, 29 April 2024, p 5.
[41] UK Treasury, 'New powers for banks to combat fraudsters', press release, 3 October 2024; see also EBA, above n 29.
[42] BusinessEurope, 'Better regulation in the new EU legislature', position paper, 17 July 2024.
[43] Zach Meyers, 'Better regulation in Europe: An action plan for the next Commission', Centre for European Reform, policy brief, March 2024.
[44] Mario Draghi, 'The future of European competitiveness', September 2024; Ursula von der Leyen, 'Europe's Choice: Political guidelines for the next European Commission 2024-2029', 18 July 2024.
[45] European Commission, 'Strengthening the foundations of Smart Regulation – improving evaluation', COM(2013) 686, 2 October 2013.
[46] Visiola Pula, 'EU countries late in transposing new EU cybersecurity rules (NIS2)', Cullen International, 18 October 2024.
[47] Zach Meyers, 'Helping Europe's digital economy take off: An agenda for the next Commission', Centre for European Reform, policy brief, 20 February 2024.
[48] DSA art 45.
[49] DSA recital 104.

without creating an environment dominated by blame-shifting. Indeed, the DSA itself encourages this, stating that "*Nothing in this Regulation prevents other service providers from adhering to the same standards of due diligence … by participating in the same codes of conduct*."[50]

Table 2. Examples of how services exploited by fraudsters can help combat APP fraud

Sending banks	Receiving banks	Telecoms firms	Platforms
● Monitor to identify unusual transactions by the sender ● Confirmation of payee schemes ● Provide education and tools for consumers to help spot scams ● Include warnings and tools to identify and report scams in online banking websites/apps ● Participate in mechanisms to share information across industry about confirmed APP fraud ● Share information / intelligence across the ecosystem	● Conduct due diligence when onboarding new customers ● Confirmation of payee schemes ● Monitor customers to identify suspicious transaction behaviour ● Freeze suspicious payment accounts ● Participate in mechanisms to share information across industry about confirmed APP fraud ● Share information / intelligence across the ecosystem	● Conduct KYC checks when accepting new customers ● Prevent inappropriate use of phone numbers, such as imitating numbers organisations only use for incoming calls (known as a 'Do Not Originate' list) ● Take steps to identify and block SMS scams[51] ● Verify legitimacy of calls and messages routed through their networks, such as through a Sender ID Register, as adopted in the UK ● Monitor suspicious use of services ● Share information / intelligence across the ecosystem	● Due diligence of new customers to prevent creation of fraudulent accounts/content including account verification ● Educate consumers to spot scams ● Allow customers to easily report fraudulent content and devote resources to reviewing reports promptly ● Take steps to avoid fraudulent advertising – e.g. conducting KYC on new advertisers, and requiring financial advertisers to be authorised ● Share information / intelligence across the ecosystem ● Guide users towards more secure payment options

<u>Step 3: ensure regulatory coherence</u>

If policy-makers eventually come to the conclusion that new interventions are required, to ensure consistency with the already-complex regulatory environment, obligations should be technology-neutral, risk-based, and outcomes-focused. They should give firms flexibility to achieve outcomes. This will be essential to effectively tackle fraud, given that fraudsters' techniques continue to change and adapt – so a single static set of techniques to identify and stop fraud will never suffice – and given that regulated businesses need to take into account competing policy objectives in the regulatory framework. For example, the EBA has suggested banks could be required to adopt an overarching "fraud risk management framework".[52] This would reflect the collaborative approach with existing laws as a basis. Such existing frameworks give banks, telecoms firms and online platforms the flexibility to trial different methods of

[50] DSA recital 103.

[51] Anti-spam filters helped UK firm EE block more than 285 million scam SMSs, leading to an 85% drop in customer scam reports: EE, 'How EE is leading the fight against scams', 12 February 2024.

[52] See EBA, above n 29.

identifying and addressing fraud, and enable them to prioritise measures that prove the most effective at deterring fraudsters from engaging in such activities in the first place.

7. **Conclusion and recommendations**

Given its complex nature and the fact that APP fraud typically involves a variety of different communications and payments channels, mitigating the problem will require co-operation and co-ordination from public authorities, law enforcement, consumer groups, banks and other payments firms, telecoms companies, online platforms, and others.

Banks, telecoms operators and online platforms have good incentives to co-operate. Changing liability rules risks undermining these incentives – while giving a strong inducement to fraudsters. Compulsory reimbursement of impacted consumers has had little impact on APP fraud (as the UK and the Netherlands showed) – and it may well have made the situation worse. Policy-makers should instead:

- Acknowledge that players in the ecosystem already have incentives to co-operate – and focus on interventions that remove legal barriers to closer co-operation and build trust.
- Carefully assess how existing tools are working, and ensure existing laws are fully implemented, before imposing complex new interventions.
- Ensure any new obligations are consistent with other EU laws and public policy objectives. An outcomes-focused and risk-based approach would be more consistent with the already-complex regulatory frameworks in which banks, telecoms operators and online platforms operate. This would enable firms to prioritise the measures which prove most effective at stopping fraud for their particular businesses.