Europe Economics

Scam calls and texts in Ireland – costs and benefits of interventions

16 June 2023

Document Reference: 23/52a

Europe Economics
4th Floor
5 Chancery Lane
London
EC4A 1BL

Tel: (0) 20 3862 9252

www.europe-economics.com

Contents

1 Executive Summary

Scam calls and texts are a scourge on society and mislead victims into thinking they are receiving calls or texts from legitimate organisations or people, so as to illegally obtain sensitive information such as bank details with the view to committing fraud. Scammers are inventive and opportunistic and use a range of approaches to obtain information, often attempting to masquerade as well-known organisations (such as banks, delivery companies and public bodies) by 'spoofing' Irish telephone numbers (call line identifiers, or CLIs) or SMS sender IDs.

Europe Economics was commissioned by ComReg to undertake an analysis of the harm caused by these nuisance communications in Ireland, and the costs and benefits of potential interventions to address this. This study assesses the harms caused by scam communications to consumers, businesses, public organisations and wider society in Ireland. It undertakes a comprehensive quantification of such harm – the first of its kind in a European country and certainly in Ireland – using empirical data and a detailed modelling approach.

We conservatively estimate that the overall harm caused by nuisance communications in Ireland amounts **to approximately €310 million per year,** which includes around **365,000 cases** of fraudulent scam communications over the last 12 months. These communications also incur a strong emotional toll with around 31 million distressing calls received last year. In light of the substantial harm, this report then considers a range of interventions to tackle voice and SMS scams and assesses the costs and effectiveness of each. In summary, the net benefits of the package of measures proposed in this report amount **to around €1.6 billion over a seven year period**.[1]

Given the opportunistic nature of scammers, they are likely to concentrate their efforts in countries where the defences against scams are (relatively) low. There is thus a risk that if Ireland takes no action in this area, it will increasingly become a target if other countries' defences improve. As an English-speaking nation, Irish residents are already targeted disproportionately compared to their EU counterparts, receiving fraudulent phone calls or emails asking for personal details 10 per cent more often than the EU28 average in 2016-19. Currently the majority of scam calls and texts targeting Ireland originate abroad, but scams originating within Ireland e.g. via pre-paid phones are growing.

We drew on a range of sources in carrying out our analysis:

- A review of the literature and evidence on the theory of harm from nuisance communications and examples of the nature and scale of scams in Ireland and internationally.

[1] Net benefits of a similar order of magnitude were found with a smaller number of telecommunications operators bearing the costs of the interventions. See section 7.1.5 for a more detailed discussion on our sensitivity analysis.

- Interviews with a range of public bodies and private companies impacted by nuisance communications, with An Garda Síochána and the Central Statistics Office and with telecommunication operators.
- Representative consumer and business surveys carried out by Behaviour and Attitudes (B&A) to gather data on the prevalence and impact of scam calls and texts, including a willingness-to-pay element.
- A detailed estimation of the harm from scam calls and texts to Irish consumers, businesses and public bodies
- A detailed cost-benefit modelling exercise of potential interventions that ComReg may use to combat scam calls and texts.

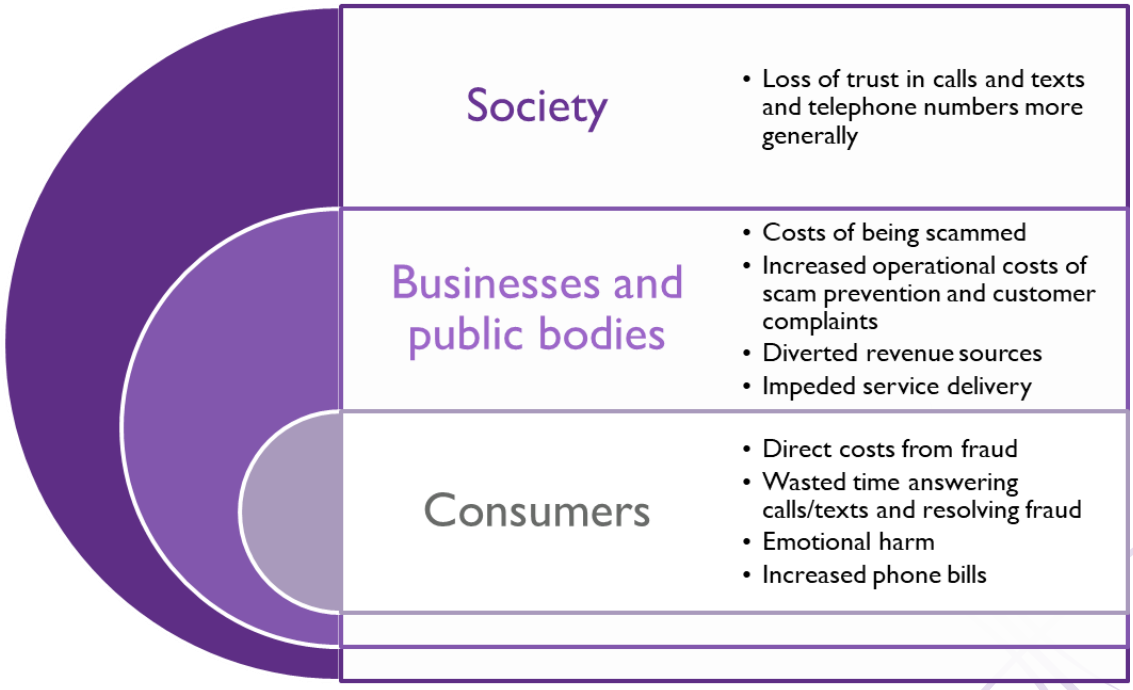
1.1 The problem of scam communications

The B&A consumer survey shows that the prevalence of scam communications in Ireland is high. Over **90 per cent of adults** received a scam call on their mobile in the last year (74 per cent on their landline) and **84 per cent of adults received some form of scam text.** The most commonly impersonated organisations were banks and courier/postal companies, followed by public organisations such as HSE and Revenue which is particularly egregious given that every citizen has a relationship with the State.

Prevalence among businesses in Ireland shows a similar pattern. Around **77 per cent of businesses** either received a scam call or text in the last year, with scam calls being more likely than scam texts (68 per cent indicated that they had received scam calls and 56 per cent a scam text). Whilst most firms in our sample were not aware of having been impersonated in a scam, **almost one third of the largest firms** (with 250+ employees) reported having been impersonated in some way.

Scam communications cause a host of harms to individuals, businesses and public organisations, and wider society, as summarised below.

Figure 1.1: Harms from scam calls and texts



Source: Europe Economics

1.1.1 Our approach to quantifying harm

This report represents the first attempt to estimate the total harms from scam communications in Ireland, and is one of the most thorough approaches of its kind in the international literature that we reviewed. We adopted three approaches to quantifying harm:

- Bottom-up cost modelling ("BUCM"), which used data derived from our consumer and business surveys and estimated tangible costs.
- Willingness-to-pay ("WTP") analysis was used to capture intangible harms from scam calls and texts. We obtained two broad estimates: an overall, forward-looking WTP capturing a fuller range of harms including the annoyance or distress recipients might feel, or fears about potential losses from fraud; and a backwards looking WTP capturing just the emotional and time cost element actually incurred.
- Illustrative case studies to provide examples of aspects of harm that were not captured in the above two tools due to their bespoke nature, in particular for businesses and public bodies. Given the great variety across organisations in Ireland it is not possible to fully extrapolate these examples, and thus the estimates provide just a partial view of the harm.

1.1.2 Harm to consumers

We estimate that there were around **365,000 cases** of fraudulent scam communications in Ireland over the last 12 months, with the financial harm ranging from small to relatively large amounts. We estimate that **175,000 people were defrauded** after receiving scam calls and lost an average of €494, while **190,000** people lost an average of €231 after receiving scam texts.

Figure 1.2: Summary of financial loss from fraud based on consumer survey results

No. of people who lost money	Highest losses	Average loss
• Calls: 175,000 • Texts: 190,000	• Calls: €5k+ • Texts: €3k-€5k	• Calls: €494 • Texts: €231

Source: Europe Economics

Scam calls caused the larger share of the total with around €75m in direct financial losses over the year (accounting for some loss recovery). Scam texts caused €35m in annual losses net of recovery. The total net financial loss from fraud caused by scam calls and texts is therefore estimated to be just under €109m in the last year.

In addition to the direct financial losses from fraud, consumers incur other costs from time spent resolving scams, time spent engaging with the calls and texts, and emotional distress and annoyance. The table below summarises all the quantified consumer harms.

Table 1.1: Summary of quantified harms to consumers

	Harm	Estimate	Approach	How included in total
A	Financial loss from fraud	€109m	Bottom-up cost modelling	Direct harm from fraud.
B	Cost of time engaging with scam calls	€40m	Bottom-up cost modelling	Indirect harm (wasted time) from scams, only relating to scam calls.
C	Cost of time resolving scams	€1m	Bottom-up cost modelling	Indirect harm (wasted time) from fraud.
D	Wasted time and emotional harm	€22m	Backward looking WTP (those receiving scam texts in past year, not victims of scam)	Indirect harm from scam SMS with no fraud (actual – assumed wasted time and emotional harm). No overlap with BUCM.
Aggregated harm (A + B + C + D)		€172m		

Source: Europe Economics analysis. Values may not add due to rounding

Scam calls and texts gave rise to **89m annoying/irritating communications** and **31m distressing communications** in the past year.

In addition to emotional harm, scam calls and texts have also eroded citizens' trust in calls and texts more generally which should be of great concern to telecommunications service providers and wider Irish society. Using our willingness to pay approach, we find **a far larger estimate for harm to consumers of €400m**. This indicates that a significant amount of harm was not directly measured in our quantification exercise described in the table above, including intangible factors such as the loss of trust in Voice/SMS experienced as a result of scam calls and texts. **The value of the trust lost by Irish consumers could therefore be as high as €230 million per annum.**[2] Many organisations – public and private – rely specifically on these communications for providing their services. This can involve information/reminders about health appointments, banking and utility bills. Our survey shows that around **65 per cent of adults that use any of these services have lost trust in these communications and pay less or no attention to them**.

1.1.3 Harm to businesses and public bodies

Businesses also suffered direct financial losses from scams in the past year, as well as the opportunity costs of time spent resolving fraud and answering scam calls and texts more generally. However, the biggest costs were related to increased operational costs from responding to consumer queries about the legitimacy of their communications, rearranging services (e.g. deliveries) and communications, and implementing measures to mitigate against scams (e.g. staff training or new software).

Some businesses will also face costs specific to their industry. For example, our consumer survey showed that consumers are sometimes able to recover some of the losses they incur after being a victim of fraud. Assuming that this is recovered from organisations (e.g. banks) rather than from the scammer this implies that there was nearly €21m in refund costs to businesses in the past year.

[2] After subtracting the quantified harm. This would represent a large fraction of the value of such services to consumers as shown by the retail revenues for such services. This appears reasonable given that trust underpins the benefits of such services – after all, a call or SMS has no utility if it goes unanswered or unread. Widespread disuse would represent a material loss of consumer welfare.

Figure 1.3: Summary of quantified harms to businesses

Source: Europe Economics analysis. Values may not add due to rounding

In addition to these costs, businesses may also have lost revenue as a result of consumers not accessing usual channels of communication. Firms that use voice and text communications as part of their revenue generating strategies link **revenue of approximately €48bn to these services**, and scam communications puts this at great risk.

Telecoms operators, whilst potentially benefitting from revenues from scam communications, would also be harmed through a general loss of trust in telephone numbers among consumers and businesses if this led to declining calls and texts.

Public bodies incur a range of harms from scam communications, predominantly increased operating costs from scam prevention strategies and wider impacts from service disruptions through not being able to communicate effectively with service users.

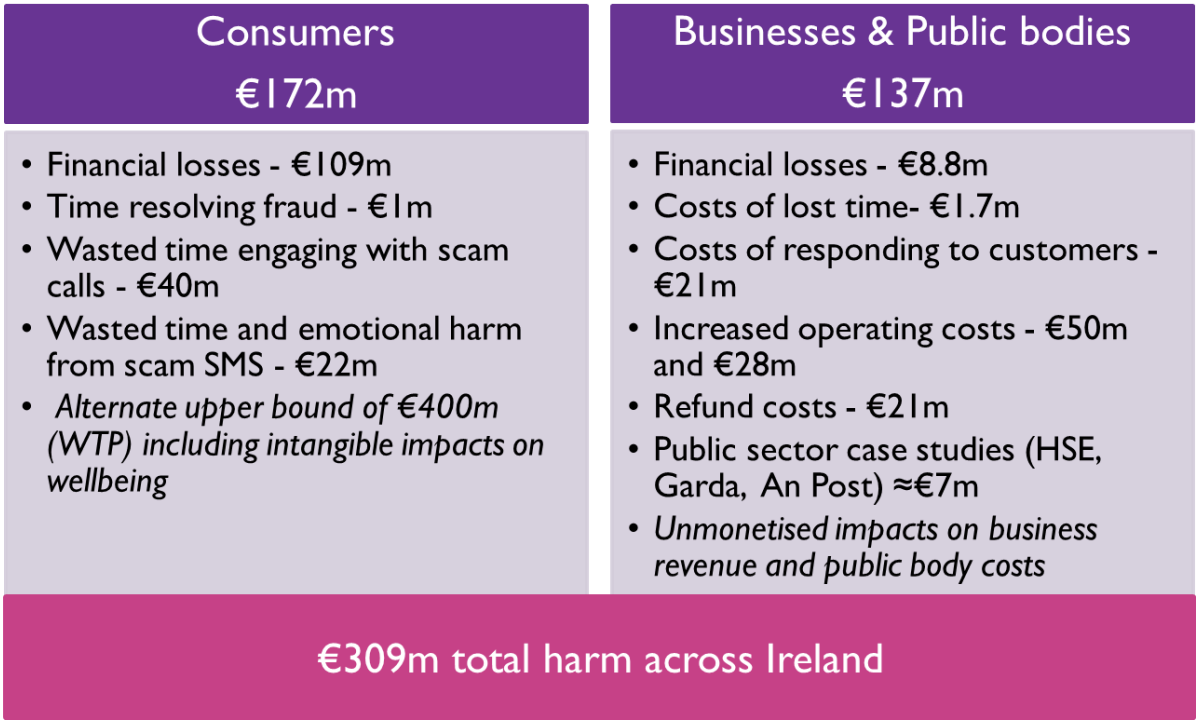
Estimating country-wide harms to public bodies was not feasible for this study as such organisations experience many different and often unique harms. There are also limited data available on harms to public bodies.

However, we conducted a number of case studies to illustrate the types of harm that could be incurred. These limited quantified examples **alone totalled €7m** and indicate a far greater level of unquantifiable harm is being borne by these and other public agencies at present. These estimates are our own partial estimates of harm, informed by our discussions with the organisations listed rather than provided by them.

1.1.4 Summary of harm

The total quantifiable harm to Irish society for one year is **conservatively estimated at €309m**. This excludes a range of costs to public bodies, revenue impacts on businesses and many intangible harms to consumers as demonstrated by our WTP analysis.

Figure 1.4: Summary of harm from scam communications in one year



Source: Europe Economics analysis. Values may not add due to rounding

Without any action to tackle scam communications, there is no reason to believe that harm would fall, given the opportunistic nature of scammers and their ability to take advantage of new events or changes in phone users' behaviour. If other jurisdictions (particularly English-speaking) continue to implement interventions of their own, Ireland will become even more susceptible to scam calls and texts as inevitably scammers would direct more scams towards unprotected Irish consumers.

1.2 Interventions

We assessed a range of voice and SMS interventions designed to tackle various aspects of scam calls and texts. These have been suggested to us by ComReg based on its work with operators in the Nuisance Communications Industry Taskforce (NCIT).

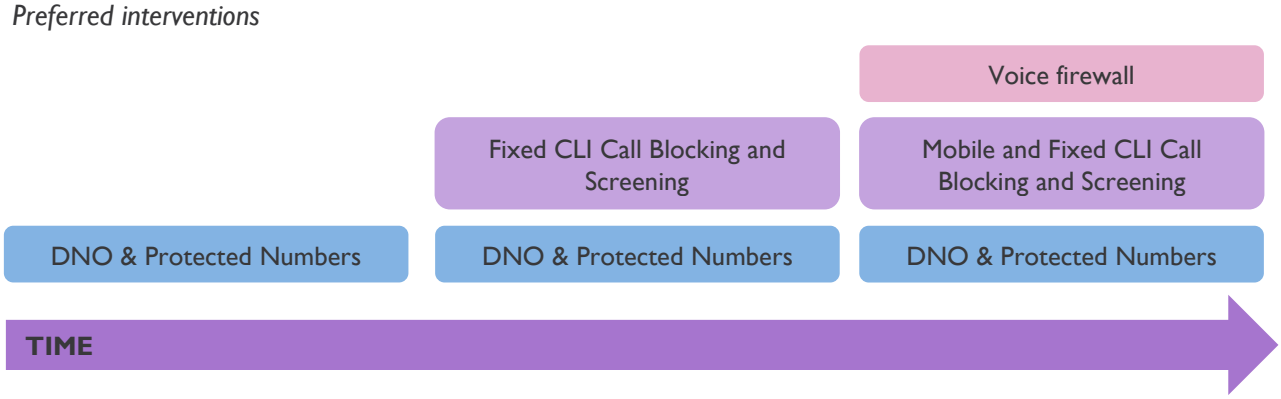
1.2.1 Voice interventions

- A **Do Not Originate (DNO)** list refers to phone numbers which are never used for outgoing calls. For example, certain banks provide numbers for consumers to contact them, but they never contact a consumer using the same number. Consequently, any calls received on these numbers are spoofed and therefore should be automatically blocked.
- A **Protected Numbers (PN)** list refers to phone numbers that have not been assigned by ComReg to any operator or business and so any calls that present them are spoofed and should therefore be blocked.

- **Mobile CLI blocking** would identify and block nuisance calls stemming from international networks which present with Irish mobile caller IDs. These calls attempt to deceive customers into thinking a call is coming from someone in Ireland on their mobile.
- **Fixed CLI blocking** operates in the same way as mobile CLI blocking but blocks nuisance calls that are spoofing Geographic Numbers (e.g., 01, 061) and/or the non-geographic numbers that businesses use (e.g., 0818).
- A **Voice Firewall**, which can be updated in real time to account for scammers' ever adapting strategies to reach consumers (e.g., exploiting newly discovered vulnerability in networks and changes to consumer behaviour). A Voice Firewall acts in the same way as any firewall by deciding which calls are allowed to pass through and which calls are likely to be from fraudsters. Voice firewalls are designed with advanced real time call data analytics using machine learning and artificial intelligent techniques to detect and act upon unusual patterns of call signalling data and traffic volumes.

We modelled the costs and benefits of these interventions in isolation, and also under a scenario where they are implemented cumulatively from the least to the most complex, as illustrated.

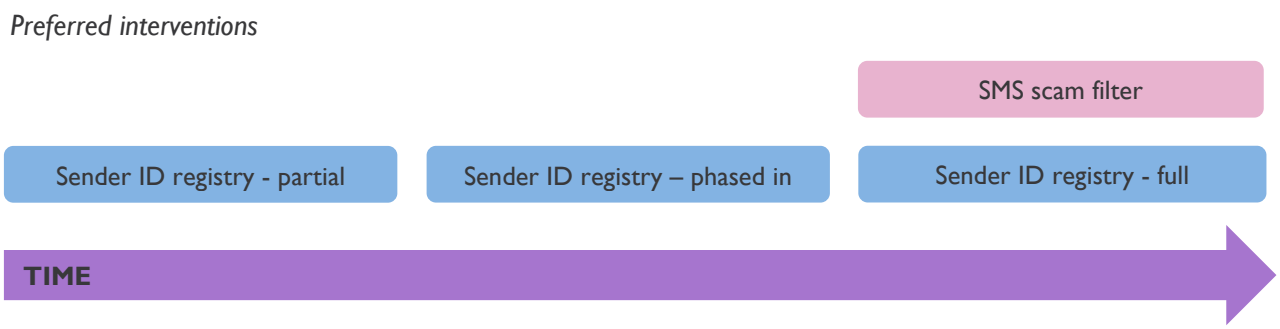
Figure 1.5: Options for interventions to tackle scam calls



1.2.2 SMS interventions

- ComReg will establish a **Sender ID Registry** which will allow businesses to register their Sender ID and operators would block any message bearing a sender ID from any source other than the registry. In this way, scammers would be unable to pose as legitimate businesses by contacting consumers using Sender IDs. We assess three versions of this – a partial registry with only the largest organisations' Sender IDs; a full registry covering all businesses; and a phased-in full registry that starts with a partial registry and migrates to a full registry over time.
- An **SMS scam filter** would operate similarly to the spam filter on email by detecting and blocking harmful links that encourages users to click on the link and then enter personal information, that is used in turn to commit fraud using that consumer's details. Similar to the voice firewall, this measure is dynamic and adjusts to evolving scams. It is also increasingly being rolled out in other English-speaking jurisdictions, which provides scammers greater incentive to target SMS communications in Ireland.

Figure 1.6: Options for interventions to tackle scam texts



Source: Europe Economics

1.3 Costs benefit analysis of the interventions

We estimated the costs of each intervention based on information received from operators, ComReg and vendors. Benefits were modelled as the extent to which each intervention is assumed to reduce the volume of scam calls or texts, and thus harm. Evidence on the likely effectiveness of each intervention was gathered from a number of sources including operators, vendors, NRAs as well as publicly available information. Costs and benefits were modelled over a seven-year period, and discounted to the present value. We analysed the costs and benefits of each intervention in isolation, and the incremental benefits if the interventions were introduced cumulatively, as is proposed by ComReg.

Notably, the incremental net benefit of each intervention depends on the effectiveness of the preceding interventions in blocking a volume of scam calls and texts (e.g., when applied one after the other). We forecast our estimate of the level of harm in 2022 (based on the B&A surveys) and its profile (based on internal operator data) into the future, and estimate the reduction harm that results from implementing the interventions.

The extent to which individual interventions are effective depends on how scammers adapt to the interventions and create workarounds so as to continue to send scam calls and texts. We model two scenarios:

(i) where scammers adapt minimally to the interventions (e.g., would keep using CLI spoofing even though such calls would now be blocked); and

(ii) where the scammers fully adapt (i.e., use other methods to contact consumers and never use CLI spoofing).

It is difficult to accurately estimate how quickly and to what extent scammers will react because this depends on the individual scammer and their capacity to adapt – however, the overall benefit will fall somewhere between the two scenarios. In reality, scammers will use a mix of methods, and while scammers are likely to adapt to ComReg's static interventions, this will require time and it cannot be ruled out that they may reinitiate old scams in the future. We estimate that the overall net benefits of the package of interventions (regardless of how scammers adapt) will range between **€1.4 and €1.6 billion** over seven years. This corresponds to **a benefit of €53 for every €1 spent** on the interventions.

The voice firewall and SMS scam filters are important and provide net benefits of €142m and €197m even where scammers only minimally adapt to the static interventions, because they offer protection that cannot be provided by the static interventions (e.g., against scams originating in Ireland). However, they become increasingly more important the more scammers adapt to ComReg's static interventions, rising to **€881m and €514m respectively in an extreme scenario where scammers fully adapt** (i.e. where the

benefits of the static interventions are zero). The key CBA results are summarised in Table 1.2, with more detailed figures provided in Chapter 6.

Table 1.2: Costs and net benefits of interventions to tackle nuisance communications

Intervention	Cost (€m)	Net Benefit	
		Scammers adapt minimally to static interventions	Scammers fully adapt to static interventions
Voice interventions			
Static interventions (DNO,PN, Fixed & Mobile CLI Blocking)	€8m	€896m	-8m
Voice firewall	€10.2m	€142m	€881m
SMS Interventions			
Static: SMS registry – Full (phased-in)	€6.4m	€366m	-6.4m
SMS scam filter	€6.2m	€197m	€514m
Combined			
Total	**€31m**	**€1.6bn**	**€1.4bn**

Source: Europe Economics analysis. Values may not add due to rounding. Note that the reported costs in the table are present value figures over the 7-year implementation horizon.

Our key finding is that **all potential interventions are cost-beneficial at our assumed levels of effectiveness**. That is to say that the benefit of each intervention far outweighs its costs.

Were scammers to adapt fully to static interventions the voice firewall would have the most significant impact of all the voice interventions, with a net present benefit of €881m over the period. This is driven predominantly by the fact that the Voice firewall is assumed to cause a 90 per cent reduction in all scam calls. Similarly, the SMS scam filter would be the most effective intervention for SMS scams if implemented in isolation as it is assumed to capture a greater share of scam texts than the registry options, with a net present benefit of €514m over the seven years.

A further important feature of the Voice Firewall and the SMS scam filter is that these are unlikely to lose their effectiveness over time, as they are based on machine learning and designed to adapt to changes in scammers' techniques in a way that the other interventions may not. Therefore, the incremental net benefits of the two firewalls would be even larger if extended beyond the seven year intervention period.

1.3.1 The distribution of costs and benefits

The costs of the interventions would largely be incurred by operators and SMS aggregators, as well as ComReg, in the first instance, as these would be responsible for implementing the technical solutions.

The interventions would benefit all of Irish society – consumers, businesses and public bodies – by reducing the harms resulting from scam calls and texts (estimated at **€309m in a year**). The benefits may be greater than estimated due to the conservative nature of our harms estimate.

In particular, benefits from reducing a loss of trust in telephone numbers could be material and would benefit all stakeholders including operators. To illustrate, 65 per cent of our survey respondents indicated that regulatory intervention to tackle scam communications would increase the trust they have in calls and texts.

1.4 Recommendations

Given the substantial harm caused to society by nuisance communications, it is clear that regulatory intervention would have benefits. Based on the costs and benefits estimated, it is evident that all the interventions are beneficial and each part of the package of interventions is required. We note however that the estimated benefits are conservative as they do not capture the full range of harms and the variety of harms experienced by public organisations, as well as the intangible harm from a society-wide loss of trust in telephone numbers.

Given the scale of harm incurred each and every year and the likelihood of this increasing – or at the very least remaining steady – in the absence of any intervention, we recommend that interventions are implemented as soon as possible, starting with those that can be implemented soonest and incorporating the more complex ones in time.

- **To combat scams texts**, we recommend implementing SMS ID Registry and SMS scam filter. The cumulative net benefits are greatest for the combination of the sender ID registry and the SMS scam filter. The SMS scam filter brings large benefits relative to its costs no matter the scenario used. Implementing the SMS ID registry absent the SMS scam filter risks undermining the SMS ID registry, were scammers to switch to scams that do not involve SMS ID spoofing. This is clearly already necessary, given the large share of recent scams that do not use SMS ID spoofing.
- **To combat scam calls**, we recommend implementing DNO/PN, Mobile and Fixed CLI Blocking and Voice Firewall. This would bring the greatest reduction in scam calls, no matter how scammers react. The three fixed interventions (DNO/PN and Fixed CLI blocking) should be implemented as these tackle slightly different types of scam call, and have low implementation costs. The Mobile CLI block is needed to address scams that spoof mobile CLIs and also brings large benefits relative to its cost. The Voice firewall brings large benefits relative to its costs no matter the scenario used. Implementing the static measures absent the Voice Firewall risks undermining the static measures, were scammers to switch to scams that do not involve CLI spoofing.

2 Introduction

Scam calls and texts have become an increasing problem in Ireland in recent years, in particular those that spoof local Irish fixed and mobile numbers or well-known SMS sender IDs in an attempt to obtain personal information from recipients and conduct fraud. In addition to fraud, a host of other harms arise from scam communications such as wasted time, emotional distress, and a loss of trust in calls and texts.

ComReg has worked, in collaboration with the telecommunications industry in Ireland, to develop a number of technical interventions to tackle scam communications. This derived from an industry taskforce ComReg founded, the Nuisance Communications Industry Taskforce ("NCIT"), which initially lead on agreeing and developing interventions to address scam calls and texts (the "NCIT Interventions").[3] ComReg has also developed a number of additional interventions, informed by other regulators (e.g., Singapore, Finland).

This report presents Europe Economics' analysis of harm caused by scam communications in Ireland, and the costs and benefits of interventions to address this. To identify the best interventions for Irish society, we have assessed the economic and social impact of these interventions on Irish consumers, businesses, public bodies and operators.

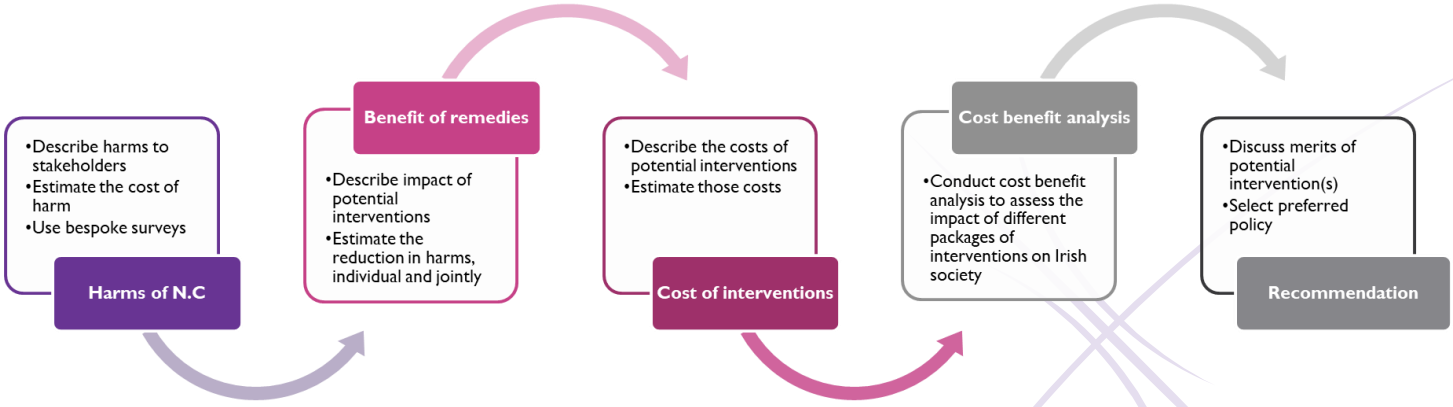
2.1.1 Overview of our work

This study assesses the harms caused by scam communications to consumers, businesses, public organisations and wider society in Ireland. It undertakes a comprehensive quantification of such harm – the first of its kind in Ireland – using empirical data and a detailed modelling approach.

We then assess a range of interventions to tackle voice and SMS scams, as informed by ComReg and the NCIT, estimating the costs and effectiveness of each. The benefits of the interventions are estimated using existing evidence and assumptions on their effectiveness in reducing the volume of scam calls and texts. We estimate the one-off and on-going cost of the interventions for operators individually and in aggregate.

Finally we compare the benefits and costs of different the interventions, for a range of potential packages. This analysis informs our recommendations as to which interventions ComReg should implement in order to maximise the welfare of Irish society. The figure below illustrates our approach.

Figure 2.1: Overview of our approach



[3] Our analysis in the report has been informed in part by outputs from this taskforce on its considerations of the technical aspects of the interventions.

2.1.2 Methodology

We gathered a wide array of evidence to inform our analysis, including:

- A review of the literature and evidence on the theory of harm from scam communications and examples of the nature and scale of scams in Ireland and internationally.
- A representative survey of over 1,200 Irish consumers to gather data on the prevalence and impact of scam calls and texts and their effect on Irish consumers.
- A representative survey of over 800 Irish businesses to gather data on the impact of scam calls and texts and their effect on business.
- Interviews with a range of public bodies to understand the impact of scams on their ability to provide critical services.
- Interviews with An Garda Siochana to understand their experience in combating scams and the evolution of scams over time.
- Interviews with Ireland's Central Statistics Office to understand the availability of data on scams.
- Interviews with operators to understand the costs of interventions.
- Information from NRAs, vendors and from public services on the effectiveness of interventions.

2.1.3 Structure of the report

This report is structured over the following chapters:

- Chapter 3 assesses the theories of harm relating to scam communications and presents evidence on the scale and nature of harm in internationally.
- Chapter 4 estimates the prevalence of scam calls and texts in Ireland and the associated harm to consumers, businesses and public bodies.
- Chapter 5 describes the interventions proposed by ComReg and the NCIT to tackle scam communications.
- Chapter 6 estimates the costs and benefits of the interventions over time.
- Chapter 7 provides our conclusions and recommendations .
- Chapter 8 and 9 contain details of our harms and cost-benefit model (Appendix 1 and 2).

3 Background to Scam Calls and Texts

This chapter outlines the most prevalent forms of scam calls and texts found in Ireland and describes the full range of harms associated with them. It describes the theory of harm and focuses largely on evidence from other jurisdictions to contextualise the problem. The harms are considered separately across five stakeholder groups: consumers, businesses, public bodies and regulators and operators. In Chapter 4, we then turn to our estimates of harm for Ireland which is evidenced through our desk-based research and our primary research through the consumer and business surveys and stakeholder interviews.

3.1 Scam calls and texts

Over recent years, nuisance communications in the form of scam calls and texts have become an increasing problem internationally and in Ireland. As an English-speaking nation, Irish residents are currently targeted disproportionately compared with their EU counterparts, receiving fraudulent phone calls or emails asking for personal details 10 per cent more often than the EU28 average in 2016-19.[4] In early 2022, the Gardaí reported a 370 per cent increase from 2020 to 2021 in communications that impersonate legitimate organisations to defraud their victims (a category that included scam emails).[5]

While data on the prevalence and harm from scam calls and texts in Ireland is limited, it is clear that there has been a sudden increase in the prevalence of scam calls and texts in Ireland in recent years. We establish this fact with our consumer and business surveys (presented in Chapter 4). Nevertheless, some industry-specific research highlights the extent of the problem in Ireland, as shown in the box below.

[4] European Union (2019). 'Europeans' attitudes towards cyber security (cybercrime)' – [online] - Note that the survey results are from October 2019.

[5] An Garda Síochána (2022) 'An Garda Síochána Vishing, Smishing and Phishing Fraud Alert – 04 February 2022'. [online].

Box 1: Evidence on the prevalence of scam calls and texts in Ireland

Research carried out in August 2022 for the Bank of Ireland found that 74 and 43 per cent of surveyed adults had received scam texts and calls, respectively, that appeared to be from their bank – increases of 37 per cent and 25 per cent on 2021 figures, respectively.[6]

FraudSMART (2021) reported that 72 per cent of its survey respondents were approached by fraudsters through scam calls, with 32 per cent via text message.[7] Around 83 per cent of respondents to this survey thought that impersonation scams were more prevalent in 2021 than in 2020, with 68 per cent saying they were a lot more prevalent.[8]

A survey conducted by AIB in 2021 found that 80 per cent of people aged between 18-34 in Ireland have been targeted by financial scams within the past 12 months, having received either a text, call or email they believed to be fraudulent. Those over 55 were more likely to be targeted by fraudsters, with 85 per cent in this age group receiving some form of fraudulent communication.[9] As part of the same AIB report, evidence from a survey conducted by Amárach found that 33 per cent of people received fraudulent communication from a bank or financial institution they were not a customer of; 30 per cent received a fraudulent communication claiming to be a technology company; and 22 per cent of people have received a fraudulent text message claiming to be from the Revenue Commissioners.[10]

The direct financial implications for victims of scam calls and texts can be substantial. However, the harms extend beyond this. An impersonation scam targeting an individual can have consequences for the organisation that it impersonates, potentially causing the individual to disengage from that organisation's legitimate communications. The integrity of and public trust in communication networks is threatened if people cannot trust the calls and texts they receive from others. Importantly, harm may be caused even when a scam attempt is unsuccessful.

This study focuses on scam calls and texts, as described below.

3.1.1 Scam calls

The most prominent types of scam calls involve **CLI (call line identification) spoofing**, whereby criminals impersonate – or 'spoof' – Irish CLIs (such as their numbers) to make fraudulent calls to Ireland. The fixed CLIs of trusted Irish organisations such as banks and public bodies are often the targets of such spoofing to mislead victims into thinking they are receiving genuine calls from these organisations. Mobile CLIs can also be spoofed whereby fraudsters impersonate mobile CLIs that may be more familiar or recognisable to the call receiver. Spoofed CLI calls mainly originate outside of Ireland, and thus the impersonation of an Irish CLI masks the international origin of the call. However, there is growing evidence of scams originating in Ireland, particularly through the use of pre-pay burner phones.

Given the effectiveness of CLI spoofing in deceiving victims, it has been a common tool used by fraudsters to perpetuate illegal calls. Nuisance communications that have used CLI spoofing have been reported where fraudsters have attempted to impersonate Irish organisations such as the Department of Social Protection, Revenue, the Gardaí.[11,12] CLI spoofing can take specific forms in the following types of illegal call: Vishing, Wangiri calls and Illegal Robocalls.

6 Leonard, R. (2022) 'Hack the human – the psychology of cyber fraud, Professor Mary Aiken', *Irish tech News* [online]
7 FraudSMART (2021) 'FraudSMART Monitor', p.4 [online]
8 FraudSMART (2021) 'FraudSMART Monitor', p.5 [online]
9 AIB (2021). 'Four out of five people have been targeted by Fraudsters in the last year', p.1 [online]
10 AIB (2021). 'Four out of five people have been targeted by Fraudsters in the last year', p.1 [online]
11 McNeice, S. (2021) 'Scam phone calls: How and why scammers are 'bombarding' the Irish public', *Newstalk* [online].
12 FraudSMART (2021) 'FraudSMART Monitor', p.4 [online]

Box 2: A CLI-spoofed call

FraudSMART reported an incident where a victim named Carmel received a call on her landline from an individual purporting to be from the head office of her bank. She was instructed that she required a temporary 'safeguard solution' on her account. Not knowing this was a fraudulent call, Carmel provided all of her personal and banking details. The fraudsters then asked her to go to the bank and withdraw her savings. She was then guided to go to a post office to wire the money into a safe account. She was further instructed that if she was asked as to why she was withdrawing the money at the bank, she was to say it was for a relative's wedding. In order to convince Carmel that the process was legitimate, the scammers guaranteed that once the account had been safeguarded, the money would be returned to her account.

Suspicious of the whole process, Carmel informed the bank clerk at her bank that she had been approached by the banks 'head office'. The bank clerk informed her that the bank would never approach customers in this way and that other customers had been targeted by similar scams. Had Carmel withdrawn and sent the funds, she would not have been able to recover them as she had taken the money out herself and consciously authorised the transaction.

Source: FraudSMART, 'Telephone scam' [online]

Voice phishing[13], or 'Vishing'

Vishing is a form of scam call that uses CLI spoofing to specifically elicit personal information from victims by purporting to be from reputable organisations. A key component of vishing is that it relies on convincing victims they are doing the right thing by responding to the caller.

Vishing communications have grown over the past year, with the media outlets reporting increased complaints received by the Gardaí.[14] Cloud security specialist Lookout has calculated that 2022 had the highest percentage of mobile phishing encounter rates ever — with over 30% of personal and enterprise users exposed to these attacks every quarter.[15]

Box 3: Examples of vishing scams

One victim was a 25 year-old woman in Dublin who received a scam call from a fraudster purporting to be from a government department. The person was instructed that a car rented using her personal details had been found to be involved in committing criminal offenses. It was reported that the woman was held on the call for hours, where she was instructed to make a €5,000 cash deposit into a cryptocurrency machine. Later after the call and making the payment, the person realised she had been defrauded.

Another victim received a scam call from a fraudster purporting to be from An Garda Síochána. Not knowing it was a fraudulent call, the person provided the caller with his Personal Public Service (PPS) before becoming suspicious and ending the call. The person went to his local police station to report this crime, where he was told that the scam attempt may have been in relation to the fraudulent claiming of the Pandemic Unemployment Payment (PUP), which had been rampant across the country at the time.

Source: Foy, K. (2021). 'Gardaí swamped with complaints over new 'vishing' scam as one woman loses €5,000.' [online] Irish Independent.

Wangiri calls

Wangiri calls are a form of CLI spoofing where fraudsters allow the call receiver's phone to ring briefly and then stop. Spoofing the CLI, either fixed or mobile, can encourage the call receiver to return the call that appears as missed, thinking that it is somebody or some organisation they can trust. In doing so, the call may be diverted to a premium-rate or international number for which the victim incurs a direct cost.

[13] 'Phishing' refers to the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

[14] Foy, K. (2021). 'Gardaí swamped with complaints over new 'vishing' scam as one woman loses €5,000.' [online] Irish Independent.

[15] Global State of Mobile Phishing Report, published on March 1, 2023.

Although less frequently used, Wangiri calls have become more prevalent in Ireland over recent years.[16] The Irish Independent (2017) reported that there had been an "unprecedented "surge in Wangiri calls in Ireland in the tens of thousands in late 2017, with operators highlighting that the genuine-looking nature of Wangiri calls due to their use of Irish prefixes made them difficult to identify, which resulted in people placing return calls and being charged premium rates.[17]

Box 4: Examples of Wangiri calls

In 2017, a wave of calls from Comoros was reported by several people in Ireland. Some recipients let the phone ring and completely ignored these calls, but others reported answering the call to nobody on the other end. It was suggested that the caller's silence provided an 'incentive' for the recipient to return the call, for which they would be charged higher rates as they are calling an international number. This followed another wave of Wangiri calls in which people received missed calls from the Seychelles, Tonga, Mauritania and Chad.

In 2018, several New Zealanders reported that they were being targeted by "hang up calls". One individual was billed $88.88 extra for a 0900 call they made. After querying it with their provider, they was told it was a call to somebody in an overseas country. Several other individuals also reported that they were receiving unknown calls from all over the world, most commonly Algeria, Albania, Cuba, Tunisia, Korea, Taiwan and Philippines.

Source: Joe (2017) 'Today's 'Comoros' phone scam in Ireland is another reason not to answer or ring back unknown numbers' [online] and NZ Herald (2018). 'Herald readers share their wangiri call scam stories' [online]

Illegal Robocalls

Illegal Robocalls are where fraudsters use auto-diallers to generate a large volume of calls that share a pre-recorded message with an interactive voice response menu option when answered. If the receiver engages with the call and selects an option, they may be connected to the fraudster who can then initiate a scam. The CLI of an incoming illegal robocall may be spoofed to convince call-receivers that the call is from a trusted source.

Box 5: Examples of Robocalls

In 2021, a person reported receiving the same robocall from four different 083 numbers over the course of two days. These calls were claiming to inform the recipient of a warrant for their arrest on charges of drug trafficking and money laundering. This person blocked the calls, and many people were irritated by the apparently constant flow of such calls.

Source: Moore, P. (2021).

3.1.2 Scam texts

Scam texts are typically referred to as SMS spoofing (sometimes referred to as SMS phishing, or 'smishing') which is a broad form of illegal SMS message whereby fraudsters attempt to impersonate individuals, businesses or trusted organisations to encourage the message-receiver to engage with the message. This sort of scam can originate from at least three sources:[18]

- Messages arriving over 'grey' routes. Foreign networks send messages with alphanumeric sender IDs which may impersonate those of trusted organisations (recipients therefore receive scam texts from "An Post" or "BOI").
- Messages arriving from malware-infected Android devices. A mobile user receives a message that contains a link to a website hosting malware which can infect their device. This user's mobile becomes the

[16] For example – in 2017 Irish Independent reported 'Wangiri' phone scam sweeping across Ireland is 'unprecedented' say operators - https://www.independent.ie/business/technology/wangiri-phone-scam-sweeping-across-ireland-is-unprecedented-say-operators-36240323.html - Accessed 22 September 2021.

[17] Weckler, A. (2017). 'Wangiri' phone scam sweeping across Ireland is 'unprecedented' say operators. [online] Irish Independent.

[18] NCIT (2022), presentation on 2 February 2022.

springboard for a flurry of further messages which are sent to a list of recipients controlled by the scammer to repeat the cycle. Note that a law enforcement operation[19] announced in June 2022 executed a take-down of the command and control infrastructure for the most common malware, Flubot. While this appears to have reduced the numbers of malware-originated messages for the moment, the door remains open to future malware variants,

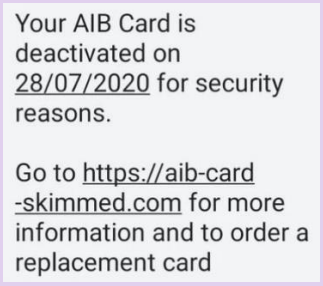
- In recent months, messages sent via specialist Sim Bank hardware, using disposable unregistered prepaid sims.

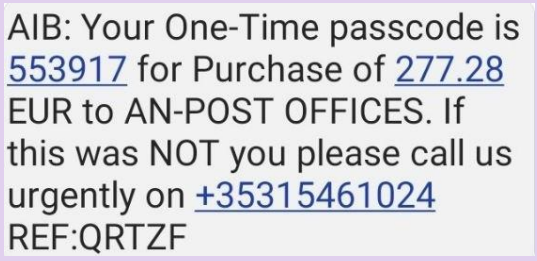
The prevalence of smishing has increased significantly in Ireland. In July 2022, Bank of Ireland stated that it had detected a 50 per cent increase in what it called a 'new wave' of scam texts over the past month.[20]

Both scam calls and texts attempt to convince their receivers that they are receiving a communication from a trusted source, thus potentially deceiving them to engage with the communication in ways that may harm them. The case presented below shows how scammers can use both scam texts and scam calls in unison to defraud people. The initial 'hook' was a scam text, and information was subsequently provided over a call.

Box 6: A smishing scam

In 2022, a person received a text that appeared to be from AIB (their bank). Given that the message had the same alphanumeric code and was in the chain of previous legitimate text messages they had received from AIB, the recipient did not question it. The pictures below are examples of some of the scam texts victims have received over the recent years purporting to be AIB:





Source: An Garda Síochána[21,22]

The scammers then called claiming that there had been suspicious activity on the account. Convinced that the text and call were legitimate, the recipient used the card reader to enter his pin and shared the confirmation code with the scammers. Days later, the recipient was contacted by actual staff at their bank alerting of suspicious activity on the account. Upon receiving this, the recipient was met with the realisation that most of their life savings had been withdrawn.

Source: De Brun, L. (2022). 'Irish man warns public after losing life savings through new 'expert' AIB scam'. *Extra* [online]

3.1.3 The opportunistic nature of scams

The type of scams and case studies highlighted above show that scammers use a range of different techniques. The persistence demonstrated by scammers in their attempts is likely driven by two key factors:

- Scammers ability to contact and con consumers.
- Scammers incentive to attempt scams.

Ability

[19] Europol (2022). 'Takedown of SMS-based FluBot spyware infecting Android phones'. – [online]
[20] Dunne, E . (2022) 'Don't be taken in by scam text factories, warns Bank of Ireland', *The Times* [online].
[21] An Garda Síochána (2020). [online]
[22] An Garda Síochána (2020). [online]

The ability to reach and successfully deceive consumers into doing something (e.g. making a payment) which may be increased by exploiting network weaknesses regarding the presentation of numbers (e.g. SMS, CLI spoofing).

Scammers have shown that they are opportunistic in responding to changes in this environment. Scammers often target specific events in the hope of increasing the number of successful scam attempts. This is referred to as the vulture effect. In order for the vulture effect to work to the benefit of scammers, it relies upon people being vulnerable to scams. They will often target people and areas that are in a state of heightened vulnerability. This could include periods following a large event of change or public uncertainty (e.g. COVID).

To reach consumers, scammers also target 'gaps' in networks or relatively less-defended networks, sometimes referred to as the weakest-link effect. As technical interventions are implemented, the less-protected countries become increasingly exposed as scammers switch their attempts to them, which may lead to a weakest-country effect . English-speaking nations are also often targeted, as scammers are able to scale-up their activities without different language barriers. In that regard, Ireland needs to be conscious of measures taken in other English speaking countries because scammers will increasingly target Ireland if measures are implemented in these countries (e.g., Australia, UK etc) but not in Ireland. Box 7 shows some of the events targeted by scammers in order to exploit an increased state of vulnerability.

Incentive

The scammer's attempts are driven by a calculation that expected profits from successful scams exceed the cost of the attempts (and the expected costs of sanctions). When this is not the case, scammers are known to switch and substitute between different scam attempts. This is important when determining regulatory measures because interventions that only target one type of scam or source of a scam will simply move the scam rather than reduce it (e.g., implementing effective voice interventions and ineffective SMS interventions will simply cause scammers to move more of their illegal activities through text messages). A package of interventions needs to consider that scammers can readily switch across scams and platforms.

If enough scam calls begin to fail, scammers face the incentive to switch to alternative techniques. And the range of alternative techniques can be minimised by limiting the ability of scammers to exploit vulnerabilities.

Box 7 : Cases of scammers exploiting specific events

Exit of KBC and Ulster Bank from Irish consumer banking market (2021/2022)
In 2021, KBC and Ulster Bank announced their plan to leave the Irish market. Exploiting this shift, scammers were reported to text many people claiming to warn of the impending cancelation of salaries, standing orders, or direct debits and utility payments.[23] By deceiving people into engaging with these texts, scammers hoped to retrieve personal details and bank account details from individuals.

COVID-19 pandemic (2020-2021)
As a result of the devastating effect of the COVID-19 pandemic on both global economies and social interaction, many individuals found themselves at greater vulnerability to scam attempts. A greater reliance was placed on electronic devices such as mobile phones to conduct daily activities.[24] [25] Scammers used this as an opportunity to prey on those already vulnerable to mobile phone scam attacks and those who may have not been as exposed before. In the UK, the reported scams included COVID-19 tax refund messages, businesses receiving false government grant

[23] Kevin Create (2022). Fraud warning as Ulster Bank and KBC Bank prepare to exit the Irish market. [online] FraudSMART.

[24] For example, Sebire (2020) reported in April 2020 that the Australia's National Broadband Network had found that daytime usage of internet had increased by 70 to 80 per cent, relative to February . Sebire K. The coronavirus lockdown is forcing us to view 'screen time' differently. That's a good thing. The Conversation; 2020 [online]

[25] A study in British Columbia Jonnatan et al (2022) found that there was an significant increase in device use during COVID-19, with this being more prominent amongst urban areas relative to rural . Jonnatan, L et al (2022). 'Mobile Device Usage before and during the COVID-19 Pandemic among Rural and Urban Adults.' International Journal of Environmental Research and Public Health, 19(14), p.8231. doi:10.3390/ijerph19148231.

calls and HM Revenue & Customs & Department for Work and Pensions impersonation scams asking for personal information and or bank details.[26]

COVID-19 relief strategy - Economic Impact Payments (2020-2021) (US)
As part of a COVID-19 recovery strategy, the Internal Revenue Service (IRS) in the USA issued three individual economic impact payments to those who were eligible.[27] Scammers were found to use text scams suggesting to individuals that they are eligible for a stimulus check. A link was usually attached which, when clicked, asked for personal information.[28] The IRS issued warnings to taxpayers in the USA about unsolicited calls attempting to defraud individuals for their money and personal details. This was also accompanied with guidance on what tell-tale signs taxpayers should look out for.[29]

Energy Bills Support Scheme (2022) (UK)
Amid the cost of living and energy crises faced by consumers in the UK, the UK government issued a £400 energy discount to households. Scammers have been reported to use this opportunity to send texts that prompt individuals to click on a link and sign up for the grant. Not knowing that the grant is credited to all household energy accounts, many have been misled into engaging with the link and providing personal information and/or bank account details.[30]

Nationwide internet outage (2022) (Canada)
In mid-2022, Rogers, one of Canada's largest mobile and internet providers, experienced a nationwide network outage that lasted more than 15 hours.[31] This affected services such as banking, transport, and emergency services. The emergency service hotline and bank ATMs were also made unavailable. Fraudsters used this opportunity to send smishing texts that impersonated Rogers and offered compensation if recipients clicked the link and engaged.[32] Individuals reported receiving text messages offering a $90 Rogers rebate.[33]

Optus security hack results in scams on Telstra (2022) (Australia)
Optus, Australia's second-largest telecommunication company, had a severe data breach in 2022 which resulted in approximately ten million users having personal data such as passport, driving license and address information exposed and stolen.[34] Scammers sent scam texts offering individuals new sim cards and service updates by engaging with a link.[35]

Given the similarity in the nature of scam calls and texts, we set out the different stakeholder groups in Ireland that may fall victim to either type, distinguishing only between 'scam calls' and 'scam texts' where necessary. Further, we distinguish between harms that are the result of being both directly targeted by a scam and indirectly as a result of a different stakeholder group being targeted. We discuss the different theories of harm that occur, providing both a qualitative and quantitative assessment of the harms in question.

[26] ActionFraud (2020). 'COVID-19 related scams - news and resources'. [online] Action Fraud.
[27] USA.gov (2022). 'Advance Child Tax Credit and Economic Impact Payments - Stimulus Checks'. USA Gov. [online]
[28] Aldridge, B. (2022). Stimulus check scams soared this summer, IRS warns. McClatchy DC. [online]
[29] Internal Revenue Service (2022). 'IRS continues with Dirty Dozen this week, urging taxpayers to continue watching out for pandemic-related scams including theft of benefits and bogus social media posts. Internal Revenue Service'. [online] www.irs.gov.
[30] Ramsey, T. (2022). Beware of this scam text offering you fake government energy bill support - Which? News. [online] Which?
[31] Cursino, M. (2022). 'Canada's internet outage caused by 'maintenance''. BBC News. [online]
[32] Nielsen, K. (2022). 'Police warn Ontario residents about Rogers outage phishing scam'. Globalnews.ca. [online] Global News.
[33] Jadah, T. (2022). 'Scam warning: Canadians receiving fake $90 Rogers rebate after outage'. Venture. [online] dailyhive.com.
[34] Turnbull, T. (2022). 'Optus: How a massive data breach has exposed Australia'. BBC News. [online]
[35] Optus (2022). Scams - Optus. [online]

3.2 Overview of the European context

Although scam texts and calls have been prevalent in Ireland over recent years, media reports indicate an increased wave of scams has also been experienced across other European countries. Therefore, European consumers and businesses are likely suffering harm from scam calls and texts also.

ComReg conducted a survey in December 2022 which asked for the views of other independent regulators in Europe on whether they had experienced an increase in 'nuisance communications' generally (which includes scam calls and texts but often different jurisdictions have different definitions). All but one responding regulators indicated that they had experienced an increase in nuisance communications.[36] Of those that said yes, it also investigated the types of nuisance communication experienced and the measures each regulator put in place to intervene. It appears that most regulators are in the process of identifying interventions, having not implemented few, if any, to date.

3.3 The harm caused by scam calls and texts

In the following sections, we describe the harm caused by scam calls and texts across different stakeholders (noting that actual estimates of harm are provided Chapter 4, namely consumers, businesses, public bodies and regulators, and telecoms operators . Harm can take different forms, covering:

- Direct harms such as
  - Direct losses from scams.
  - Other costs of dealing with scams, including emotional distress and opportunity costs (i.e., wasted time).
  - Costs of avoiding/preventing scams.
- Second-order impacts such as the loss of benefit to consumers from
  - a loss of trust in telephone numbers.
  - reduced use of and reliance upon SMS and Voice services.

We present the drivers of harm in each case, and provide evidence for such harm from the literature. In the next chapter we focus on the scale of the problem in Ireland.

3.4 Harms to consumers

Consumers can be caused harm, both as a result of being the target of a scam attempt (i.e., financial fraud) and as a consequence of others being targeted. The following is an overview of the different drivers of harm that impact consumers as a results of scam calls and texts.

3.4.1 Financial losses from fraud

Fraudsters may send scam calls and texts to present themselves as established Irish organisations to gain the trust of their victims. Some consumers may believe the call is genuine and proceed to engage with the fraudsters. They may then provide details that can be used to extract money or commit other types of fraud.

[36] Three NRAs indicated that they were not the competent authority overseeing communications in the member state, which means it is possible the relevant Member States had also experienced an increase. Only one NRA reported no increase in nuisance communications.

Whilst fraudsters are always on the look-out for somebody to lower their defences, they habitually adapt their approaches to exploit current developments and bolster their ability to convince victims of the veracity of their communications. Box 7 above describes a number of opportunistic scams that exploited events such as the withdrawal of certain banks from the Irish market, the COVID pandemic, and the impact of Brexit on An Post delivery or customs charges. Consumers engaging with these communications risk their financial information being exposed and potentially incurring a financial loss.

Many sources have reported on this form of harm, notably FraudSMART (2021, 2022) in Ireland, UK Finance (2022) and Ofcom (2015) in the UK, the FCC (2022) in the US and the Communications Fraud Control Association (CFCA) (2021) globally. There have been myriad articles in the press reporting anecdotal evidence of individuals losing large sums due to scam calls and texts. These estimates are all presented in the following subsection on the magnitude of harm.

Box 8: International evidence on financial losses

The financial loss from fraud is by far the most widely-reported harm in international literature. Based on a survey of fraud experts at communications service providers, the Communications Fraud Control Association (CFCA) in 2021 estimated a global loss of $2.63bn to fraud caused by to CLI and IP spoofing, $2.03bn to smishing and hacking, and $1bn to phishing/pharming (the fraudulent practice of directing users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information).[37,38]

Other estimates of losses caused by fraud are vague about the exact drivers of the fraud. Europol (2019) reports that the cost of telecommunications fraud is €29 billion per annum.[39] It is unclear what type of fraud is considered within this estimate, but the report behind this figure covers a range of fraud including telecommunications subscription fraud (exceeding $12 billion annually), vishing calls, wangiri calls and international revenue sharing fraud.[40] Furthermore, UK Finance reported that £26.3m was lost to card ID theft in the UK, mainly driven by 'data harvesting' in the form of phishing emails, scam texts and theft of mail from external mailboxes.[41] Australia's Scamwatch recorded 18,000 imposter scams in the first seven months of 2021, of which 95 per cent were made through phone calls and 2 per cent suffered financial loss.[42]For Robocalls, the FCC in the US estimated that financial losses incurred by the American population is estimated at $10bn annually.[43]

The Communications Consumer Panel (2020) conducted independent research to understand the prevalence of scam calls and texts in the UK. Fraud or 'scams' cost the UK £190bn a year with £6.8bn as a result of fraud that directly targeted individuals.[44] They found that telephone scams accounted for 12 per cent of people who lost money, with 64 per cent of people losing more than £100, and 28 per cent lost more than £500.[45] Text scams were estimated to account for 15 per cent of people who lost money, with 63 per cent of people losing £100 this way.[46]

[37] The way data are collected on scam communications means that it is not always possible to separate out harm from different sources, such as isolating the fraud deriving from CLI spoofing or smishing alone.
[38] Communications Fraud Control Association (2021) 'Fraud Loss Survey Report 2021', p.7 [online].
[39] Europol (2019) 'Hold the phone! The threats lurking behind a missed call and other forms of telecom fraud' [online].
[40] Europol (2021) 'Cyber-Telecom Crime Report 2019'. p.6 [online].
[41] UK Finance (2022) 'Annual Fraud Report: The Definitive Overview of Payment Industry Fraud in 2021', p.24 [online]
[42] FraudSMART (2021) 'FraudSMART Monitor', p.18 [online]
[43] Federal Communications Commission (2022b). 'FCC mandates that phone companies implement caller ID authentication to combat spoofed Robocalls' [online]
[44] The Police Foundation (2018). 'More than just a number: Improving the police response to victims of fraud.' p.66 [online]
[45] Communications Consumer Panel (2020). 'Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?', p.10 [online]
[46] Communications Consumer Panel (2020). 'Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?', p.10 [online]

The Scottish Government commissioned a study in 2018 to analyse the impacts of actions set out in the nuisance calls commission action plan and to examine the outcomes of past interventions. Within this report, a summary of separate estimates is provided which evidences the vulnerability of consumers due to different types of telephone scams.[47] For instance, it references Citizens Advice's finding that the median loss of a 'phone scam' is £693 (based on three months' worth of case reports in 2017), and trueCall's estimate from 2016 that £845 was lost per successful 'phone scam'. As a result of courier fraud phone scams in 2016, £176 was lost per call, with 5,695 reported calls.

3.4.2 Opportunity cost of wasted time

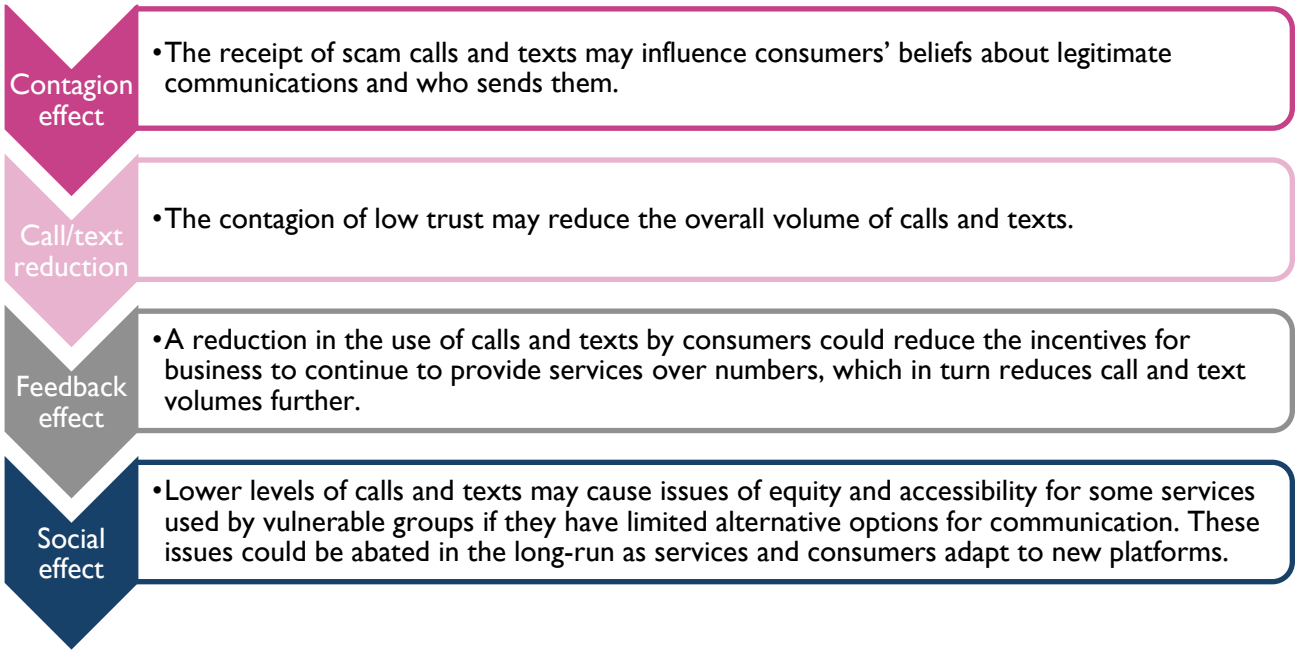
Consumers incur an opportunity cost when they receive and engage with scam calls and texts as these actions consume time and resources that could otherwise be allocated to other things. Scam calls and texts received during working hours take time out of a productive activity that, in aggregate, could be costly to the economy; those received out of work hours takes away valuable leisure time.[48]

3.4.3 Lost trust in voice and SMS communications

One of ComReg's motivating factors in addressing scam calls and texts is that these can reduce trust in the integrity of Irish telecommunication services.[49] The issue of trust has been considered previously in the context of non-geographic numbers (NGNs), where ComReg considered that a lack of transparency could have wide-ranging impacts on how consumers interact with the rest of the telecommunications platform and cause consumer harm.[50] These impacts are relevant to scam calls and texts in the ways described below. Scam communications can lead to a significant loss of trust in telephone numbers and telecommunications more generally, which can have wider impacts on society through contagion effects and an accelerated reduction in the use of calls and texts by both consumers and businesses. This robs consumers, businesses and wider society of the benefits of telecommunications and can cause particular harm for certain vulnerable groups in terms of accessibility.

[47] Antelope Consulting for the Scottish Government (2018) 'Effectiveness of actions to reduce harm from nuisance calls in Scotland', Annex F [online]
[48] Ofcom (2015). 'Review of how we use our persistent misuse powers', Annex 7, p.5 [online]
[49] NCIT (2022) 'NCIT – Progress Report after 6 months', p.4.
[50] ComReg 17/70 (2017) 'Review of Non-Geographic Numbers' [online]

Figure 3.1: Social impacts of scam calls and texts



Source: ComReg.

A further impact is that lower trust in calls and texts could accelerate the trend of consumers and businesses switching to less-regulated communication services, such as platforms provided over the internet -this a 'deregulatory effect'. Alternative, web-based messaging platforms have historically been difficult to regulate given their inherently cross-border nature, but they have become the focus of policy action more recently due to their potential to be misused for online child abuse[51] and potentially detrimental competition impacts,[52] *inter alia*. The movement towards less-regulated services thus has implications for how regulators and policymakers can protect the public from detrimental activity.

3.4.4 Costs of resolving cases

In the case of scam texts, specifically those carrying malware, consumers' devices may need to be fixed or replaced to fully resolve the issue. This could impose additional costs on those consumers. In the context of cybercrime more broadly, Anderson et al. (2019) state that individuals may expend additional effort to clean the devices that become infected with malware, although it does not quantify this possibility.[53] The prevalence of this harm was estimated following a wave of Microsoft spoofed calls in 2011 through a survey of 7,000 computer users in Ireland, UK, US and Canada.[54]

Another potentially significant area of cost arises from consumers seeking to resolve the impacts of scam calls and texts, such as time spent reporting instances to the police or their bank, or seeking refunds for fraud.

[51] European Commission, COM/2022/209: Proposal for a regulation laying down rules to prevent and combat child sexual abuse, para. 5 [online].

[52] European Commission (2022) 'Digital Markets Act: rules for digital gatekeepers to ensure open markets enter into force' [online]

[53] Anderson et al. (2019) 'Measuring the Changing Cost of Cybercrime', presented at: *The 2019 Workshop on the Economics of Information Security*, Boston, US, 3-4 Jun 2019, p.4 [online].

[54] ActionFraud (2011) 'Microsoft reveals extent of phone scam' [online]

3.4.5 Emotional harm

Consumers may experience emotional distress as a result of a scam call or text, whether they are left financially worse-off by it or not. For example, FraudSMART (2021) notes that whilst only two per cent of those caught by imposter scams in Australia reported a financial loss, many more are expected to have suffered from anger and stress at being targeted in this way.[55] Receiving unwanted calls and texts in excess may be perceived as harassment. A consumer engaging with those calls and texts can lead them to be confronted, harassed, threatened and/or verbally abused by the fraudster. The awareness of being scammed (or facing a scam attempt) can cause people to feel violated, which may be exacerbated if they feel particularly vulnerable (e.g. in their own home).

A Citizens Advice report from the UK in 2017 gave an example of someone who had been receiving scam calls impersonating Virgin Media in which the fraudsters started to verbally abuse the victim and also threaten physical abuse.[56] In a survey of UK adults carried out by Ofcom (2015), seven respondents (out of 46) agreed that emotional harm in the form of annoyance, inconvenience and anxiety were primary harms of concern.[57] The FCC's 2022 report notes the possibility that feelings of interruption and irritation can be caused by unwanted calls.[58]

3.4.6 Increased phone bills

Some spoofed CLI calls, especially Wangiri calls and to some extent Illegal Robocalls, can cause unwanted increases in phone bills. A consumer returning the call (in the case of Wangiri) or selecting an option (Illegal Robocall) can often be connected to a line that charges a premium rate. Europol (2018, 2019) suggests that the scammer in these instances will try to keep their victim on the line for as long as possible to extract the largest charges.[59,60]

3.5 Harms to businesses

Businesses can be caused harm, both as a result of being the target of a scam attempt and as a consequence of the scam culture affecting consumers' attitude to voice and SMS communications. The following presents an overview of the different mechanisms of harms that impact businesses as a result of scam calls and texts.

3.5.1 Financial losses from fraud

Following the same mechanisms discussed above for consumers, businesses may fall victim to fraudulent calls and texts. For example, if businesses engage with a call and pay fraudulent invoices, significant financial losses could be incurred.[61] Similar to that of consumers, businesses are also susceptible to fraudulent calls in the form of Wangiri and Robocalls, resulting in the connection to premium line services.

Another form of fraud encountered in the literature is Private Automatic Branch Exchange (PABX) fraud (see box below). This is where scammers reconfigure a company's telephone system to accept incoming calls

[55] FraudSMART (2021) 'FraudSMART Monitor', p.18 [online]
[56] Couture, X. and Pardoe, A. (Citizens Advice) (2017). 'Changing the story on scams Protecting consumers and increasing reporting.' [online].
[57] Ofcom (2015). 'Review of how we use our persistent misuse powers' [online]
[58] Federal Communications Commission (2022) 'Combatting Illegal Robocalls', p.3 [online]
[59] Europol (2018). 'Toll fraud, international revenue share fraud and more:' [online].
[60] Europol (2019). 'Hold the phone! The threats lurking behind a missed call and other forms of telecom fraud' [online].
[61] FraudSMART (2022). 'Text message scams cost victims average of €1,700 in H1 2022 with businesses suffering average losses of €14,000 due to invoice fraud' [online]

and relay them onward to premium and international numbers.[62] The victim businesses then become liable for the premium-rate calls, which can cause significant financial harm.

Box 9: International evidence on financial losses

There is relatively little published evidence of harms to businesses from scam calls and texts to date. The financial loss due to fraud is the most widely-reported harm caused to businesses in the context of communication scams. However, it is not always clear (or perhaps known) whether the fraud losses quantified are specifically the result of scam calls and texts, or if they are a consequence of communications scams perpetrated across a range of communications media.

The Communications Fraud Control Association (CFCA) estimated global Private Automatic Branch Exchange (PABX) fraud at $3.88bn in 2019.[63] This estimate is obtained by surveying experts from within the industry as to what proportion of turnover is lost to fraud and then scaling-up to a global figure after adjusting responses to account for company size.[64]

3.5.2 Loss of trust and engagement, potentially causing revenue reduction

A consequence of consumers being targeted scams is that their subsequent actions can adversely affect legitimate business. As indicated by FraudSMART (2021), trusted Irish businesses have been the victim of impersonation scams targeting consumers. These businesses may find it more difficult to engage with customers e.g. to sell genuine products or create brand awareness.

This harm has been noted in the literature on email phishing and wider cybercrime. Ramzan (2010) notes that an indirect consequence of phishing scams is that organisations that use email to reach their customers could suffer if customers start to think legitimate emails are scams and ignore them. These organisations could potentially lose out on the benefits of email as a low-cost and convenient communications channel.[65] Moreover, a vendor of anti-phishing technology notes that a phishing attack could cause customers to leave a business, a drop in the number of new customers, and a loss in consumer confidence besides the direct cost of the amount taken by the scammer.[66] These drivers may well also apply to scam calls and texts.

3.5.3 Opportunity cost of wasted time

If a business engages with a scam call or text, the time spent dealing with it results in time and resources wasted that could have been allocated to more productive uses. Dealing with the consequences of successful attacks could likewise cause employee productivity losses, as noted in a recent study on the costs of phishing emails.[67] In aggregate, this diversion of employees from their productive tasks may become costly to businesses and the wider economy.

Box 10: International evidence of opportunity costs

Whilst we have not encountered studies relating this harm to scam calls and texts, we found evidence of its quantification in the phishing literature. Ponemon Institute (2021) finds that the loss in employee productivity

[62] Anderson et al. (2019) 'Measuring the Changing Cost of Cybercrime', presented at: *The 2019 Workshop on the Economics of Information Security*, Boston, US, 3-4 Jun 2019, p.16 [online].
[63] Anderson et al. (2019) 'Measuring the Changing Cost of Cybercrime', presented at: *The 2019 Workshop on the Economics of Information Security*, Boston, US, 3-4 Jun 2019, p.16 [online].
[64] As stated in Anderson et al. (2019).
[65] Ramzan (2010). 'Phishing Attacks and Countermeasures', *Handbook of Information and Communication Security*, Peter Stavroulakis and Mark Stamp (eds.) [online]
[66] Retruster (n.d.). 'The true cost of a phishing attack' [online].
[67] Ponemon Institute (2021). 'The 2021 Cost of Phishing Study' [online].

due to having to deal with a phishing email is the most costly consequence.[68] Using a survey of 590 IT workers in the US who reported an average of 6.83 hours annually dealing with phishing emails, and an average hourly pay for non-IT users, the study finds that the average business loses $3.2m a year to productivity loss caused by phishing. (We note that the average business in this context has a headcount of 9,500 – smaller businesses would incur proportionately lower costs.)

3.5.4 Increased operating costs

Businesses may incur material other costs as they implement anti-impersonation technology and/or adjust their communications strategy to mitigate the risk that they are targeted or impersonated. This may require new software and/or staff resulting in increased overall costs. As discussed in Chapter 3, a key affected industry is the banking industry, as banks are either often impersonated by scammers, or indirectly affected by the fraud perpetrated by the scammer once he or she has obtained banking details through a scam.

A business could incur costs from handling a large volume of complaints from the public. This could happen if many people begin receiving scam calls and texts purporting to be from the business and expect it to do something about this nuisance. This could strain existing call handling facilities and potentially require additional resource for handling and logging complaints.

Moreover, a successful scam attack could cause significant downtime and other processes that would divert resources from other uses (similar to the concept of opportunity cost described above). In the context of phishing attacks, IBM has noted a number of increase operating costs, immediately following an attack. For example, a business may conduct internal investigations, organise a response team, communicate with its customers and regulators and implement lessons learnt.[69] In the longer term, the business may engage third party support and track the effects of the attack on its customer base (as well as other things). For their part, banks may need to process customer refunds and carry out other administrative tasks each time one of their customers is defrauded. These activities would all incur costs for the business.

3.6 Harms to public bodies

Public bodies can be harmed typically as a consequence of the impact of scams on people's attitudes to communications made through voice and SMS communications channels. The following presents an overview of the different mechanisms of harms that impact government/public agencies as well as regulators as a results of scam calls and texts.

3.6.1 Increased operating costs

As with businesses, public bodies may incur costs as they implement anti-impersonation technology and/or adjust their communications strategy to mitigate the risk that they are targeted or impersonated. This may require new software and/or staff resulting in increased overall costs.

It is also possible that public bodies allocate expenditure to certain segments of society expressly to mitigate the harm caused by scam communications. In the absence of scam communications, these funds could be allocated elsewhere. For example, the call blocking project noted in the UK's National Lottery Community Fund (mentioned in the previous section) appears to have been funded by public funds.[70] In this small-scale trial, total funding of £405,000 was provided over three years to purchase call blocking equipment and a package of support services to 840 households that were at high risk from predatory scammers

[68] Ponemon Institute (2021) 'The 2021 Cost of Phishing Study', p.6 [online].
[69] Retruster (n.d.). 'The true cost of a phishing attack' [online].
[70] The National Lottery Community Fund (2020) 'Trading Standards -Blocking Scam and Nuisance Calls for People Living with Dementia', [online]

(approximately £482 per household). We note that this particular issue relates to the distribution of harm rather than the total volume, as public mitigation funding would largely offset the harm experienced by consumers.

Public bodies may also have a responsibility to engage in finding solutions to the scam problem with operators and other organisations, incurring staff and project costs. Other public bodies, such as law enforcement agencies, need to commit time and resources to criminal investigations into scam cases. An estimate of the social cost of fraud in England and Wales per crime committed to individuals (both reported and unreported) is £1,290 (in 2015/16 prices).[71] This measure includes police operating costs and a wider set of costs to society, such as physical/emotional costs to the affected individuals.

3.6.2 Loss of trust and disengagement

As an organisation frequently impersonated by scammers, a public body may find that citizens are less likely to answer its communications as citizens become more uncertain of the veracity of the communication.

A loss of public trust and disengagement could spark a host of potential knock-on impacts. For example, if Irish citizens are less trusting of HSE (Health Service Executive) communications, some may not respond to appointment availability notifications and reminders, causing the HSE to bear the cost of other communication strategies and missed appointments (Did Not Attends, or DNAs) which themselves cause further delays to people awaiting an appointment. We interviewed the HSE as part of our fieldwork, and explore this issue further in Chapter 4. Less trust in communications from one department could generate suspicion of communications from others. Less trust in Gardaí communications could make some people less likely to take genuine communications (in all formats) seriously – including those warning against scams and other causes of harm. In all these examples, lower levels of public engagement could threaten the ability of public bodies to carry out their core duties.

Scam calls and texts could also lead to the public losing trust in the communication regulator's ability to mitigate the harms caused by scam calls and texts. This could jeopardise the regulator's ability to garner public support for its interventions in other fields, and potentially damage the reception of its published support and guidance.

The regulator's ability to respond to telecommunication crises is also effected by scam calls and texts. As highlighted in Box 7, Rogers in Canada experienced a nationwide network outage that lasted more than 15 hours in 2022. Fraudsters used this opportunity to send smishing texts that impersonated Rogers and offered a compensation of $90 to individuals who engaged with their message. This could divert the resources of the regulator away from their primary responsibilities of managing and monitoring the telecommunications network.

3.6.3 Cost of handling complaints

Public services fielding a large volume of complaints could strain existing call handling facilities and potentially require additional resource for handling and logging complaints. This could happen if many people begin receiving scam calls and texts purporting to be from the public body and expect it to do something about this nuisance. In early 2022, the Gardaí experienced such a wave of complaints as consumers raised concerns about vishing attempts claiming to be Gardaí, officials from the Department of Social Protection and the

[71] Heeks et al. (2018) 'The economic and social costs of crime' , Home Office Research Report 99, Table E1 [online].

Attorney General's Office.[72] In 2021, the Gardaí reported that it had received numerous reports of people receiving calls that had spoofed the CLI of a genuine Garda station.[73]

Garda members responding to illegal communications represents an opportunity cost, taking member time away from other activities. In addition, very large volumes of complaints about scam calls or texts received within a small timeframe (as seems to be the case with different waves of scam attempts) could mount pressure on existing infrastructure. We interviewed the Gardaí as part of our fieldwork and they highlighted this as a particular issue for them. We explore this further in Chapter 4.

The prevalence of scam calls and texts, both successful and attempted, can lead to complaints from citizens and businesses which in turn can increase operating costs for the regulator receiving these complaints.

Box 11: International evidence on complaints to regulators

The additional resource pressures caused by public complaints to the communications regulator can also be gleaned from the experiences in other jurisdictions. The US FCC (2022) reports having received approximately 500,000 complaints of scam calls between 2019 and 2021 in 2019.[74] Furthermore, in the first three quarters of 2021, the US Federal Trade Commission received an average of more than 300,000 robocall complaints per month.[75] Ofcom (2022) also reported that the Information Commissioner's Office received 131,491 complaints regarding texts or call scams in 2021.[76]

3.6.4 Opportunity cost of wasted time

When public bodies and their employees are targeted by scammers, the time spent on scam calls may take resources away from more productive uses. In aggregate, this may become costly to public bodies and generally complicate the task of discharging their duties.

Especially important for law enforcement agencies is the opportunity costs of investigating scam cases. By committing resources to the problem – increasingly so as the problem worsens and as budgets permit – organisations such as the Gardaí may be faced with difficult trade-offs. Resources that could be allocated to other crimes may instead be directed to scam cases.

3.7 Harms to operators

3.7.1 Potential revenue reduction

Operators can be caused harm by scam calls and texts, but – unlike other stakeholders – may also stand to benefit from scams which can generate revenues known as "toxic revenues". Some operators may benefit financially from scams, given that scammers generate revenues through call and SMS traffic termination, origination and/or transit. However, not all scammers would pay their bills, and it is not known whether this activity would be profitable.

On the other hand, consumers may decrease their phone usage as a result of being scammed or otherwise losing trust in voice and SMS networks due to the fear of being scammed.

[72] Foy, K. (2022) 'Gardaí swamped with complaints over new 'vishing' scam as one woman loses €5,000', *Independent.ie* [online].
[73] An Garda Síochána (2021) 'Fraud Prevention Advice - Automated Phone Calls from Garda Station Phone Numbers' [online].
[74] Federal Communications Commission (2022) 'Combatting Illegal Robocalls' [online]
[75] Federal Trade Commission (2021). 'Biennial Report to Congress Under the Do Not Call Registry Fee Extension Act of 2007 Federal Trade Commission.' [online]
[76] Ofcom (2022). 'Tackling scam calls and texts. Ofcom's role and approach.' [online]

Operators were clearly aware of the potential impacts of scam calls and texts on the communications they facilitate. One MNO, in particular, noted that interventions to curtail fraudulent communications could increase trust in mobile numbers, and suggested that there was scope for operators to benefit commercially from being able to offer networks of trust. The operators were also clearly aware of damage scam calls and texts can do to organisations' reputations, and hence also the trust consumers have in the communications they send.

3.7.2 Costs of handling complaints

Even if operators' customers do not turn away from voice and SMS methods of communication, they may file complaints. Large volumes of complaints could strain existing call/other handling facilities and potentially require their expansion; and some complaints may require escalation and action to be taken. This activity consumes resources.

We understand from ComReg that certain operators claim to receive thousands of complaints from customers regarding the receipt of nuisance communications each year. The operator notes that this datapoint was provided on a 'best effort' basis, suggesting that it does not routinely collect this information. Indeed, other operators could not provide any such information.

3.7.3 Diverting resources away from legitimate communications

Having to facilitate high volumes of inbound calls or mobile originated text messages sent by malware infected devices can 'flood' networks and consume network resources that would otherwise facilitate legitimate calls.

4 The Scale of the Problem in Ireland

4.1 Introduction

This chapter presents the evidence on the scale of the problem in Ireland. It contains the results of our modelling of the harms caused by scam calls and texts and is evidenced through our desk-based research and our primary research through surveys and stakeholder interviews.

Section 4.3 outlines the prevalence of scam calls and texts (SMS messages) in Ireland. Sections 4.4-4.7 present the evidence on the magnitude of harms to different stakeholder groups. The harms are quantified where data and evidence are available to provide sufficiently robust estimates, meaning that not all of the harms identified in Chapter 3 have been quantified. This means that the estimates provided in this chapter are necessarily conservative relative to the overall harm caused to Irish society. Section 4.8 draws conclusions on the total harm in Ireland.

4.2 Modelling methodology

Our estimation of harm is based on evidence from public data sources, our interviews and selected case studies. A key source of evidence were our consumer and business surveys, as described below.

4.2.1 Description of the surveys

The consumer and business surveys were conducted by Behaviour and Attitudes ("B&A") between October and December 2022.

Consumer survey

The consumer survey received 1,219 responses from adults aged 16+ across Ireland. All of the results were sourced and obtained through B&A's online research panel. The survey captured roughly equal shares of male and female respondents and covered a broad range of ages and incomes. Responses were received from Dublin, the Rest of Leinster, Munster and Connaught/Ulster. The survey was quota-controlled in terms of age, gender, socio-economic class and region. We extrapolated the harms calculated from the survey to the relevant population in Ireland based on Irish population statistics[77] and the shares of people that reported having received scam calls and texts in the past year in the survey. The details of how we calculated these population variables are provided in the harms modelling appendix.

Business survey

The business survey received 794 responses from businesses across Ireland. Most responses were received through telephone and the rest through an online research panel. The survey covered micro, small, medium and large firms located in Dublin, the Rest of Leinster, Munster and Connaught/Ulster. The responding firms covered a range of industries, with the top five being Construction, Professional, scientific & technical, Transportation, storage & communication, Retail Trade & Repairs and Accommodation & food service activities. B&A weighted the responses to each question in the business survey to estimate the number of firms in Ireland that would be captured by each question. This is based on the distribution and characteristics of firms in Ireland and a total number of businesses of 309,366. This allowed us to model the business harms directly using the figures from the survey.

[77] World Population Review (2022) people over age 18 in Ireland in 2022 [online]

The business survey was similarly controlled in terms of size (employee number), region and industry sectors. This ensures that the responding samples reflect the profile of the adult population and businesses of Ireland.

4.2.2 Summary of estimated harm in Ireland

Not all harms described were possible to estimate. Although we have endeavoured to gather all information possible, some harms are inevitably difficult to estimate with any reasonable margin of certainty, given the data available or lack of certainty regarding future market trends. Therefore, our estimates of harm are necessarily lower-bound estimates, as many harms are not quantifiable. Table 4.1 below summarises all the harms we identified, whether we were able to quantify them and the evidence used to make our decision.

Table 4.1 : All harms identified

Stakeholder	The harm	Quantified? Yes/No	Evidence/Reason?
Consumers	Financial losses from fraud	**Yes**	Estimated using the Consumer survey and CSO data
	Costs of resolving fraud cases	**Yes**	Estimated using the Consumer survey and CSO data
	Opportunity cost of wasted time	**Yes**	Estimated using the Consumer survey, CSO data and estimates of the value of time from the Department of Transport
	Emotional harm	**Yes**	This is indirectly measured via the WTP analysis and supported by evidence of emotional harm provided separately in the surveys.
	Lost trust in voice and SMS communications	**Yes (indirectly)**	This is indirectly measured via the WTP analysis and supported by evidence of lost trust provided separately in the surveys.
	Increased phone bills	**No**	No sufficiently detailed information available
	Total of all harms	**Yes**	Using the Willingness-to-Pay methodology, we calculated the overall disutility of scam calls and texts to Irish consumers
Businesses	Financial losses from fraud	**Yes**	Estimated using the Business survey and CSO data
	Loss of revenues	**Yes**	Estimated using the Business survey and CSO data, however not relied upon due to uncertainty
	Opportunity cost of wasted time	**Yes**	Estimated using the Business survey and CSO data
	Increased operating costs	**Yes (partially)**	Using case studies
	Total of all harms	**Yes**	Using the WTP methodology
Public bodies	Increased operating costs	**Yes (partially)**	Case studies from the Gardaí, the HSE
	Loss of trust	**No**	Depends on difficult to predict second order effects
	Cost of handling complaints	**No**	Lack of data
	Opportunity cost of wasted time	**No**	Lack of data
Operators	Potential revenue reductions	**No**	Too much uncertainty as this is a second order effect
	Costs of handling complaints	**No**	No sufficiently detailed information available
	Inefficient investment	**No**	Too much uncertainty as this is a second order effect

The remainder of this chapter is laid out as follows.

- Section 4.2.3 describes our overall approach to estimating the harms
- Section 4.3 describes the prevalence of scam calls for consumers and businesses in Ireland.
- Section 4.4 describes and estimates the harms to consumers.
- Section 4.5 describes and estimates harms to businesses.
- Section 4.6 describes and estimates the harms to public bodies.
- Section 4.7 describes and estimates the harms to operators.

- Section 4.8 estimates the total harm in Ireland.

Sections 4.3 to 4.7 are structured in the same way. First, we set out the evidence that is already available from existing studies and reports ("existing evidence"). We then provide an update based on the fieldwork specifically carried out for this study, including business and consumer surveys, stakeholder interviews and our bottom-up modelling of harms ("fieldwork"). Section 4.8 concludes with an assessment of the total harm in Ireland and how this might evolve. As noted at the outset of this chapter we have provided estimates where sufficiently robust data is available – therefore the estimates are necessarily conservative.

4.2.3 Overview of the approach

Our approach to estimating the harms from scam calls and texts consisted of three tools, and combined evidence from public data sources, our interviews and results from consumer and business surveys (the fieldwork) and selected case studies, with extrapolation to the relevant Irish population.

- Bottom-up cost modelling used data points derived from our consumer and business surveys to estimate the costs and prevalence of a range of harms, such as losses from fraud, the monetary value of time spent resolving scams; or the monetary value of time spent engaging with scam calls or texts. These individual harm estimates were then added together for consumers and businesses separately. Bottom-up cost modelling cannot capture all harms, such as intangible harms of annoyance or distress, or second-order effects of a loss of trust in calls or SMS.

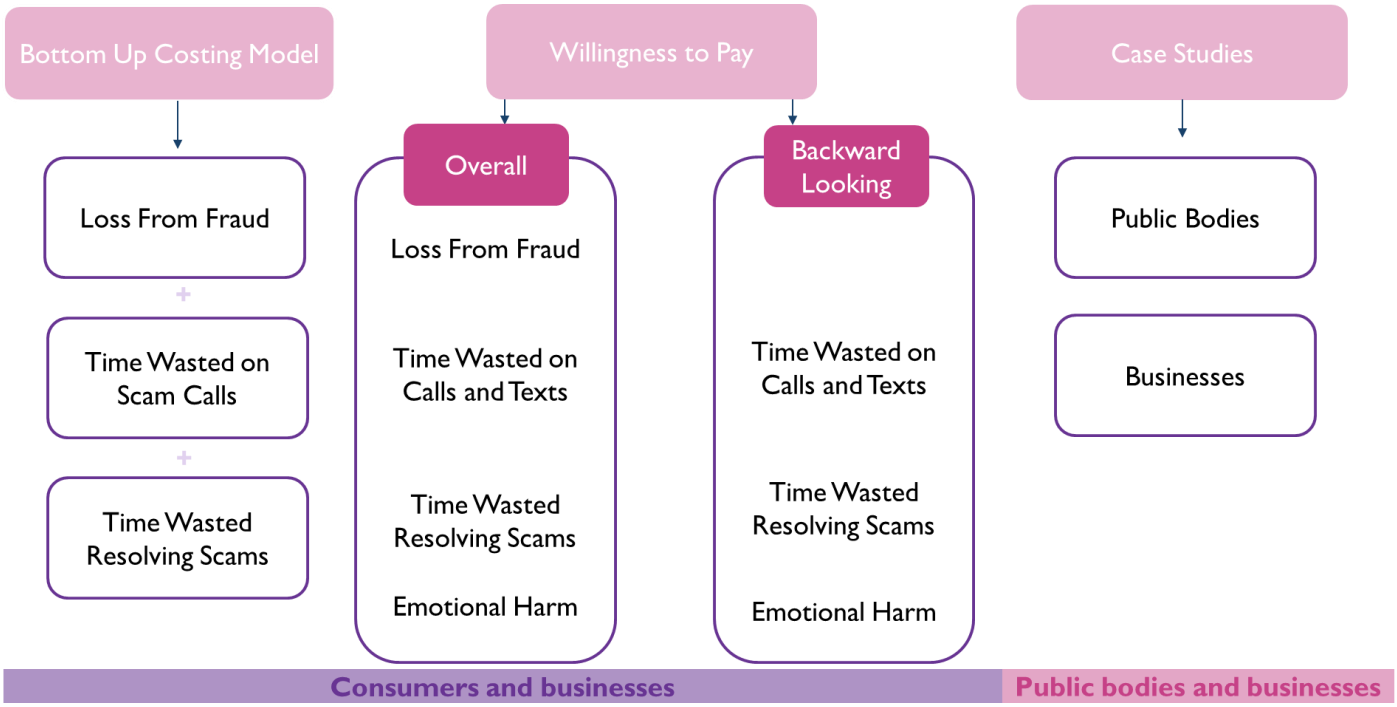
- Willingness-to-pay (WTP) analysis was used to capture intangible harms from scam calls and texts. In our surveys we asked consumers and businesses how much they would be willing to pay to avoid receiving scam calls and texts (using a variety of question formats). This enabled us to estimate a fuller range of harms including the annoyance or distress recipients might feel, or fears about potential losses from fraud (what we term 'overall WTP'). The overall WTP estimates represent a different approach to estimating harm compared to the bottom-up cost modelling, and as such the two sets of harms estimates should not be added together and are instead used in order to act as sense check on each other and produce more reliable estimates of the harm caused by scam calls and texts.

  For consumers, we also included a 'backwards looking' willingness to pay estimation, limited to actual consumer experiences of receiving scam calls and texts.[78] As this only included those who had received scams calls or texts and had not experienced losses from fraud, this WTP estimate captures more accurately just the annoyance/distress and time cost element of the harm. As such, it is possible to add this to different elements of the bottom-up estimates such as losses from fraud.

- Illustrative case studies provide examples of aspects of harm that were not captured in the above two tools due to their bespoke nature, in particular for businesses and public bodies.

[78] Consumers were asked how much they would be willing to pay to not have received the scam calls and texts they received in the past year, rather than being asked what they would be willing to pay to avoid receiving all scams in the future.

Figure 4.1: Summary of techniques applied



In relation to consumer harms, we have only relied upon selected estimates as many techniques produce results covering overlapping harms. Such estimates cannot simply be added together as this could lead to double-counting. We therefore carefully selected which results to use to build up an aggregate figure of harm to consumers, choosing the most direct estimation of harm wherever possible.

As a robustness check, the forward looking WTP question produces and "all-in" estimate of the overall harm to consumers.

A detailed description of our approach is contained in the Appendix. It should be noted that our approach represents the most comprehensive attempts to estimate harm from scam calls and texts that we are aware of,[79] and is the first such attempt in Ireland.

4.3 The prevalence of scam calls and texts in Ireland

4.3.1 Existing Evidence

As described in Chapter 3, there are a number of industry estimates of the prevalence of scam calls and texts in Ireland:

- Bank of Ireland research (2022) found that 74 and 43 per cent of surveyed adults had received scam texts and calls, respectively, that appeared to be from their bank.[80]
- FraudSMART (2021) reports that 72 per cent of its survey respondents were approached by fraudsters through scam calls, with 32 per cent via text message.[81]

[79] As mentioned in Chapter 3, Ofcom conducted an analysis using a time-cost approach, willingness to pay and costs of mitigation activities, that was limited to silent and abandoned calls. See Ofcom (2015). 'Review of how we use our persistent misuse powers' [online]

[80] Leonard, R. (2022) 'Hack the human – the psychology of cyber fraud, Professor Mary Aiken', *Irish tech News* [online]

[81] FraudSMART (2021) 'FraudSMART Monitor', p.4 [online]

- AIB research (2021) found that 80 per cent of people aged between 18-34 in Ireland had been targeted by financial scams within the past 12 months, having received either a text, call or email they believed to be fraudulent. Those over 55 were more likely to be targeted by fraudsters, with 85 per in this age group receiving some form of fraudulent communication.[82]

These estimates of prevalence are all somewhat lower than those found through our fieldwork of consumers, as described below. We would note that the fieldwork presented below is more recent and more detailed such that it refers to scam communications more generally rather than related to particular institutions (e.g. banks or financial institutions). However, the overall picture is one of a high and increasing prevalence of scam calls and text calls in Ireland.

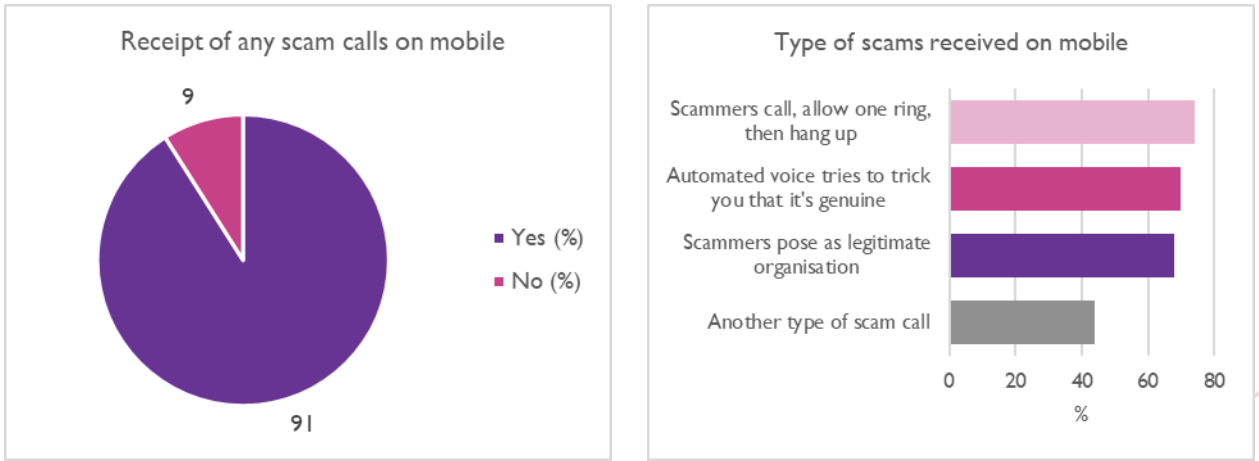
4.3.2 Fieldwork: prevalence amongst consumers

Scam calls received by consumers

The consumer survey shows that 91 per cent of adults in Ireland received a scam call to their mobile phone in the last year (Figure 4.2, left panel). A lower proportion of adults (74 per cent) received a scam call on their landline (Figure 4.3, left panel). This shows that scam calls are affecting the vast majority of the adult population in Ireland, and that even though scammers appear to be focussing on mobile phones, landlines are also subject to significant scam call traffic. These results combined with an estimate of the Irish consumer population capable of receiving calls suggest that consumers received 59m scam calls in the last year.

More than 65 per cent of adults have received scam calls to their mobiles where the scammers pose as legitimate organisations (Spoofing), where an automated voice appears (Robocall), and where the (suspected) scammer rings once then hangs up (Wangiri) (Figure 4.2, right panel). This is consistent with growing prevalence identified with CLI spoofing in Ireland to administrate impersonation scams and the use of Wangiri calls. More than half of adults have received scam calls to their landlines where scammers pose as legitimate organisations and where automated voices greet them (Figure 4.3, right panel).

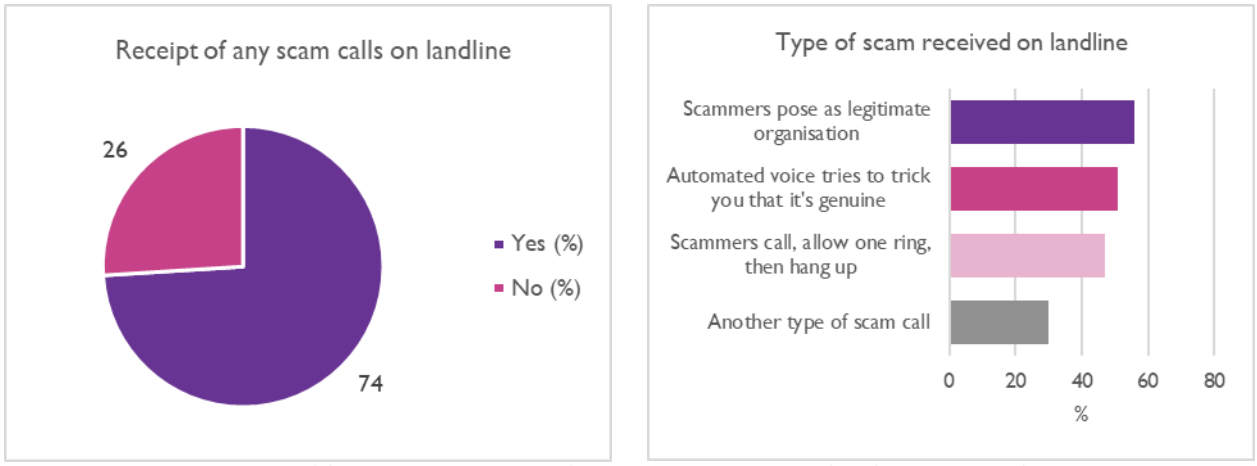
Figure 4.2: Prevalence and type of scam calls received on mobiles (% of respondents)



Source: Europe Economics analysis of ComReg consumer survey. Q.6a Have you received any of the following types of scam call in the past year on your mobile phone?

[82] AIB (2021). 'Four out of five people have been targeted by Fraudsters in the last year', p.1 [online]

Figure 4.3: Prevalence and type of scam calls received on landlines (% of respondents)

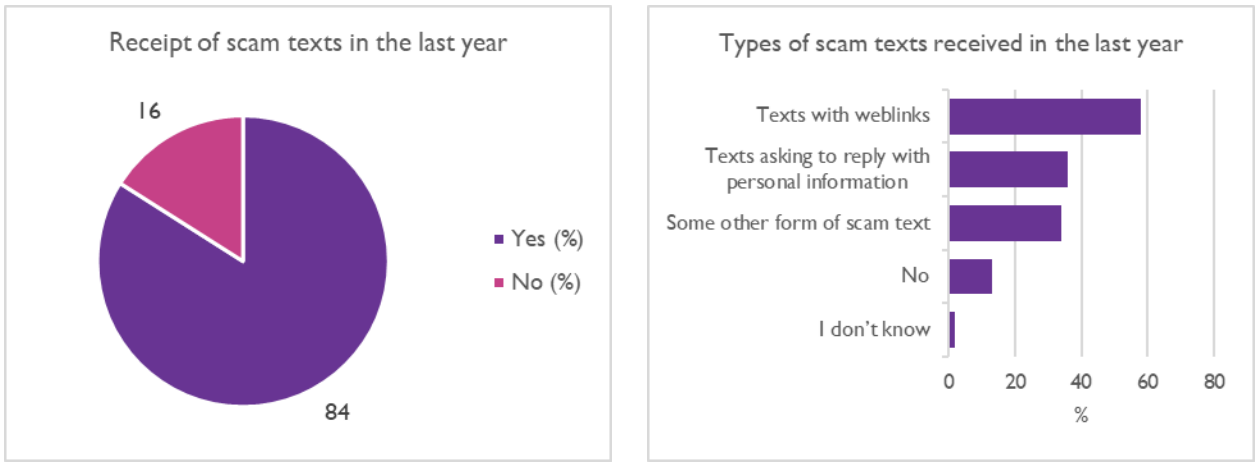


Source: Europe Economics analysis of ComReg consumer survey. Q.6b Have you received any of the following types of scam call in the past year on your landline?

Scam texts received by consumers

The consumer survey shows that 84 per cent of adults have received some form of scam text in the past year (Figure 4.4, left panel). Most adults (58 per cent) have received a scam text with weblinks, whilst more than a third have received texts asking for personal information or some other form of scam text (Figure 4.4, right panel). These results suggest that consumers received 47m scam texts in the last year.

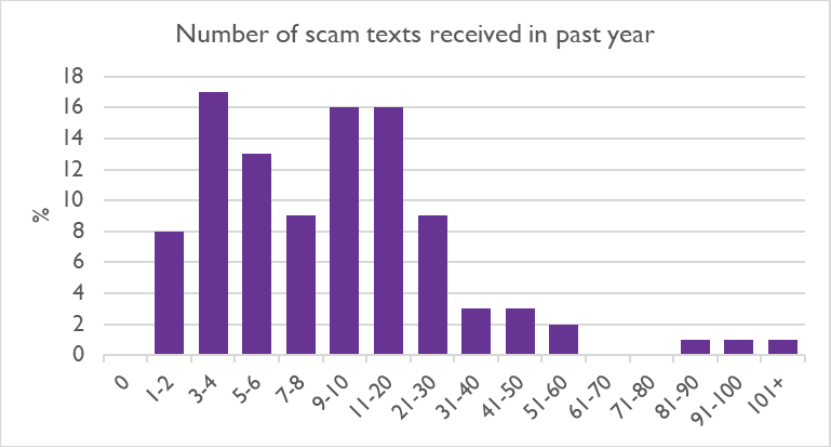
Figure 4.4: Prevalence of scam texts (% of respondents)



Source: Europe Economics analysis of ComReg consumer survey. Q.24 Have you received a scam text in the past year?

The survey asked how many scam texts had been received in the last year. The results are characterised by a 'twin peak' pattern, where relatively larger shares of adults received either 3-4 scam texts (17 per cent) or 9-20 scam texts (32 per cent) (Figure 4.5). The mean number received was 15.

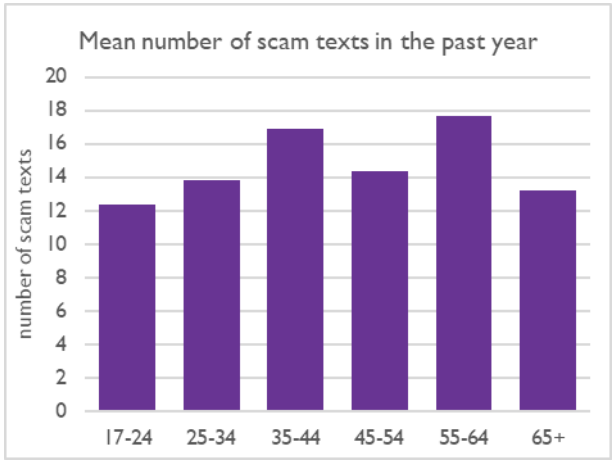
Figure 4.5: The number of scam texts received in the past year (% of respondents)



Source: Europe Economics analysis of ComReg consumer survey. Q.25 Approximately how many scam texts have you received in the past year?

The number of scam texts received in the past year varies somewhat by age, as shown in Figure 4.6. The mean number received is highest for adults in the age bands 35-44 (17) and 55-64 (18). Older-age adults report receiving a greater number of scam texts than most other age groups.

Figure 4.6: The mean number of scam texts received in the past year by age

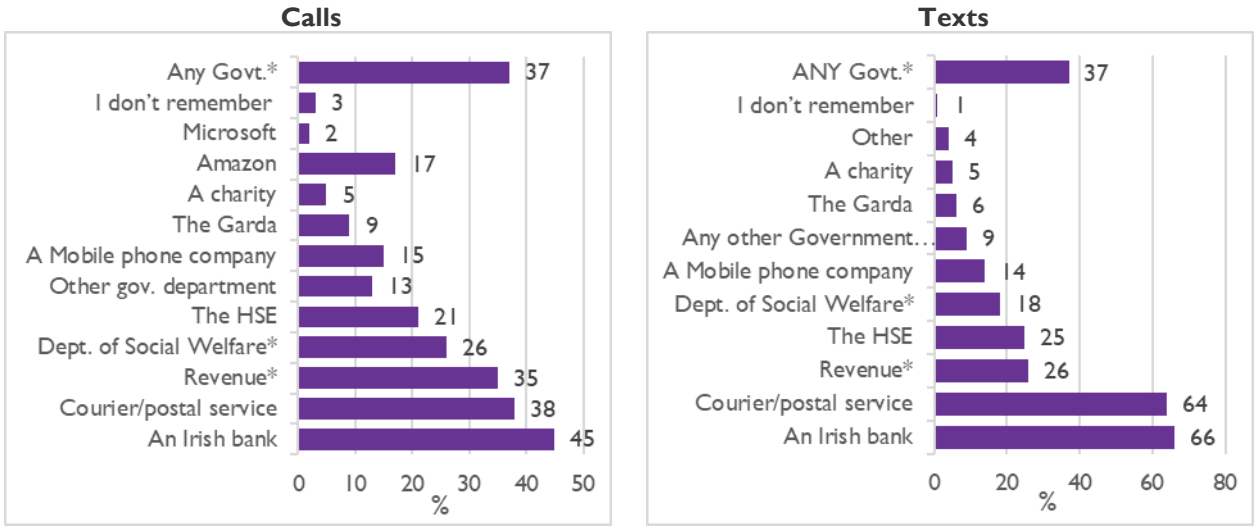


Source: Europe Economics analysis of ComReg consumer survey. Q.25 Approximately how many scam texts have you received in the past year?

Prevalence of organisation impersonation attempts directed at consumers

Our consumer survey gathered information about the types of organisations being impersonated in scam calls and texts. Figure 4.7 shows the share of different organisations impersonated in the scam calls and texts received by survey respondents in the last year. The most commonly impersonated organisations are banks and postal services, followed by the HSE and other public bodies. A broadly similar distribution of impersonations is seen across scam calls and texts.

Figure 4.7 : Share of different organisations impersonated in scam calls and texts (% of respondents)



Source: Europe Economics analysis of ComReg consumer survey. Q.10b Which organisations have they impersonated in calls to you? (Left panel) Q.27b Which organisations have they impersonated in the texts to you? Note that order is different for scam calls and texts, with scam texts graph including 'other' category.

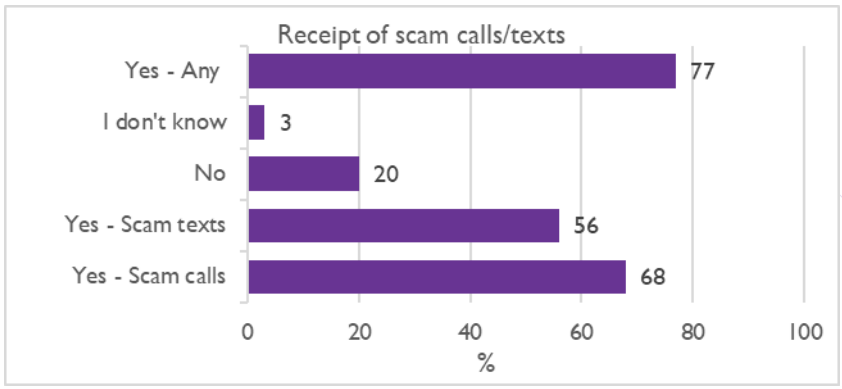
4.3.3 Fieldwork: prevalence amongst businesses

Scam calls and texts received by businesses

The business survey shows that 77 per cent of businesses in Ireland either received a scam call or text in the last year (see Figure 4.8). Some 68 per cent indicated that they had received scam calls and 56 per cent a scam text; 20 per cent had not received either in the past year.

All surveyed businesses were also asked about the level of concern they felt towards receiving a scam call or text. In both cases, approximately 60 per cent of businesses indicated that they felt some level of concern towards the possibility of receiving a scam call or text. Concern was considerably higher as firm size increased with 73 per cent and 94 per cent of firms with 50-249 and 250 + employees indicating some level of concern, respectively. This suggests that Irish businesses received over 6m scam calls and nearly 4m scam texts in the past year.

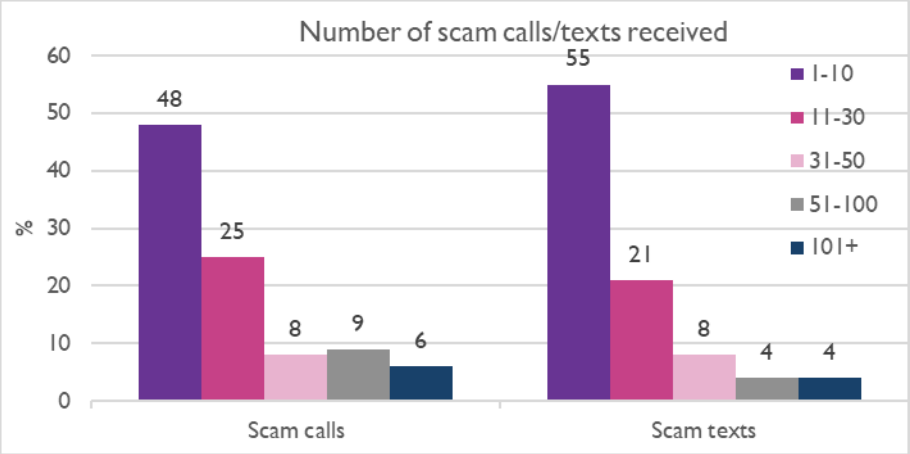
Figure 4.8 : Receipt of scam calls/texts in the last year (% of respondents)



Source: Europe Economics analysis of ComReg business survey. Q.3 Has your business received scam calls or SMS (texts) in the past year?

The majority of businesses indicated that they received 1-10 scam calls or scam texts over the past year (48 per cent and 55 per cent respectively) (see Figure 4.9). The mean number of scam calls received last year was 30, whilst for scam texts it was 22.

Figure 4.9 : The number of scam calls/texts received in the past year (% of respondents)

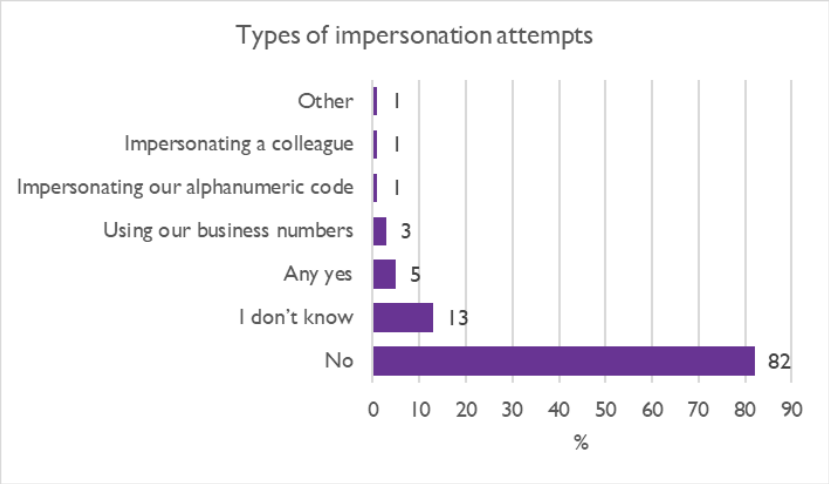


Source: Europe Economics analysis of ComReg business survey. Q.4a Approximately how many scam calls has your business received in the past year? And Q.4b And approximately how many scam texts has your business received in the past year?

Impersonation of organisations in scam calls and texts

Figure 4.10 shows that 82 per cent of firms said that they had not been impersonated by scam calls/texts to their knowledge. Only 5 per cent of businesses experienced at least one form of impersonation, either using their number to contact customers, impersonating their alphanumeric codes, impersonating their colleague internally, or some other form of impersonation. Larger businesses were more likely to be impersonated, with over a third of firms with 250+ employees reporting to be impersonated in some way.

Figure 4.10 : The types of organisations that were impersonated by scams calls/texts (% of respondents)



Source: Source: Europe Economics analysis of ComReg business survey. Q.16 Has your business ever been impersonated by a scam call/text to your knowledge?

4.3.4 Summary of prevalence

Our fieldwork shows that **91 per cent of consumers** in Ireland have received scam calls to their mobile in the past year – and that a significant proportion have received scam calls on their landline (74 per cent). This reflects the different levels of usage between mobile and landline, with our survey showing that 100 per cent of the population uses a mobile, but only 40 per cent use a landline.[83] Scam texts are also very common – **84 per cent of consumers** reporting having received these in the past year.

[83] See appendix for further contextual survey statistics.

Prevalence among businesses in Ireland shows a similar pattern. Around **77 per cent of businesses** either received a scam call or text in the last year, with scam calls being more likely than scam texts (68 per cent indicated that they had received scam calls and 56 per cent a scam text).

Consumers considered the most commonly impersonated organisations to be **banks and postal and courier services, followed by the HSE and other public bodies.** From the businesses' point of view, only five per cent of businesses experienced at least one form of impersonation, either using their number to contact customers, impersonating their identity using alphanumeric codes, impersonating their colleague internally, or some other form of impersonation.

4.4 Harms to consumers

4.4.1 Existing evidence

A comprehensive study of direct harm to consumers from scam calls and texts in Ireland has not previously been conducted. An Garda Síochána offers a broad estimate of harm caused by account takeover fraud (which included but is not limited to fraud caused by scam calls and texts) of €22.5m in 2021.[84] The CSO reports that fraud crime, largely driven by unauthorised transactions and attempts to obtain personal or banking information online or by phone, nearly doubled to 17,354 incidents in the year to the end of March 2022.[85] Furthermore, offenses have more than trebled from 5,382 in the year to Q2 2018 to 16,202 in the year to Q2 2022. Within this period, the number of incidents had been increasing steadily between 2018 and 2021 but a large volume increase was observed between 2021 and 2022. FraudSMART (2022) estimates that consumers that fell victim to smishing attacks lost an average of €1,700 in the first half of 2022.[86]

4.4.2 Fieldwork

Financial loss from fraud

The consumer survey asked respondents about their experiences of scam calls and texts separately. The survey implies that over 365,000 people were defrauded for various amounts in the past year – 175,000 people were defrauded after receiving scam calls and lost an average of €494, and 190,000 lost an average of €231 after receiving scam texts (Figure 4.11). The survey results show that a number of victims were able to recover at least some of their fraud losses, and so we account for that in our estimates of harm.[87]

Figure 4.11: Summary of financial loss from fraud based on consumer survey results

No. of people who lost money	Highest losses	Average loss	Average share of loss recovered
• Calls: 175,000 • Texts: 190,000	• Calls: €5k+ • Texts: €3k-€5k	• Calls: €494 • Texts: €231	• Calls: 28% • Texts 34%

Source: Europe Economics analysis.

[84] An Garda Síochána (2021) 'GNECB Fraud Awareness Week - Account Takeover Fraud - 1 April 2022' [online]
[85] CSO (2022). 'Recorded Crime Q1 2022'. [online]
[86] FraudSMART (2022) 'Text message scams cost victims average of €1,700 in H1 2022 with businesses suffering average losses of €14,000 due to invoice fraud' [online]
[87] We assume that the majority of the recovered money was recovered by banks, and thus represents a loss to banks. We present this in the subsequent section on harms to businesses.

Whilst fewer people are estimated to lost money as a result of scam calls, they nevertheless caused the larger share of total loss owing to the higher average loss: €75m over the year (accounting for some loss recovery). Scam texts caused €35m in annual losses net of recovery. The total net financial loss from fraud caused by scam calls and texts is therefore estimated to be €109m in the last year. We note that this is much higher than An Garda Síochána's €22.5m estimate of the loss from account takeover fraud. This is expected as people are unlikely to report small scams – our survey shows that only around one in four people who lost money from a scam text would consider reporting the scam to the Gardaí.[88]

Opportunity cost of time resolving issues associated with scam calls and texts

As we saw above, some people are able to recover at least some of the loss they incurred after being scammed via calls and texts. However, many survey respondents indicated that it took time to resolve the subsequent issues caused to them. Again, we assume that this time could have been spent more productively or on leisure activities.

The opportunity cost is calculated as the total time wasted due to resolving issues resulting from scam calls and texts (not including the time spent on the actual call) multiplied by the value of time. The total harm from resolving issues associated with scam calls is thus estimated at €776,000 over the year and scam texts is €248,000 for the year. Together this yields a total harm of €1m over the year.

Table 4.2 summarises the total quantified costs from successful scams.

Table 4.2: Financial loss from successful scams – consumers (€m)

	Gross loss Before recovery	**Net loss** Accounting for recovery	**Total net loss due to fraud (incl. time)**
Scam calls	86	75	75.78
Scam texts	44	35	35.25
Total	**130**	**109**	**111**

Source: Europe Economics analysis. Values may not add due to rounding

The opportunity cost of time engaging with scam calls

Communicating with a scammer before recognising them as such takes time out of one's day. It is reasonable to assume that this time could have been spent more productively or on leisure activities. We estimate the opportunity cost of this time (which is effectively a measure of the nuisance value associated with dealing with such calls).[89] This harm is assumed to be specific to scam calls and thus we have not calculated a scam text equivalent.

Based on the mean time spent on a call with a scammer and estimates of the values of leisure and work time, we estimate the opportunity cost of time engaging with scam call was €40m in the last year.

Lost trust in voice and SMS communications

Scam communications can lead to a significant loss of trust in telephone numbers and telecommunications more generally, which can have wider impacts on society through contagion effects and an accelerated reduction in the use of calls and texts by both consumers and businesses. This robs consumers, businesses and wider society of the benefits of telecommunications and can cause particular harm for certain vulnerable groups in terms of accessibility.

Quantifying the impacts of a loss of trust in telecommunications is challenging given difficulties in obtaining this data from users. However, our research provides an indication of the potential impact. Based on consumers' willingness to pay to avoid scam calls and texts, we estimate an upper bound of harm of nearly

[88] Further, only three per cent of all scam text recipients would consider reporting to the Gardaí. Europe Economics analysis of ComReg consumer survey. Q.31 What do you typically do when you receive a suspected scam text?

[89] It may be that some proportion of costs relating to consumers' time (e.g. by engaging with scam calls or resolving fraud) is in fact borne by businesses if such time is incurred during a working day. For simplicity we incorporate all these costs into the consumer section (as there is no danger of double-counting with our business survey).

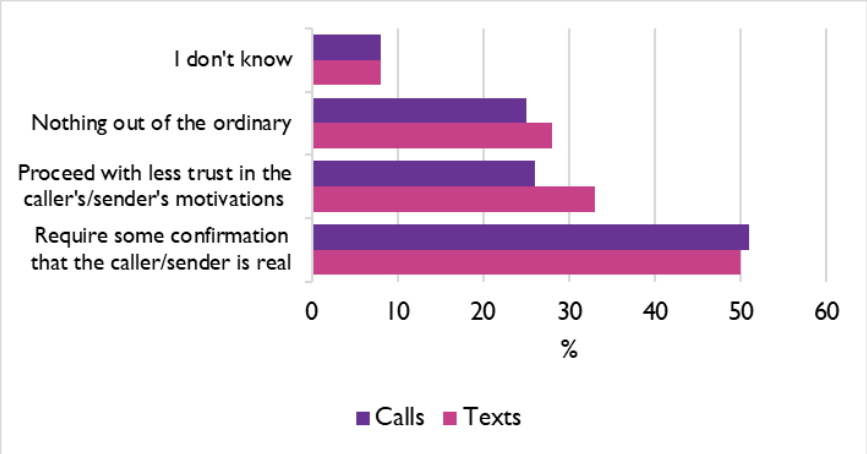
€400m. If we assume that around €170m (the 'backward looking', quantified consumer harm) accounts for direct harm to consumers from scams experienced in a year, then the remaining €230m could represent potential harm from a loss of trust in telecommunications and other potential harms anticipated by consumers. This is an unsurprisingly a high figure, as trust underpins use and the value of SMS and Voice to Irish consumers and businesses, and given the high number of calls and SMS sent each year, and the revenues consumers pay for such services.

In addition, businesses that rely on calls and texts as part of their revenue-generation activity (e.g. marketing, reminders etc.) have estimated that around four per cent of their revenue could be at risk as a result of consumers' loss of trust in calls and texts. This reflects the forgone benefits of these telecommunications to consumers and businesses.

The consumer survey allows us to gauge the extent to which scam calls and texts might have impacted upon public levels of trust in mobile communications. Our survey results show that around 20 per cent of adults have lost trust in calls and texts in general, and that many have started switching to other messaging platforms (e.g. internet-based). In addition, around 65 per cent of adults have lost trust in call/text information and reminders from service providers such as banks, utilities, health services and other public bodies.

We first asked respondents how they react when they receive calls or texts from an organisation that they know has recently been the target of spoofed communications. Figure 4.12 shows that around half would typically require some confirmation of the legitimacy of the caller/sender. Around a third of those who received scam texts would proceed with less trust in the sender's motivations. A quarter of those who received scam calls would do the same.

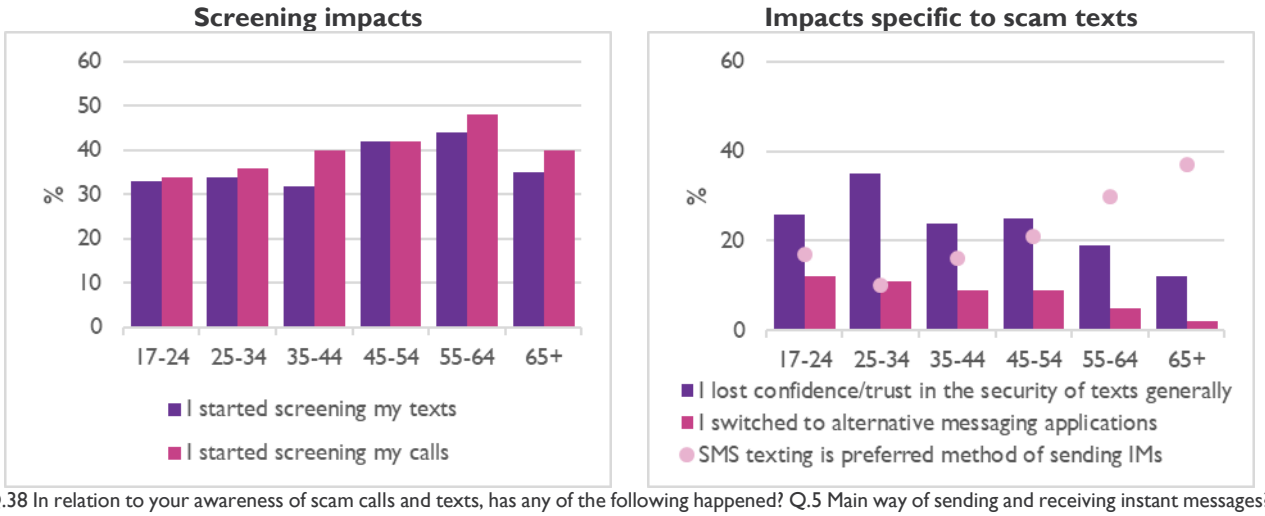
Figure 4.12: Actions taken after receiving call/text from recently spoofed organisation (% of respondents)



Q.19 What have you done if you answered a call from an organisation, for example your bank, and you were aware scammers had recently been impersonating these organisations? Q.35 What have you done if you received a text from, say your bank (or another organisation), and scammers had recently been impersonating these organisations?

We also asked respondents about their actions in response to their awareness of scam calls and texts more generally. The left panel of Figure 4.13 displays the impacts of scam calls and texts on people's proclivity to screen the calls and texts they receive (i.e. to check the number before responding). The tendency broadly increases with age. The right panel suggests that scam texts are a contributing factor in young people losing trust in the security of texts and switching to alternative applications to send instant messages (IMs). It also shows that older people are likely to continue to be exposed to scam texts as they are less likely migrate away from text messaging onto other platforms, and continue to place reliance on the SMSs they receive (including scam texts).

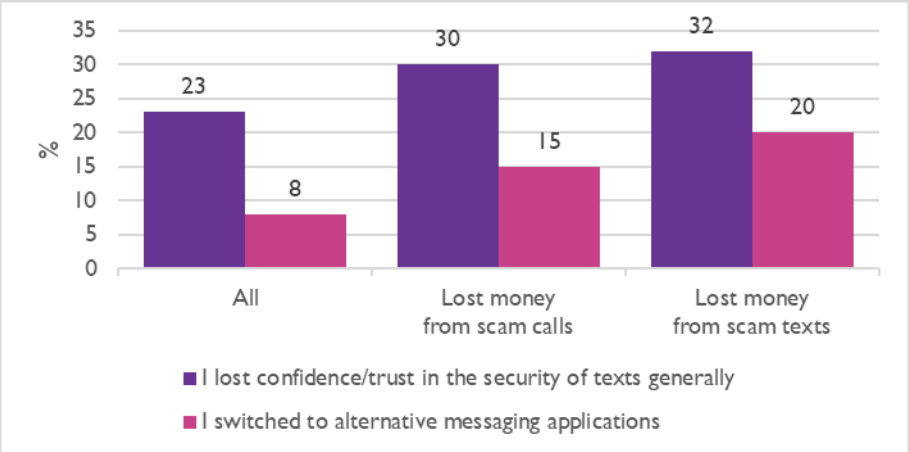
Figure 4.13: Trust and confidence impacts of awareness of scam calls and texts (% of respondents, by age)



Q.38 In relation to your awareness of scam calls and texts, has any of the following happened? Q.5 Main way of sending and receiving instant messages?

Figure 4.14 compares the impacts on trust between all respondents in the survey and those who lost money as a result of scam calls and scam texts. It shows that losing money from either type of communication can affect the level of trust people have in the security of texts. Whilst 23 per cent of adults have lost trust in texts generally, the figure increases to 30 and 32 per cent amongst people who lost money from scam calls and texts, respectively. Those who lost money are more likely to switch to alternative messaging applications when sending messages to others.

Figure 4.14: Trust and confidence impacts of awareness of scam texts (% of respondents, by money loss)



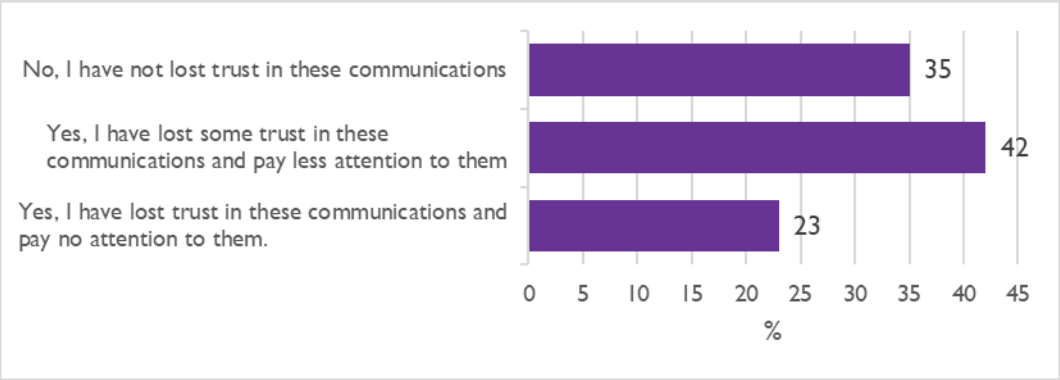
Q.38 In relation to your awareness of scam calls and texts, has any of the following happened? Base: All; and respondents who lost money.

Whilst trust in voice and SMS communications is important for the efficient functioning of communication in general, many organisations – public and private – rely specifically on these communications for providing their services. This can involve information/reminders about health appointments, banking and utility bills. Figure 4.15 shows that 42 per cent of adults that use any of these services have lost trust in these communications and pay less attention to them, and 23 per cent have lost trust and pay no attention to them. Overall, this suggests that 65 per cent of adults have lost trust in call/text information and reminders. This compares to relatively high levels of trust prior to waves of nuisance communications over the past two to three years. For example, at the start of 2021, only 10 per cent of consumers did not trust the Geographic location associated with the number.[90] Indeed, trust in geographic numbers was primarily related to

[90] ComReg: Review of the Numbering Conditions of Use and Application Process – Consultation – Document 21/28 - [online]

businesses being required to have a physical presence in the relevant geographic area. Scammers have taken advantage of this trust through fixed and mobile CLI spoofing as previously discussed.

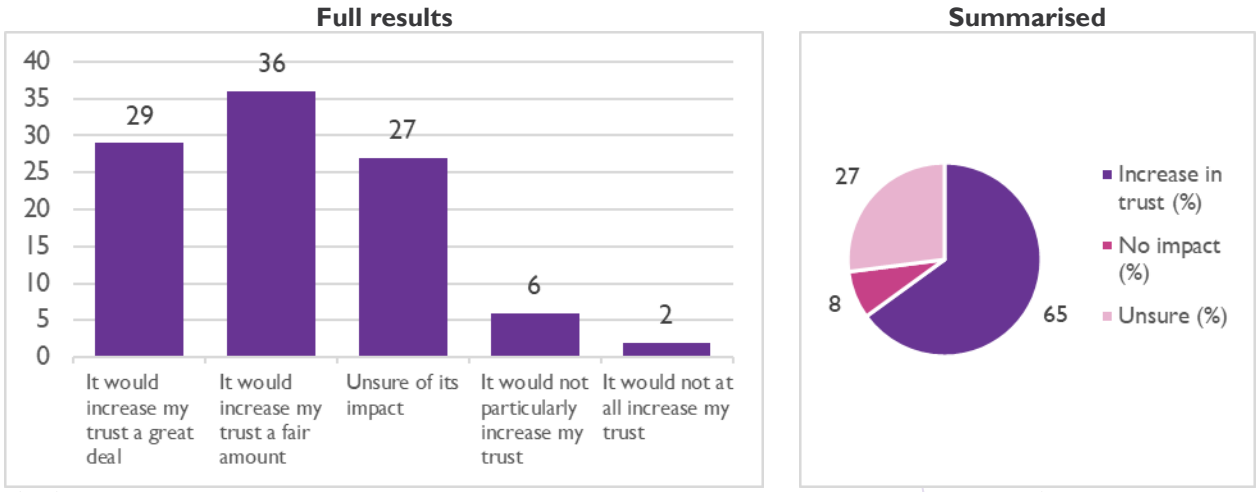
Figure 4.15: The effect on trust in communications from organisations that provide call/text services (e.g. notifications, reminders) (% of respondents)



Q.40c Has your experience of scam calls and texts affected your trust in communications from the organisations that provide the aforementioned services? Base: Respondents that use any service.

The impact of scam calls and texts on communications can also be shown by how many people would have more trust if a regulator were to intervene. Figure 4.16. shows 65 per cent of adults indicate that regulatory intervention would increase the trust they have in calls and texts. More than a quarter of adults would be unsure of the impacts, suggesting there is a strong case for any regulatory intervention in this area to be clearly explained.

Figure 4.16: To what extent would regulatory intervention impact the level of trust you have in calls and texts you receive in the future? (% of respondents)



Q.45 If regulatory interventions were made to block scam calls and texts, to what extent would this impact the level of trust you have in calls and texts you receive in the future?

Emotional harm

In addition to the monetised costs of harm caused to individuals, scam calls and texts impact upon people's wellbeing and emotional state. To illustrate this harm, we estimated the total number of annoying/irritating and distressing communications received as a result of scam calls and texts in the last year.

The survey results imply that there was a total of 89m annoying/irritating communications due to scam calls and texts in the last year. Following the same methodology and substituting with the share of communications that are 'distressing', the survey results imply that there were 31m distressing communications due to scam calls and texts.

A respondent in the consumer survey could indicate whether they found a given scam communication to be 'annoying/irritating', 'distressing', or both. This means that the numbers described above are not independent events and so should not be added together. We have not quantified this cost here but the large volume of annoying or distressing communications highlights the hidden harms caused by these types of communications.

A measure of harm through willingness-to-pay analysis

The harms quantified above each consider one contributory part of the overall detriment caused by scam calls and texts, but do not monetise all of them (in particular the emotional harm). Another but separate measure of this harm can be gained by considering the value consumers place on not receiving scam calls and texts. We have used willingness-to-pay (WTP) analysis for this purpose. This separate approach was used to add to the robustness of the overall conclusions on harm.

WTP analysis can capture some or all of harms – such as the risk of being defrauded, financial losses and emotional distress – in a single measure. A survey is used to elicit this values from respondents. What harms are included ultimately depends on the question that is asked of consumers, and what they factor into the value they provide. Respondents are effectively asked to weigh the value they place on the object – in this case, not receiving scam calls and texts – against all other expenditures, subject to their budgets.[91] The stated WTP is the maximum the consumers say that they are prepared to pay, and we assume that they would actually pay the stated amount.

A WTP question needs to define the 'payment vehicle' – the manner and timing of the hypothetical payment. This could be a monthly payment for a subscription, or a one-off purchase price, for example. The WTP approaches that we took and are reported below involve two payment vehicles:

- Product purchase: a monthly payment for a product that would stop all scam calls and texts received in the future. We consider this to represent a 'overall' WTP to avoid scam calls and texts.
- Scam calls and texts actually received: the total figure that a consumer would pay to not have received all the scam calls and texts they received in the past year. We consider this to represent a 'backward looking' WTP to avoid the time and emotional harm from scam calls and texts.

Importantly, our WTP approaches require the respondent to consider a hypothetical scenario where the payment guarantees that they would not receive the stated calls or texts. We assume that the relevant Irish adult populations would then pay the average values reported to estimate a nationwide measure of harm. The full details of the approaches are contained in the harms modelling appendix.

Product purchase: A monthly payment to purchase a perfect blocking product

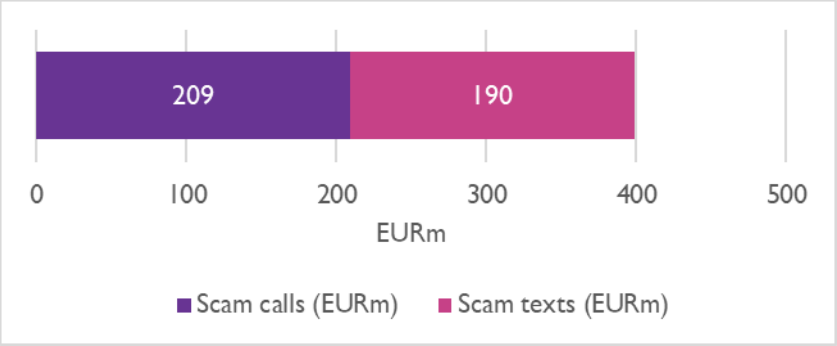
In this WTP approach, respondents were asked how much they would pay per month to not receive any scam calls or texts. It is therefore concerned with all the scam calls and texts they could potentially receive in the future, and how much they would pay each month for an unspecified length of time to avoid them.

Figure 4.17 shows the results of this analysis, based on adults in Ireland paying a median of €5 per month for a product to block all scam calls received on their mobiles and landlines and €5 per month to block all scam texts (both around €60 for the year). To put this into context, this would imply that the two blocking products are together valued at about half the average monthly mobile contract (€20.04[92]). Extrapolating to the relevant landline- and mobile-owning populations in Ireland, this implies that the overall harm caused by scam calls and texts was nearly €400m in the past year.

[91] Ofcom conducted Willingness-to-Pay analysis in its assessment of nuisance communications. See Ofcom (2015). 'Review of how we use our persistent misuse powers', Annex 7.

[92] Monthly average revenue per user (blended) mobile phone services, Q2 2022 [online]

Figure 4.17: Results of WTP – Product purchase method



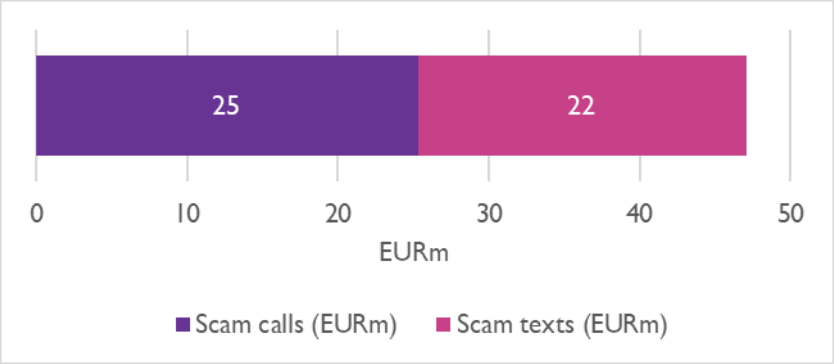
Source: Europe Economics analysis. Median value used.

An annual payment to not have received all the scam calls and texts received over the past year

In this WTP approach, respondents were asked to consider the scam calls and texts they *actually received* over the past year, and to state how much they would pay to not have received any of them. This question therefore aims to elicit the value of avoiding the experiences they actually had and the harms they incurred. We removed from our estimates any respondents who had actually been scammed in the past year, such that this figure can be assumed to represent largely the wasted time and emotional costs experienced by respondents.

Figure 4.18 shows the results of this analysis, based on adults in Ireland paying an average of €7.64 to not have received all the scam calls and €7.32 to not have received the scam texts they received in the past year. This implies that the emotional and time-related harm caused by scam calls and texts was just over €47m in the past year.

Figure 4.18: Results of WTP – Scam calls and texts actually received



Source: Europe Economics analysis.

That respondents were asked to isolate their valuations to their actual experiences over the past year could explain the lower values compared to the previous approach, in particular as these values do not include fears about potential losses from fraud, or expectations about increasing volumes of scams. This highlights that the way in which the WTP question is framed can impact upon how respondents answer.[93]

The backward looking annual payment method represents the more conservative estimate of harm and is more aligned with elements of the bottom-up modelling approach. This harm estimate from the product purchase approach ('overall WTP) provides a valuable upper-bound estimate of the future harm perceived

[93] A further payment vehicle was the subject of another WTP question in the consumer survey. It asked consumers to place a value on both their current mobile contract and one with guaranteed scam blocking. We had concerns with this approach, so we do not reported its results here. The details of this approach are in the harms modelling appendix.

by consumers based on their individual expectations of how scam calls and texts will evolve over time and indicates the potential magnitude of harm from scam communications.

Summary of harms to consumers

The results of our fieldwork shows evidence of significant harm to consumers from scam calls and texts. Using our bottom-up cost modelling approach, we have quantified harms totalling more than €150m for the year, including financial losses and the opportunity costs of wasted time engaging with scammers and of resolving any resulting issues. The financial losses from scam calls are almost double those from texts, even though the likelihood of being scammed via a call is lower than via a text, suggesting that successful scam calls can be very detrimental indeed. It also highlights the need to implement interventions that appropriately target both voice and text scams. If only voice interventions are used it is highly likely that scammers will simply increase the rate of spam texts which simply moves the harm across technologies. In order to reduce harm, interventions are required across both voice and text communications.

The bottom-up costs represent a conservative estimate, as these do not include any costs from emotional harm, nor other intangible costs such as loss of trust in voice and SMS services.

Our WTP approaches provide alternate estimates. The 'overall harm' WTP estimate of around €400m represents a more comprehensive value of harm, including for example the perceived costs to consumers of wasted time, emotional distress and annoyance, and actual and perceived losses from fraud. This therefore represents an upper bound to our modelled estimates. The 'backward looking' WTP estimate of €47m could be considered analogous to the bottom-up estimates of wasted time whilst also including a value for intangible emotional harm.

If we include alongside the bottom-up estimates of wasted time for *calls* the WTP backward-looking estimate for *texts* (to capture both wasted time and emotional harm), we arrive at €172m.

Table 4.3: Summary of quantified harms to consumers (€m)

Bottom-up cost modelling	Scam calls	Scam texts	Total
Financial losses from fraud	75	35	**109**
Opportunity cost of wasted time	40		**40**
Opportunity cost of resolving cases	0.8	0.2	**1**
Total monetised harm BUCM	**115**	**35**	**150**
Willingness-to-pay analysis			
Wasted time and emotional harm (WTP)	25	22	**47**
Overall Harm WTP estimate	209	190	**400**
Consolidated estimate			
Financial losses from fraud (BUCM)	75	35	**109**
Opportunity cost of wasted time (BUCM)	40		**40**
Wasted time and emotional harm from texts (WTP)		22	**22**
Opportunity cost of resolving cases (BUCM)	0.8	0.2	**1**
Total (consolidated estimate)			**172**

Source: Europe Economics analysis. Values may not add due to rounding. Note: BUCM = Bottom-up cost modelling approach

In addition, our fieldwork shows significant emotional harm (120m 'events' in a year), as well as loss of trust in calls and texts in a majority of respondents (65 per cent). There is clear evidence that regulatory intervention in this area would be valued by respondents.

In the following sections, we analyse the harm to businesses and public bodies from the prevalence of scam calls and texts, both as a result of being impersonated, and as a result of being directly targeted.

4.5 Harms to businesses

4.5.1 Existing evidence

There is some existing evidence of businesses being scammed in Ireland. FraudSMART (2022) reported on cases of scammers notifying firms that supplier payment details have changed and providing alternative details. It finds that there were over 100 cases of invoice fraud in the first half of 2022, and that the average business victim incurred a loss of €14,000 (but it ranged up to €50,000).[94] It also notes that firms in Ireland during that period were also exposed to the opportunism exhibited by scammers during the market exit of Ulster Bank and KBC. However, the source is not clear about whether such invoice fraud is committed via calls, SMS or some other medium, as it also suggests that scam invoices and payment instructions could arrive via letters and emails (e.g. phishing emails).

In 2020, the Gardaí reported that invoice redirect fraud or business email compromise fraud cost Irish businesses €10.5m.[95] In 2021 this figure fell to nearly €6m.[96] In both these cases, the Gardaí 's figures appear to be based on the attacks reported to it, and they explicitly relate to fraudulent invoices and payment instructions received by businesses via email.

In addition, businesses are affected by the general scam culture and by belonging to a set or business types that are regulatory impersonated by scammers. FraudSMART (2021) reports the results of a survey of 1,000 adults in Ireland in July 2021. It found that 36 per cent of people had experienced a scammer impersonating a bank, nearly 20 per cent a delivery company, and just over 10 per cent each for a retailer/online retailer and a software company.[97] According to that survey, 72 per cent of respondents contacted by scammers reported to have been contacted by phone and 32 per cent by SMS. In another survey of Irish consumers conducted by AIB, 33 per cent of people received a scam communication from a bank or financial institution they were not a customer of in 2021, and 30 per cent received one claiming to be a technology company.[98]

4.5.2 Fieldwork

Financial loss from fraud

The survey work conducted by B&A directly relates to fraud through calls and texts. Results from the business survey suggest that 5,100 businesses may have been the victim of fraud after receiving scam calls and texts in the past year. Respondents reported an average loss of €1,707. Assuming that none of this loss is recovered by businesses, we estimate the total financial loss to be €8.8m in the past year.

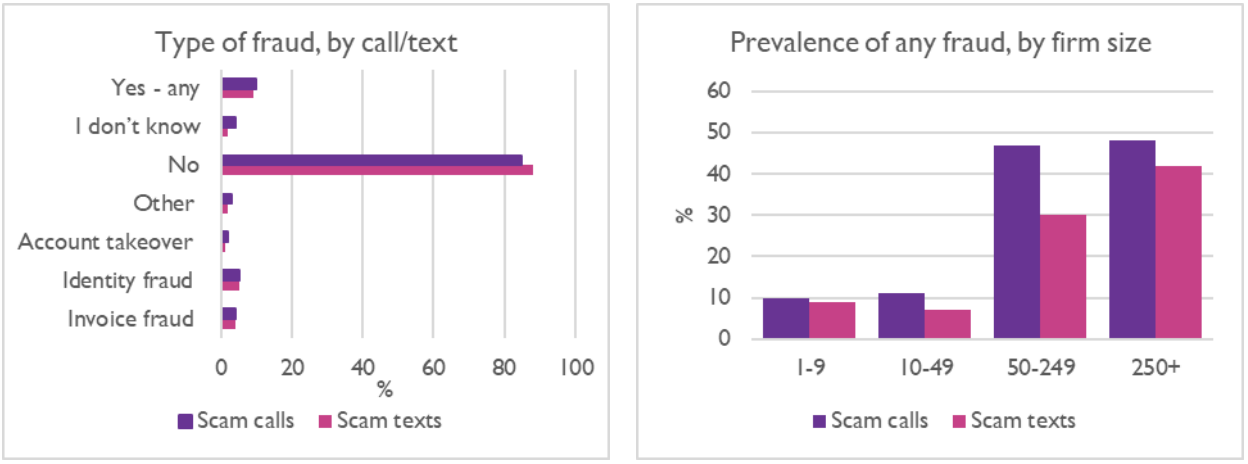
Figure 4.19 (left panel) shows that regardless of whether a firm received a scam call or a scam text, the prevalence of fraud seems to be similar and generally low compared to consumers. Around 10 per cent of firms stated that they experienced some type of fraud. Whilst this is a small share of the total number of firms, it amounts to about 30,000 firms across Ireland. Around 85 per cent of those that had received scam calls had not fallen foul to any of the listed fraud types, and the same was true for 88 per cent of firms that had received scam texts. This shows that firms that received scam calls/texts were generally unlikely to have been scammed by them.

The results also indicated that larger businesses, those with more than 50 employees, were much more likely to experience fraud from scam calls and texts (Figure 4.19, right panel). Over 45 per cent of businesses with

[94] FraudSMART (2022). 'Text message scams cost victims average of €1,700 in H1 2022 with businesses suffering average losses of €14,000 due to invoice fraud.' [online]
[95] An Garda Síochána (2021) 'Fraud Week - Invoice Redirect / Business Email Compromise (BEC) Fraud' [online].
[96] An Garda Síochána (2022) 'GNECB Fraud Awareness Week: Business Email Comprise Fraud' [online].
[97] FraudSMART (2021) 'FraudSMART Monitor', p.4 [online]
[98] AIB (2021) 'Four out of five people have been targeted by Fraudsters in the last year', p.1 [online]

50-249 employees experienced fraud from cam calls (30 per cent scam texts), and closer to 50 per cent of the largest businesses had experienced fraud from scam calls (42 per cent scam texts) in the past year.

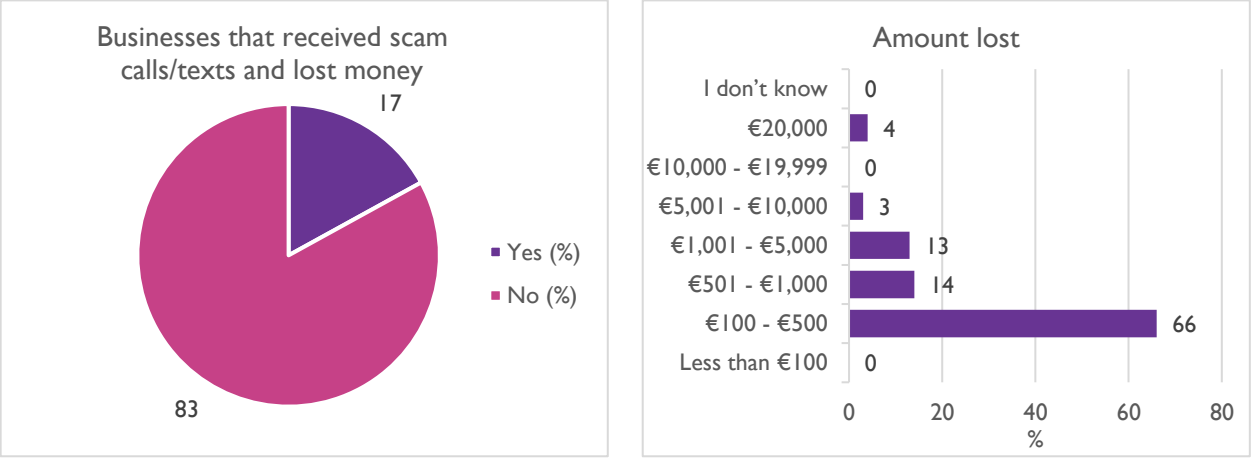
Figure 4.19 : Fraud from the scam calls/texts received in the past year (% of respondents)



Source: Europe Economics analysis of ComReg business survey. Q.6a Has your business been a victim of any of the following fraud as a result of a scam call in the past year? And Q.6b Has your business been a victim of any of the following fraud as a result of a scam text in the past year?

The businesses survey showed that 17 per cent of firms that had received scam calls or texts in the past year incurred a financial loss (Figure 4.20, left panel). Of these, the majority (66 per cent) incurred a loss in the range €100-€500. The mean loss during the past year was €1,707. Notable shares of firms also reported losing amounts of €1,001-€5,000 (13 per cent) and more than €20,000 (four per cent).

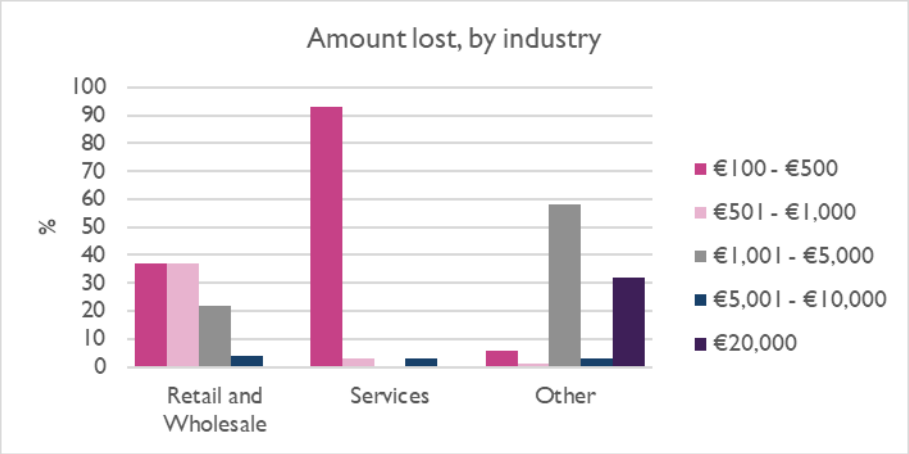
Figure 4.20 : Financial loss due to scam calls/texts in the past year (% of respondents)



Source: Source: Europe Economics analysis of ComReg business survey. Q.7a Has your business lost money in the last 12 months as a result of scam calls/texts you indicated previously? And Q.7b/Q.7c About how much your business lost in the last 12 months as a result of scam calls and texts.

Striking results are found between different firms. Some 93 per cent of firms in the services industry reported incurring smaller loses in the range €100-€500, whilst the losses among firms in the retail and wholesale trades were more evenly distributed across the ranges (Figure 4.21). We note that a small number of firms that identify being in some other industry reported a loss of more than €20,000.

Figure 4.21 : Financial loss due to scam calls/texts in the past year, by firm industry (% of respondents)



Source: Source: Europe Economics analysis of ComReg business survey. Q.7b/Q.7c About how much did your business lose in the last 12 months as a result of scam calls and texts? And Q.7b/Q.7c. Note for practicality, where businesses provided no responses, categories were removed.

Opportunity cost of time engaging with scam

Businesses lose time engaging with a scam call or text (i.e. answering the call, reading the text message, speaking to the caller). Based on the mean time spent engaging, we estimate an opportunity cost of this time at €1.7m in the last year.

Opportunity cost of time responding to customer queries regarding communication legitimacy

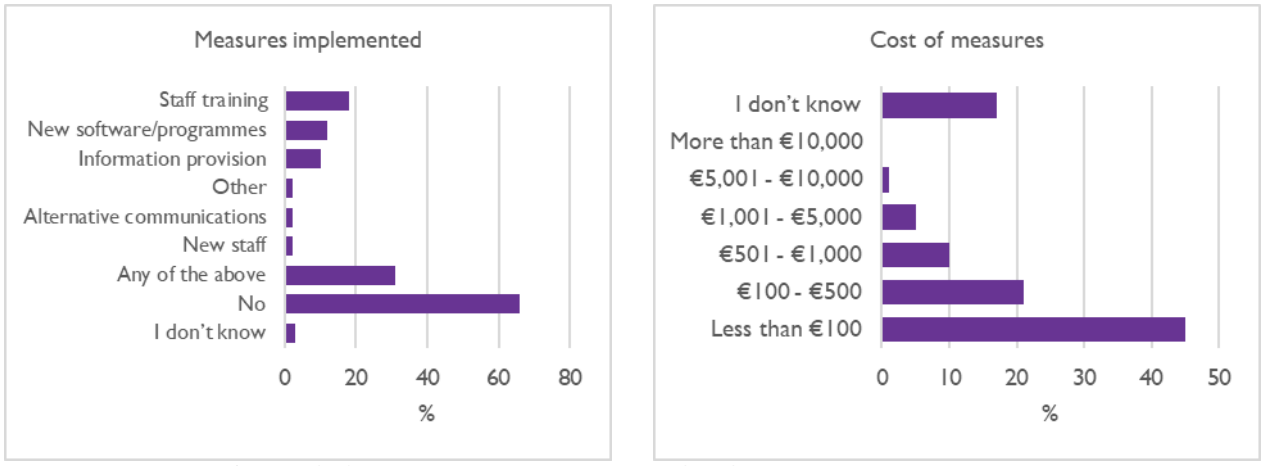
Many scam attempts on consumers involve the scammer impersonating an organisation. The consumer survey asked questions which captured how consumers would behave had they received a scam call/text from an organisation that had recently been impersonated. Unsurprisingly, some 50 per cent of respondents indicated that they would require some level of confirmation from the sender (such as identification or confirmation of consumers details)(see Figure 4.12). Businesses have also reported having to address customer queries regarding the legitimacy of their call and text communications as a consequence of this. This estimates the cost to businesses arising from consumers contacting them to confirm whether or not a call or SMS received by a consumer was valid or not. Based on the mean time spent on resolving customer problems caused by impersonation attempts, the opportunity cost of time responding to customer queries is estimated to be €21m in the last year.

Cost of scam-prevention measures

The volume and detrimental effect of scam calls and texts received by businesses has prompted some to implement measures to mitigate them (see Figure 4.22, left panel). Using the average total cost incurred by businesses to implement scam-prevention measures, the total cost across Irish businesses is estimated at €50m in the last year.

In response to scam calls and texts, the survey shows that 66 per cent of businesses have not implemented any scam-prevention measure and 31 per cent have implemented at least one measure. This could include new software/programmes, information produced and circulated, new staff, staff training or switching to alternative communications. The firms that have implemented measures reported an average cost of these measures of €519 over the past year (Figure 4.22, right panel).

Figure 4.22 : Scam-prevention measures to mitigate against scam calls/texts (% of respondents)



Source: Europe Economics Analysis. Q.10 Has your business put in place any of the following scam-prevention elements in the past year to reduce the amount of scam calls and texts it receives? And Q.11 Please estimate the approximate total cost of implementing the various scam-prevention elements over the past year. Including for example purchasing software, installation, staff time etc.?

In addition to implementing scam-prevention measures, firms have had to adjust specifically as a result of the impact of scam calls and texts on trust in phone networks. The survey shows that 13 per cent have been moving away from traditional telecommunication by reducing their reliance on public phone networks and SMS aggregators for contacting customers (i.e., the feedback effect referred to above), which should be concerning for operators and SMS aggregators.[99] Over a third (35 per cent) have increased their use of alternative methods of communication such as customer portals, web-based messenger apps and advertising through other channels. This shows the growing nature of scam culture affecting business decisions at all levels and ultimately on the effectiveness of the numbering platform.

Potential revenue impacts of scam calls and texts

The business survey also included questions aimed at understanding the value of telecommunications services to firms. The results indicate that 56 per cent of firms use mobile calls or texts for one part of their telecommunication strategy,[100] indicating that more than half of businesses surveyed are exposed to scam calls and texts. We also asked what proportion of revenue was generated or facilitated by mobile communication in the past year. The results indicate that a potentially high level of revenue is supported (Figure 4.23, left panel). On average, 10 per cent of revenue was supported in the past year by telecommunications amongst firms that use calls or texts for reminders and other services provided to customers. Accounting for the number of relevant businesses, if for illustrative purposes we were to apply this value to the average revenue of firms in Ireland,[101] this would imply that €48bn in revenue could be at risk due to scam calls and texts. (i.e., scammers are targeting a large pool of revenue – meaning that only a small number of successful scams are required for scammers to be profitable).

A further question asked firms about the extent to which they thought that revenue had been lost due to difficulties experienced by consumers not engaging with them via voice or text communications. More than a third of businesses indicated that 2.5 – 5 per cent of their revenue was lost to this challenge (Figure 4.23, right panel). However, around half of businesses also indicated that they either lost less than one per cent or did not know. The average indicated loss amongst responding firms was around four per cent. Again, if we were to apply this to the average revenue of firms Ireland, this would indicate an illustrative loss in revenue of €2.4bn due to scam calls and texts. This figure is subject to uncertainty, not least as it would be difficult

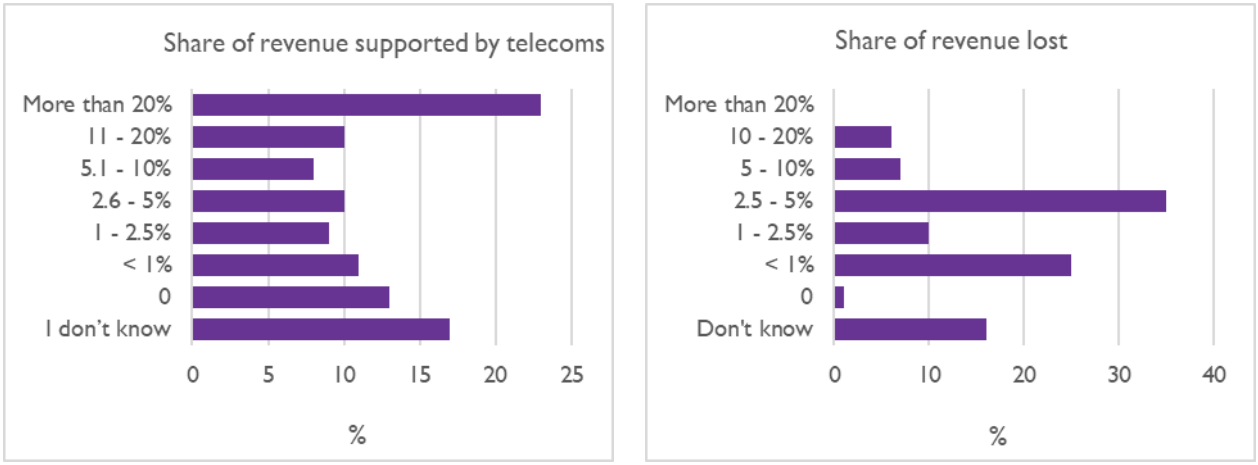
[99] Business survey. Q.22 As a result of the impact of scam calls/texts on consumers' trust in public phone networks, has your business …?

[100] Business survey. Q.19(a) Does your business use mobile calls (text) for any of the following parts of its telecommunication strategy?

[101] CSO, Enterprises in 'total business economy', 2020, Average turnover, uplifted to 2021 prices. [online].

for respondents to verify how much revenue they might have lost as a result of changing usage of calls and texts and to disentangle changes in revenue over a year from many other factors. It may also be that some of this 'lost' revenue is in fact earned through other channels. Nevertheless, this exercise provides a valuable illustration of the potential scale of harm to businesses from scam calls and texts.

Figure 4.23 : The share of revenue generated by telecommunications, and the share of revenue that may have been lost in the past year due to scam calls an texts (% of respondents)



Source: Source: Europe Economics analysis of ComReg business survey. Q.20 Approximately what proportion of your business revenue is generated or facilitated by mobile communication in the past year? And Q.25 Thinking of indirect costs, how much revenue do you think you may have lost in the past year as a result of consumers not engaging with you via voice or SMS communications?

Additional expenditure on contacting customers and arranging appointments and services

Businesses reported experiencing additional costs that they attribute directly to scam calls and texts. This includes difficulties trying to communicate with their customers, arranging appointments, arranging distribution and/or collection services, and receiving information and payments. Using the average direct cost for businesses that experienced this cost (€1,997), the total harm of this additional expenditure is estimated at €28m in the last year.

Cost of refunding consumers for their losses from fraud

As stated in section 4.4.2, consumers are sometimes able to recover some of the losses they incur after being a victim of fraud through scam calls and texts. We assume that this loss is recovered from the consumers' banks, rather than from the scammer or some other party (or that the fraudulent payments are stopped before the money leaves the bank). Hence, the refunded amount can be interpreted as a transfer of this share of the harm from consumers to banks. We calculated that the recovered losses to consumers in respect of scam calls and texts – and thus the reallocated harm to banks – was €21m in the past year.

Case Study 4.1: Costs of reprocessing funds

On top of bearing the harm of refunding consumers, our interviews with banks showed that they bear administrative costs of processing such refunds. We heard that processing a scam could be four-times the loss faced by the consumer, as it accounts for refunding the customer as well as other administrative work undertaken by bank staff.

We apply this rough approximation to the part of the consumers' defrauded loss that is refunded (€21m). Thus an illustrative estimate of the costs to processing refunds could be an additional €60m for banks. However we do not count this in our estimate as it is speculative in nature.

Case Study 4.2: Cost to banks having to respond to customer fraud alerts

Our interviews with banks found that banks typically engage both call centre and fraud team resources to deal with waves of scams. This case study is concerned specifically with the opportunity cost of time responding to customer queries regarding the communications they receive purportedly from banks. The interviews provided a case study of

a scam wave in which 10,000 calls were alerted to the bank's call centre, 400 of which were relayed to the fraud team.

Assuming that call handlers – both in the call centre and the fraud team – take 5 minutes to respond to each issue, we estimate a cost of €19,000 per bank per scam wave. If we were to scale this up to all banks in Ireland using an approximate market share of the bank from which this case study was drawn the cost multiplies to €57,000 per scam wave.

A measure of the total harm through willingness-to-pay analysis

The business survey included one question on the willingness to pay to avoid scam calls and texts. It asked how much firms would be prepared to pay, per month, for a product/service for its mobiles and landlines that guarantees to stop all scam calls and texts without having to take any further action. This question was asked of all businesses, regardless of whether they had received scam calls or texts.

Using the estimated number of businesses in Ireland and the median WTP amount (€10 per month), we estimate that businesses would pay €37m over the last year to avoid scam calls and texts.

Summary of harms to businesses

The results of our fieldwork show evidence of a broad range of harms from scam calls and texts befalling businesses in Ireland. We have quantified harms totalling €130m in one year , including financial losses from fraud, the opportunity costs of wasted time engaging with scammers and of responding to customer queries, the cost of implementing scam-prevention measures, and certain harms that are specific to banks given their relationships with their customers. The costs from wasted time is likely to be a conservative estimate as these do not include the other aspects of responding to scam calls and texts which also have a time-cost element, such as backroom administration, governance for implementing measures, or any staff training.

The WTP analysis for businesses is a useful sense-check of the bottom-up harm calculations. The median WTP of firms gives a total WTP of €37m, and we note that the monthly WTP amount (€10) is similar to the monthly WTP amount for the 'overall WTP' estimate for consumers.

The WTP concept is most useful amongst consumers who have full information about their ability to pay the values they provide (i.e. they know their income, their budgets etc). It is not clear whether all respondents in the business survey had comparable information about the businesses they represent (in particular as the values given were very similar to consumer values), and thus the WTP concept arguably less applicable to firms.

Table 4.4: Summary of quantified harms to businesses (€m)

Quantified harm	Total (scam calls and texts)
Financial losses from fraud	8.8
Opportunity cost of wasted time	1.7
Opportunity cost of responding to customers	21
Cost of scam-prevention measures	50
Cost of contacting customers, arranging appointments	28
Banks: Cost of refunding consumers for losses	21
Total monetised harm	**130.5**

Source: Europe Economics analysis. Values may not add due to rounding.

4.6 Harms to public bodies and regulators

4.6.1 Existing Evidence

Various surveys and news outlets have reported the likelihood of public bodies being impersonated by scammers. For example, FraudSMART (2021) surveyed 1,000 adults in Ireland and found that 56 per cent of respondents who had been targeted experienced spoofing of public bodies such as Revenue and the Gardaí.[102] The survey covered people targeted by phone, text and email. According to a survey of Irish consumers conducted by AIB in 2021, 22 per cent of received scam texts claimed to be from the Revenue.[103] A wave of calls purporting to originate from the Department of Social Protection and the HSE was recorded in late 2021.[104]

This pattern has been echoed by recent crime statistics. In June 2022, the CSO announced the near-doubling of fraud crime in the year to March, to approximately 17,000 incidents.[105] This increase was driven in most part by unauthorised transactions and attempts to obtain personal or banking information online or by phone. There has been a marked increase in the number of people being arrested for fraud in Ireland: from 30 or fewer in the years 2012-2018, to lurching upwards to 232 in 2019.[106] These figures have continued to climb, reaching a peak of 519 in 2021, partially due to improved fraud awareness amongst the public. These figures suggest that the total costs of investigating and prosecuting fraud cases is growing, too.

In addition, ComReg as a public body will also incur costs relating to scam calls and texts such as dealing with complaints. We understand from ComReg that it does not track the volume of customer complaints related to scam calls and texts specifically. However, it does track the volume of 'nuisance communications issues reported' more generally, which it collects through its social listening, stakeholder feedback and the number of queries it receives at its contact centre.[107] Whilst this metric includes nuisance communications beyond scam calls and texts, (e.g. email phishing), it shows that customer complaints has been on an upward trend since at least Q3 2020. The reported volume peaked at 249 in Q4 2020 and at 317 in Q2 2021. The consumer survey suggests that just 3 per cent of consumers typically report suspected scam texts to ComReg.[108]

4.6.2 Fieldwork

Results from interviews

We interviewed a handful of public bodies, HSE, An Garda Síochána and An Post, and regularly discussed the wider issues of scam calls and texts with ComReg. This gave us a valuable insight into the range of problems faced by public bodies in Ireland as they grapple with scam calls and texts.

It is not possible to estimate more than a small fraction of the harm to public bodies from scam calls and texts, given the time and resources available. This arises due to the inability to survey the harm for a sample of public bodies and extrapolate to the wider public sector – as the harms and organisation are all different and unique. Therefore, our estimated harm is used to illustrate that even a fraction of the harms suffered by a handful public bodies can be considerable.

All the representatives we interviewed agreed that scam calls and texts have changed the way their organisations operate. An Post, for example, emphasised that its texts never carry website links, noting the

[102] FraudSMART (2021) 'FraudSMART Monitor', p.4 [online]
[103] AIB (2021) 'Four out of five people have been targeted by Fraudsters in the last year', p.1 [online]
[104] O'Riordan, E. (2021) 'Scam calls are on the rise: what should you do if a fraudster rings?', *The Irish Times* [online].
[105] CSO (2022) 'Press Statement Recorded Crime Quarter 1 2022' [online]
[106] The Journal (2022) 'WhatsApp scam crops up in Ireland as new figures reveal a surge in fraud arrests' [online]
[107] Note that in situations where a consumer contacts ComReg several times about the same case, this is only counted once. These statistics also potentially include email related scams in addition to voice/text.
[108] Consumer survey. Q.31 What do you typically do when you receive a suspected scam text?

opportunity this would give scammers to impersonate these texts with links to fraudulent websites. One of the case studies, below, is about how the Gardaí has needed to adapt its counter-scam enforcement arm.

The Gardaí drew our attention to the resource-straining impact of scam communications. The Garda National Economic Crime Bureau (GNECB), which is responsible for investigating scams, has faced increased resource pressures in the wake of the recent uptick in scam cases in Ireland. But regular Garda are involved in device seizures and registering complaints at local stations, which leads scams to divert resources away from other important issues. The opportunity costs of such resource diversions in terms of investigations into other criminal activity is potentially very high.

The interviewees noted that their organisations had created material for their service users, in an attempt to shore-up trust in their communications and communications more widely. When a new variation of call/text scam emerges (e.g. ones for COVID boosters), the Gardaí's GNECB warns the public about it through information campaigns. The GNECB emphasised the concern that some callers claiming to come from a bank actually are (i.e. insider criminals). An Post has created an online Security Hub to offer information about scams, and its direct mail campaign (one of the case studies) was intended to inform the public about scams and maintain their trust in legitimate communications.

A theme identified in our case studies based on the interviews is the impact on trust. This was clearly an important issue for the organisations we interviewed, who emphasised the importance of their mobile communications with service users. The HSE's use of texts grew exponentially over the pandemic (the same time that scam texts also grew in prevalence); texts have been the only channel capable of facilitating certain activities, e.g. organising appointments and vaccinations. HSE stated that the first minute of a call with a service user is often occupied by having to dispel any fears about the caller's legitimacy. This wastes time and caller resources. One of the quantified examples for HSE is about the impact of trust amongst HSE's own staff.

Quantified examples

Estimating country-wide harms to public bodies was not possible in this study as public bodies are unique with many unique harms, and thus extrapolating estimates from our fieldwork was not feasible (in the same way that we were able to do for consumers and businesses). In addition, there is limited data available on harms to public bodies, such that our estimates are illustrations only of selected harms, and our aggregated figures should be considered only partial estimates of harm. These estimates are our own, informed by our discussions with the organisations listed rather than provided by them.

The following presents several case studies to illustrate the range of harms borne by public bodies. Details are contained in the Appendix.

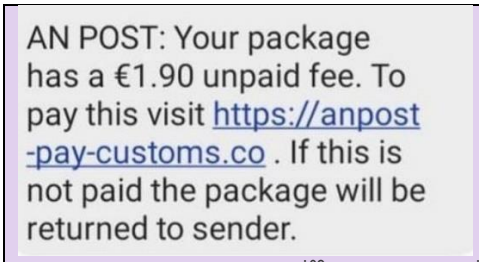
An Post

Case Study 4.3: Direct mail campaign

An Post is the state-owned provider of postal services in Ireland. An Post provides postal services to the whole of Ireland as a member of the Universal Postal Union. Services provided include letter post, parcel service, deposit accounts, Express Post, and Express mail services.

Evidence from our interview with An Post indicates that the majority of its communications with customers are conducted via SMS and emails. Since Brexit, the completion of a customs declaration and a payable charge have been introduced for goods sent between Ireland and the UK. To bring customers up to speed with this change, An Post increased its communication with customers, largely through SMS, postcards and emails. It has since received a growing number of complaints from customers reporting fraudulent scam texts attempting to impersonate An Post. See 'Opportunity cost of time responding to customer queries regarding communication legitimacy' above.

The picture below provides an example scam text Irish households received where they were prompted to pay a customs fee:



Source: Garda Síochána Donegal[109] and Irish Mirror.[110]

The prevalence of scam calls and texts has impacted An Post in a number of ways. For example, the customs charge has affected the Bank of Ireland because people paying those charges are often customers of the Bank, and this has required collaboration with the Bank to avoid customer scams. Its call centres have received various complaints about scams. As a result, An Post now takes a more proactive approach, letting customers know what it would and would not do (e.g. not sending links sent in texts). An Post suggested that this caused it to incur opportunity costs: the decision to remove weblinks from SMS messages might not have been taken as quickly in the absence of scams.

One activity An Post has carried out was a campaign of sending a direct mail to every household in Ireland warning about the dangers of scam calls and texts.

An Garda Síochána

Case Study 4.4: Costs of personnel

An Garda Síochána is the national police service in Ireland. It is responsible for carrying out all policing duties in Ireland, with the addition of providing state security services and enforcing all criminal and traffic law enforcement. Our interview with An Garda Síochána raised the concern that increased scam activity seen of late has resulted in an increased demand for personnel within the specific fraud team we spoke to, the Garda National Economic Crime Bureau (GNECB). The GNECB suggested that an additional dedicated sergeant and five fraud analysts would be required to deal with the additional workload in the department.

[109] Garda Síochána Donegal (2022). [online]
[110] Irish Mirror (2022). 'Gardai warn of An Post scam targeting online shoppers as they reveal the simple trick used by fraudsters'. [online]

Health Service Executive (HSE)

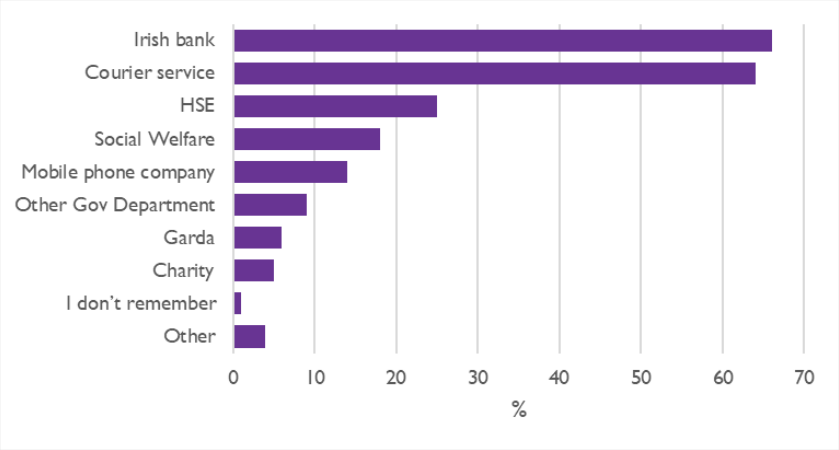
Case Study 4.5: Increased operating costs due to Did Not Attends

The HSE is a state owned and funded health care system which is responsible for the provision of health and personal social services in Ireland.

Our interview with the HSE indicated that health care providers can incur costs from excessive numbers of missed appointments (DNAs). We estimated this cost by relying on assumptions in published research that text reminders sent to outpatients can reduce the number of DNAs. Hence, if scam texts reduce public trust in telecommunications, it is possible that scam texts erode the trust placed in appointment text reminders, too. The consumer survey provides estimates for this effect. Crucially, this approach assumes that the erosion of trust in texts caused by scam communications translates directly into outpatients ignoring their text reminders and not attending their appointments (thus eroding cost savings of the reminders).

Figure 4.24 shows the share of different organisations impersonated as a result of scam texts received by survey respondents in the last year. Some 25 per cent of respondents indicated that they received a scam text impersonating to be HSE.

Figure 4.24 : Share of different organisations impersonated in scam texts (% of respondents)



Source: Europe Economics analysis of ComReg consumer survey. Q.27b Which organisations have they impersonated in the texts to you?

Case Study 4.6: Increased operating costs due to HSE's cybersecurity measures

Our interview with the HSE highlighted that it faces increased operating costs due its cybersecurity measures. Over the recent years, HSE indicated that its staff had experienced increased scam calls and emails. In an attempt to mitigate this, HSE has channelled major investment in personnel and projects to improve cybersecurity. This includes the appointment of a Chief Cybersecurity Officer and the training of HSE staff. One initiative used has been to send dummy scam calls and phishing emails. HSE employees who answer calls and click on the weblinks are then later referred for training to help them recognise cyber scam attempts.

Case Study 4.7: Increased cost of time responding to HSE staff queries about texts

Given the general scam culture, employees are likely to be cautious when receiving texts from their organisations, particularly if the organisations run regular scam awareness training. The HSE gave an example of a recent project to upgrade HSE staff phones to the latest software. This involved the HSE's provider communicating with the staff who used the c.5,000 phones, but a number of staff rang HSE to check that the provider's communications were legitimate. Whilst HSE note that only a 'small percentage' of staff might react this way, it would only take 1 per cent of recipients to a bulk campaign of 5,000 texts to place a burden on internal communications staff in dealing with their queries.

The table below summarises the illustrative harms to some public bodies from scam communications, which aggregate to €7m. As noted earlier, these represent only a fraction of the likely harms to public bodies.

Table 4.5: Summary of selected harms to public bodies from scam communications

Public body	
An Post – mail campaign	
An Garda Síochána – personnel	
HSE - DNAs	
HSE – cybersecurity measures	
Aggregated partial harms	€7m

4.7 Harms to operators

4.7.1 Fieldwork

Results from interviews

The two main harms identified by operators were (i) commercial harm caused by lack of trust in numbers and (ii) reputational damage caused by volumes of scam calls and texts. Operators noted that interventions to curtail fraudulent communications could increase trust in mobile numbers, and also suggested that there was scope for operators to benefit commercially from being able to offer networks of trust.

It is not possible for us to estimate the harm suffered by operators from scam calls and texts, given the limited data available. This arises due to the difficulties in estimating the damage to an intangible asset like a brand. Similarly we are unable to estimate revenues deriving from scam traffic specifically. Therefore, our discussion of the harms to Irish operators is qualitative and does not come to any firm conclusion as to the net effect of scams on operators.

While we cannot measure the net harms to operators from scam calls and texts, any such harms in the short run appear to be dwarfed by the harm to Irish consumers, businesses and public bodies. This creates what is known as a "negative externality", whereby the relevant actor lacks sufficient incentive to invest the social optimal amount in tackling a problem as they do not bear the full benefit (cost) of their action (inaction). While it is beyond the scope of our work to predict operators' future actions – we are assessing the benefits of the interventions to consumers and businesses – we consider this worth bearing in mind.

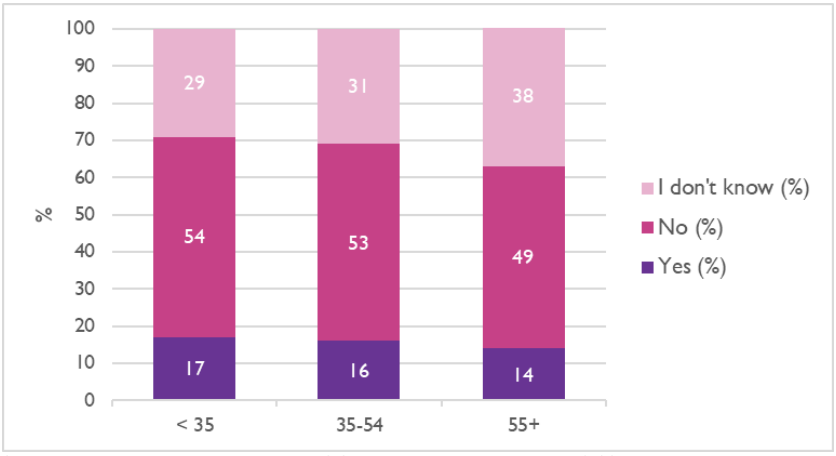
Our analysis suggests that operators may not face sufficient incentive in the short run to invest their capital to fully combat scams and save trust in their Voice and SMS services. Any delay in investment entails unnecessary harm to consumers and businesses as well as a reduction in the benefits of SMS and Voice as many switchers may not return. Therefore, even were operators to act eventually it appears that regulation may bring additional benefits from making such interventions sooner.

Insight from surveys

The consumer survey asked respondents whether they thought that their operators had done enough to protect them from scam calls and texts. The results from this means that it is possible to get a sense of the scale of the need for action, as well as the expectations of consumers on their operators.

Figure 4.25 shows the results by broad age group. Overall, just 16 per cent of respondents thought that their operators had done enough; 52 per cent thought not.

Figure 4.25: Share of respondents reporting that their mobile operator has done enough to protect them from scam calls and texts, by age group

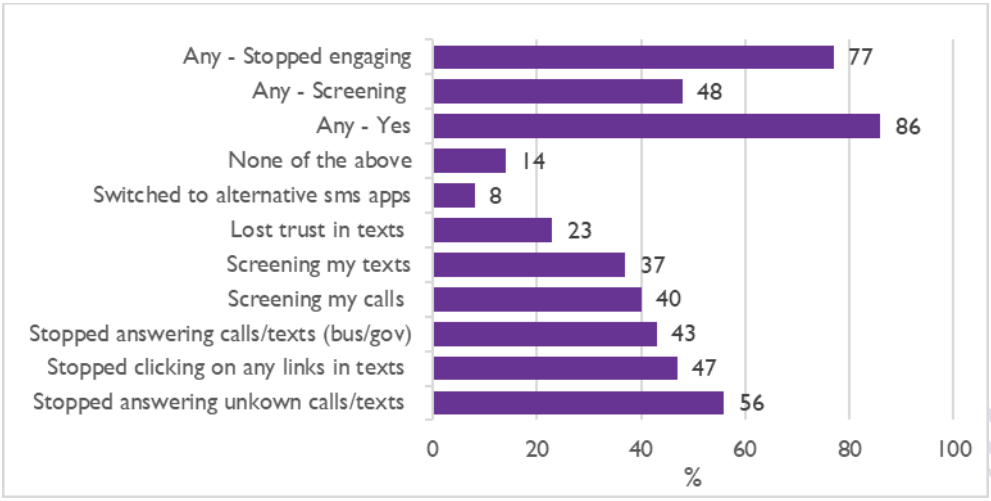


Source: Europe Economics analysis of ComReg consumer survey. Q44. Do you think your mobile service provider has done enough to protect you as a consumer from scam calls and texts?

The consumer survey found that 77 per cent of consumers have stopped engaging with calls and texts in some way (Figure 4.26). This includes not answering calls/texts from unknown numbers, not answering communications claiming to be from businesses of public bodies, and not clicking on links. Generally, consumers have shown a significant shift in behavior, with 86 per cent of respondents indicating that they have at least taken one of the approaches when engaging with incoming calls and texts. This is further indicative of a wider impact on trust affecting telecommunications which directly impacts on operators. However, just eight per cent stated that they had switched to alternative messaging applications.

We also note that temporary switching behaviour may become permanent, for example consumers migrating to alternative messaging providers (e.g. OT providers like WhatsApp) may remain there even after scam SMS issues are remedied. This highlights the importance of timely action to address scam communications. Further, migration in one channel (messaging) could lead to migration in another (to continue our example, once using WhatsApp messaging the consumer may also use WhatsApp calls).

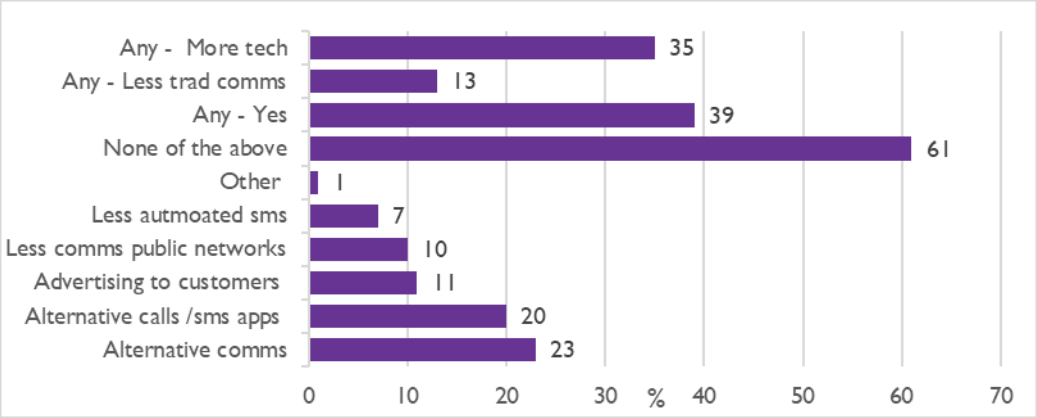
Figure 4.26 : Changes made by consumers due to their awareness of scam calls/texts (% of respondents)



Source: Europe Economics analysis of ComReg consumer survey. Q.38 In relation to your awareness of scam call and texts, has any of the following happened?

The businesses survey also asked respondents the impact scam calls and texts had had in the past year and actions they had taken to combat these issues. Figure 4.27 shows some loss of trust and move away from traditional telecommunications services, for example the use of fewer automated texts, and using alternative call or messaging platforms.

Figure 4.27 : Changes made to increase consumer trust in public phone network (% of respondents)



Source: Europe Economics analysis of ComReg business survey Q.22 As a result of the impact of scam calls/texts on consumers' trust in public phone networks, has your business?

4.8 The total harm in Ireland

Consolidated results of our modelling to present an overall figure of harm

The results presented in the previous subsections provide a range of estimated harms from scam calls and texts. Consumer harm is estimated at €172m, a conservative blend of our bottom-up cost modelling and elements of our willingness-to-pay analysis, with a further estimate of €400m as a broad upper bound. Harms to businesses are estimated at €130m, along with unmonetized impacts on revenues. A selection of harms to public bodies are estimated at €7m, representing only a fraction of harm.

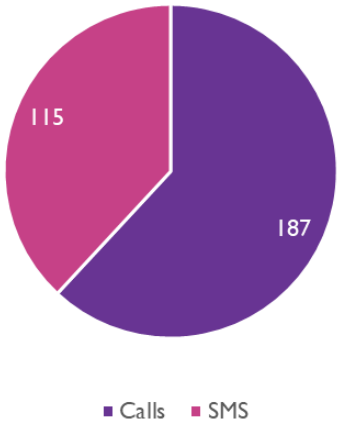
Figure 4.28: Summary of harm from scam communications in one year

Consumers €172m	Businesses & Public bodies €137m
• Financial losses - €109m • Time resolving fraud - €1m • Wasted time engaging with scam calls - €40m • Wasted time and emotional harm from scam SMS - €22m • *Alternate upper bound of €400m (WTP) including intangible impacts on wellbeing*	• Financial losses - €8.8m • Costs of lost time- €1.7m • Costs of responding to customers - €21m • Increased operating costs - €50m and €28m • Refund costs - €21m • Public sector case studies (HSE, Garda, An Post) ≈€7m • *Unmonetised impacts on business revenue and public body costs*
€309m total harm across Ireland	

Source: Europe Economics analysis. Values may not add due to rounding

Harms to consumers and businesses can be broadly split between calls and texts, as shown in the figure below.

Figure 4.29: Split of consumer and business harm between calls and SMS in a year (€m)



Source: Europe Economics

The harms we have quantified are those for which we have been able to identify sufficient data. As Chapter 3 shows, it is possible that many other harms exist and could be quantified given the right data. The surveys provided valuable – and unique – insight into the harms faced by consumers and firms in Ireland, but do not cover all types of potential harm.

4.8.1 How the harm might evolve

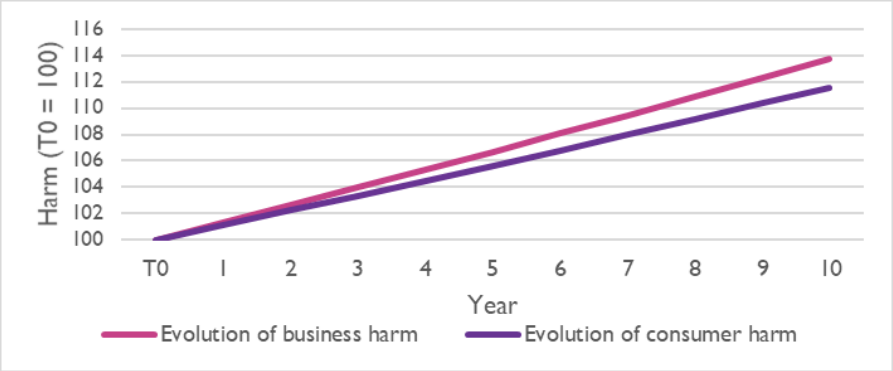
The harm from scam calls and texts is unlikely to remain static over time in the absence of any intervention. As a central scenario, it is likely that as the population grows the prevalence of consumers and businesses being exposed to scam calls and texts will also grow. In a high-growth scenario, scammers would become increasingly opportunistic and aggressive in the volumes of scam calls and texts they make and in the nature of the scams. In a low-growth scenario, consumers may become increasingly savvy at identifying and avoiding scam calls and texts (and assuming that scammers are not commensurately able to increase the effectiveness of their scams).

For the purposes of our cost-benefit modelling, we assume a central growth scenario, based on CSO statistics for population and business growth.[111] This counterfactual implicitly assumes that developments in either the ability of consumers/businesses to avoid scams, or the ability of scammers to outwit consumers, balance each other out such that the prevalence and impact of scams grow linearly with population growth. Other growth scenarios are addressed in the Appendix.

Figure 4.30 plots the evolution of consumer and business harms over a 10-year horizon. We have indexed the euro amount in millions from T0.

[111] For consumers, we use the 11-year compound average growth rate of persons over 15 in Ireland between 2021 and projected in 2031, 1.1%. For firms, we use the 11-year compound average historical growth rate of enterprises in Ireland over 2010-2020, 1.3%. These growth rates are assumed to reflect the annual growth over the next 10 years. See CSO, cited in Pensions Committee (2021) [online] and CSO 'Business Demography 2020' [online]

Figure 4.30: The evolution of harms to consumers and businesses in the baseline counterfactual (T0 = 100)



Source: Europe Economics analysis. Note: T0 refers to the year for which the harms are calculated in Chapter 4.

5 Interventions to Combat Scam Calls and Texts

There are a number of technical interventions that can be applied to tackle scam calls and SMSs. The interventions covered are:

Voice interventions:

- Do Not Originate (DNO) database
- Protected Numbers list
- Fixed CLI Traffic Blocking
- Mobile CLI Traffic Blocking
- Voice firewall

SMS interventions:

- Full or partial Sender ID registry.
- SMS scam filter.

What follows is a summary of each intervention, covering an overview of the intervention, affected stakeholders, and implementation in other jurisdictions. We also summarise the impacts of the interventions in addressing scam communications, including the drivers of harm they each address, their likely effectiveness and costs. We begin with a summary of the main ways in which scam calls and texts are made.

5.1 Summary of main scam call and text types

5.1.1 Call Line Identification spoofing

Call line identification (CLI) spoofing is where a scammer intentionally changes their CLI in an attempt to deceive the call receiver that they are calling from a number which may be more trusted. The CLI is the number, or non-numeric code (e.g. a company name), that appears on phone screens when a call is received. Individuals may be more likely to fall for scams if they believe that they are being called from a trusted organisation, such as a bank, HSE, Revenue etc. Many scam calls to receivers in Ireland originate abroad. The callers spoof their CLI with an Irish number to make receivers believe that they are being called from a trusted, Irish source. CLI-spoofed calls can be received by both fixed line phones and mobiles.

Interventions targeting this type of scam are the Do Not Originate (DNO) database, Protected Numbers list and CLI Traffic Blocking. The CLI Call Blocking & Screening interventions would be operated via international gateway operators, which would identify and block illegal calls from entering Ireland.

International calls purporting to originate from Irish fixed line numbers would generally be blocked.

International calls purporting to originate from Irish mobile numbers would checked with the Mobile Network operator as to the roaming status of the user as indicated by the CLI and the call would be blocked if not coming from a genuine roamer.

Voice firewalls represent a state of the art intervention whereby incoming calls are analysed against a set of rules to ascertain their legitimacy.

5.1.2 Spoofed SMSs, or 'smishing'

Smishing occurs when scammers use SMS messages to fish for personal information. Scammers attempt to dupe individuals by sending them texts often using an edited sender ID, which may give the impression that the SMS is from a trusted source. Consumers may be more likely to fall for scams if they believe that messages are from a trusted, Irish source.

SMS scams have evolved, and many now contain a link that, when followed, takes individuals to what they believe is the website of a trusted organisation. The website then prompts the individual to input personal details which can then be used to gain access to personal accounts and commit fraud. SMS scams can also contain malware that infect the recipient's phone to make it become the source of multiple further scam texts. Those messages may also contain a link which continues the malware infection-message cycle. Mavenir suggests that an infected phones can send 500 to 5,000 scam massages a day.[112]

Interventions targeting these types of scams are the Full sender ID screening (Basic firewall), and Anti-malware Content Scanning, URL Detection & Classification, and Content Filtering (Advanced firewall) interventions.

5.2 Voice call interventions

5.3 Do Not Originate (DNO) database

5.3.1 Description

The Do Not Originate (DNO) database is a database that contains phone numbers which cannot be used to originate calls. These numbers are used to receive inbound calls only and are associated with trusted organisations such as banking, parcel delivery services, police, Revenue, DSP, HSE.[113] A call made from one of these numbers – whether from abroad or within Ireland – would not be legitimate and thus likely to be a scam. The intervention allows operators to identify and block calls originating from DNO numbers, therefore preventing one avenue of potential scams.

The database of DNO numbers would require initial set-up by ComReg. Operators would need to set up mechanisms to regularly update their call blocking facilities with new DNO numbers. Operators' call-blocking facilities could consist of switch analysis/blocking tables or a voice firewall (described in a later section). However, the precise nature of the call blocking technology used would be dependent on each operator's network setup. Other stakeholders impacted by this intervention would be businesses and government organisations, who would be required to notify ComReg of the numbers they wished to add to the DNO database.

The UK, Australia, and the US are known jurisdictions where the intervention has been implemented. [114,]

5.3.1 Impacts

The drivers of harm it could address

This intervention would prevent Irish businesses and residents from receiving scam calls from numbers they (think they) recognise as belonging to Irish public bodies and well-known companies. Call recipients would

[112] Mavenir (2022) 'Mavenir Fraud Management and Security Suite', p.11.
[113] NCIT (2022) 'NCIT – Progress Report after 6 months', p.6.
[114] ACMA (2019) 'ACMA recommends immediate action to combat scams' [online]

thus not be misled into thinking they were receiving a legitimate call and into providing personal or financial information which could be used in a scam.

As CLI spoofing largely involves scammers using numbers from well-known public organisations and businesses such as banks, couriers, public services and government agencies, this intervention could also help combat a loss of trust in these numbers and lead to greater ability for the organisations to connect with customers and citizens. There may be spillovers from this, in that even organisations that do not submit numbers to the DNO list benefit from an improvement in public trust in all voice communications.

Effectiveness

The intervention has the potential to be dynamic but only to the extent that the composition of numbers on the database can change over time. This would require constant vigilance in identifying the numbers to add to or remove from the database, and can therefore only adapt to evolving threats through direct human intervention. For this reason, the DNO database intervention is considered 'static'. It is also only as effective as the reach of the DNO list – all other numbers not included in the list would remain candidates for spoofing. It also relies on organisations coming forward to place their numbers on the DNO list.

The DNO database is one of the interventions that would be capable of blocking scam calls that originate domestically or transit into the State (being applied by IGOs also). This hedges against the risk that such domestically-originating scam calls increase in volume in the future.

The intervention has proved effective in other jurisdictions such as the UK, with the NCIT report highlighting a 97 per cent reduction in scam reports related to HMRC after different fraud protection measures, such as the DNO list, were put in place.[115] In the first month of the UK DNO database, reports of HMRC spoofed calls fell by 25 per cent compared with the previous month, and a further 23 per cent in the second (i.e. a reduction of 42 per cent in two months).[116, 117] Moreover, Singapore, Australia and the US have implemented a DNO list which suggests that other jurisdictions also believe that it could be an effective fraud protection measure. In 2016, the FCC in the US found that a DNO list was deemed effective after having blocked 90% of spoofed inbound-only calls.[118]

The DNO list is unlikely to reduce the number of scam calls significantly in the Irish context. The list is likely to be relatively short, thus scammers will have multiple other CLIs to spoof. We understand from operators that the vast majority of scam calls present with spoofed CLIs and originate internationally.

Scammers may be able to evade this intervention in the medium term as they become aware of the sorts of numbers on the DNO database. When this happens, they will likely switch to using other numbers that are less likely to be nominated to the DNO database (such as those of other organisations and those of ordinary citizens) and which therefore cannot be blocked with this intervention. This could affect the longevity of this intervention.

Costs

ComReg would incur costs of staffing from the setup of the DNO database and from the establishment of associated processes and procedures.

Operators have stated that implementation is straightforward and low cost.. Some operators may have call blocking technology that enables them to more rapidly implement the actions required by the DNO database,

[115] See https://www.gov.uk/government/news/scam-hmrc-call-reports-drop-by-97

[116] Which (2019) 'Who's really calling you? An investigation into the worrying rise of 'number spoofing'' [online].

[117] More recently, Ofcom in the UK has introduced rules requiring operators to run 'know-your-customers' checks on business customers. TalkTalk, one of the companies to take part, reported a 65 per cent reduction in complaints about scam calls since it introduced the measures. FT (2022) 'Regulator orders 'number spoofing' crackdown to combat fraud' [online]

[118] CALLTRANSPARENCY (2017). 'Protect Your Inbound Lines from Spoofing' [online].

whilst others may need to update theirs. Operators that cannot upgrade their systems may look for wholesale/'white-label' services that can provide the necessary functions.

Ongoing costs would be incurred by operators as they update their blocking facilities to accommodate numbers as they are added to the DNO database. These costs may be minimal if efficient processes are in place.

Monitoring metrics

The success of this intervention may be measured by recording the number of calls operators have blocked based on its cross-referencing with numbers on the DNO list. We understand that creating the systems to monitor the number of calls blocked may create some costs for operators but again these would be minimal

5.4 Protected Numbers list

5.4.1 Description

A protected numbers list is a database which contains number ranges, sub ranges and individual numbers that have not yet been allocated, or have been withdrawn, by the communications regulator. A call that presents as being from any of these numbers is therefore illegal, regardless of where it originates. Operators would be able to identify whether calls are attempting to originate from these numbers which could, in turn, allow them intercept potential scam calls before they reach consumers and businesses. The interception in this intervention could result in blocking calls presenting with CLIs on the list.

This intervention could be enhanced with the addition of other types of numbers, such as non-geographic numbers (NGNs; e.g. 1800 or 0818), or premium rate numbers (e.g. 1550), since these should not appear as the CLI on any calls. It could also include any number that does not have the correct number of digits, including mobile voicemail numbers which have eight digits (i.e. mobile numbers prefixed with 5, e.g. 0875XXXXXX).

The technological requirements, and the costs of set-up and upkeep of this intervention, for the regulators and operators, are understood to be low, and the overall mechanism similar to that required for the DNO intervention. The key difference between these two measures is the method in which the numbers for the database are obtained.

ComReg and operators would both incur costs in the initial set-up of processes for and ongoing costs of implementing those processes. ComReg would need a procedure for disseminating the protected numbers list regularly to operators. Operators, in turn, would need to update their call blocking facilities to block, or remove the CLIs from, calls presenting with CLIs on the list.

ComReg informs us that the UK has implemented an intervention similar to this, having created and maintaining a database of protected numbers. Ofcom shares these numbers with operators which then update their call blocking facilities.

5.4.2 Impacts

The drivers of harm it could address

This intervention would have a similar mechanism as the DNO list, in that it would prevent scammers originating calls with particular Irish numbers. Scams caused by calls using protected numbers could have a somewhat different mechanism from scams caused by calls from well-known numbers, in that in the latter situation, recipients may be in danger of recognising the number and being misled into thinking it is a legitimate call from government agencies or a business.

Effectiveness

This intervention is likely to be similar in the scale of its effectiveness as the DNO intervention given their similar mechanisms. The UK has had a protected numbers list for several years which is regularly shared with operators to enable them to check the validity of calls.[119] In Ireland, the PN list will be lengthier than the DNO list and thus capture a wider pool of potentially spoofed CLIs. The protected numbers list will help to reduce the number of spoofed CLIs known to be associated with trusted organisations, however, given the evolving nature of scam calls, its overall effectiveness is likely to be limited.

Again, the intervention has the potential to be dynamic only to the extent that the composition of numbers on the list can change over time. This would require regular review by ComReg in identifying the numbers to add to or remove from the list, and can therefore only adapt to evolving threats through direct human intervention. For this reason, the protected numbers intervention is considered 'static'.

Costs

The implementation and ongoing management of the list is likely to be inexpensive, and ComReg notes that it is possible to include a protected numbers list within the same processes as a DNO list. This flexibility would allow scope for cost synergies from implementing the two interventions together.

Monitoring metrics

A basic measure would be to record the number of calls operators block based on cross-referencing traffic with the protected numbers list. However, scammers may be able to evade this intervention in the medium term as they become aware of the sorts of numbers on the protected numbers database. Therefore, gauging the attempted and/or successful scam calls claiming to be from trusted organisations would be important, as it could show whether and to what extent scammers adjust their tactics in response to the protected numbers list.

The monitoring of blocked calls would indicate the success of this intervention, but would need to be read together with other monitoring (e.g. regular surveys) to ensure that the overall volume of scam calls was also declining than that scammers were not simply finding other ways of spoofing CLIs.

5.5 Fixed CLI Traffic Blocking

5.5.1 Description

Fixed CLI blocking would involve the operators that transit international calls into Ireland blocking those calls presenting with fixed Irish CLIs.

Irish operators that deal with international calls coming into Ireland would put blocking in place for any numbers with +353 in their CLI (the Irish country calling code) – excluding numbers that start with +353 8X. Crucially, the intervention would need to be implemented by all international gateway operators and operators in Ireland to be most successful as without implementation by all international gateway operators, calls intended as scams may still ingress the Irish PSTN.

The key stakeholders impacted by this would be ComReg and operators of the international gateways into Ireland. Some businesses could be negatively impacted by this measure, for example, those that use call centres located outside Ireland but make calls using fixed Irish CLIs. Such businesses would need to be provided with a direct connection to the Irish PSTN, such as a 'long-line' (direct SIP connection).

[119] See, for example: Ofcom (2021) 'Nuisance calls and messages', p.9 [online]

Other jurisdictions have implemented this intervention in various forms, including France, Australia, Norway, Latvia and Singapore.

5.5.2 Impacts

The drivers of harm it could address

The intervention would prevent scammers from abroad impersonating legitimate Irish organisations via their CLIs such that call receivers think they are receiving a call from a trusted source (or at least from a fixed Irish number). In turn, this would reduce the extent to which consumers are called by scammers based abroad who may ask them to provide personal details which can then be used to commit acts of fraud. In doing so, this intervention could reduce the extent of financial and emotional harm caused to consumers from being duped by scammers.

Reduced spoofing of CLIs using legitimate business and government agency numbers means consumers may maintain more trust in communications from these organisations. This could lead to a reduction in costs for businesses and government organisations who otherwise may need to adjust their communications to convince customers that they are who they say they are. The greater levels of trust achieved also allows government agencies to better carry out their core objectives.

Effectiveness

The intervention should prevent calls from outside Ireland presenting with national fixed CLIs. If implemented in full, it has the potential to severely limit the ability of scammers calling from abroad to impersonate fixed Irish numbers. The intervention would be particularly effective at reducing the risk that people fall for scams when CLIs present with numbers nearly identical to local fixed numbers, save for a few different digits (sometimes referred to as 'neighbour spoofing'[120]). We understand from discussions with stakeholders that fixed CLI spoofing accounts for a large proportion of scam calls.

Some call receivers may still fall victim of international callers that do not attempt to conceal their location, and instead rely on persuasion during a call to convince their victims that they are calling from a trusted organisation.

Similar interventions implemented elsewhere have made sizeable contributions to stemming the flow of scam calls. In Australia, the scam calls code introduced in 2020 is credited with the 61 per cent reduction in reports about phone scams and the blocking of 549m calls.[121] The reduction is being credited to the scam calls code the industry brought in to identify, block and trace incoming calls from scammers in 2020. In Norway, one large operator's implementation of a mechanism for blocking national CLI spoofs blocked around 37m calls in 2021 and 77m in 2022.[122] The same operator blocked around 45m calls across Sweden, Denmark and Finland in 2022.

Costs

The set-up costs may be relatively low and the intervention would mainly rely on existing network capabilities. However, blocking a potentially large volume of international calls could lead to revenue losses for some operators, albeit predominantly toxic in nature.

Monitoring metrics

The intervention could be monitored by recording the volumes of call attempts blocked by this intervention.

[120] Quann, J (2021) 'Scam calls now mimicking our own mobile numbers', *News Talk* [online]
[121] The Guardian (2022) 'SMS scams rise despite success blocking sham phone calls' [online]
[122] Telia (2023) 'Norway at the top of fraud throughout last year. - Stay alert in 2023, advises Telia' [online].

5.6 Mobile CLI Call Blocking and Screening

5.6.1 Description

The mobile call blocking and screening intervention works on the same principle as the Fixed CLI Traffic Blocking and Screening, but it would incorporate roaming checks on *mobile* CLIs to ensure that calls from legitimate Irish roamers making call back to Ireland would not be blocked.

Irish international gateway operators would perform checks with Irish Mobile Operators as to the roaming status of mobile CLI presented for that call to Ireland. This would allow the operators to see whether the number making a call into Ireland is genuinely an Irish mobile roaming user calling from abroad or if it is spoofing its CLI to appear as though it is. Any internationally originating calls presenting with Irish mobile CLIs that are that are not from legitimate Irish roamers would be blocked. The intervention therefore has the valuable characteristic of denying scammers the opportunity to impersonate mobile numbers, which may be perceived as more trustworthy since these numbers could resemble those of the receiver's friends or relatives.

The roamer checks would be based on standard interfaces and signalling that are already in use within mobile networks.

International transit operators who ingress calls to Ireland and who for technical reasons might not yet have the capability to directly perform roamer check would transit international calls presenting with a Irish Mobile CLI to an Irish operator who has the roamer check capability.

The stakeholders impacted by this intervention are international gateway operators who transit calls into Ireland, Irish mobile operators, businesses, government agencies and consumers.

This intervention is planned to be activated in Finland during 2023.

5.6.2 Impacts

The drivers of harm it could address

The drivers of harm this intervention addresses are similar to those of the Fixed CLI Blocking and Screening intervention. This intervention could limit the ability of scammers to impersonate mobile numbers that may be more familiar to consumers, (e.g., businesses), or at the least make an international mobile call appear as a local mobile call (08x numbers in general).

An indirect harm that this intervention addresses is the cost to mobile operators from handling complaints of mobile CLIs being impersonated. By reducing the number of spoofed mobile CLIs, the number of associated complaints may fall, and hence operators may be able to refocus resources away from dealing with such complaints, to the benefit of their wider business.

Effectiveness

This intervention addresses the problem of spoofing CLIs to display a number more familiar or recognisable to the person receiving the call. Approximately 88 per cent of all call minutes in Ireland are accounted for by mobiles, and there are 3.6 times more mobile international/roaming minutes than the total number of fixed international outgoing minutes.[123] This intervention is therefore likely to be especially effective at limiting the risk of fraud caused by CLI spoofing scams in general.

Costs

[123] Europe Economics analysis of ComReg data. Source: Fixed Line Statistics and Mobile Statistics, Total Fixed International Outgoing Minutes (000's) and Mobile International/Roaming Minutes (000's), Q2 2022 [online].

For the mobile operators, the set-up and internal project costs may be moderate and the intervention would mainly rely on existing network switch capabilities. However, some international transit operators which are not Irish MNOs that do not currently have compatible technology are expected to need to deploy new technology infrastructure and/or potentially implement new interconnects.

Monitoring metrics

The intervention could be monitored by recording the volumes of call attempts blocked by this intervention and the volumes of call attempts allowed through the roamer checks.

5.7 Voice firewall

5.7.1 Description

A voice firewall would offer a real-time analysis of incoming calls to identify potential scam calls. This intervention would involve inspecting the signalling traffic and comparing the signalling information (e.g. CLIs) against a set of rules. Based on this analysis, the firewall could allow, strip or otherwise replace the CLI, or block the call. As well as outright blocking, technologies that are currently available from vendors enable suspected scam calls to be forwarded to private voicemails that the call receiver may choose to check if they wish.[124] The rules it uses could potentially be configured to detect fixed CLI spoofing and robocalls, as well as support the use of DNO and PN lists. For calls with mobile CLIs, the firewall could require mobile operators to check, through interoperation with other operators, whether the mobile CLI of an incoming call belongs to a user that is currently roaming – a 'roamer check' similar to that of the traffic blocking and screening interventions.

The ability to reconfigure the checking rules – and to employ machine-learning capabilities that can adapt to new threats – means this intervention is very much a dynamic intervention by nature. Call information from the firewall and other data sources may enable the detection of unusual traffic patterns and spark action to speedily, and/or with a minimum human intervention, implement new rules on the firewall. One vendor indicates that its voice firewall can automatically scan through phone number databases, ranges and destinations to determine 'blacklist' callers.[125]

Alternatively, we understand that some vendors provide voice firewalls that provide pre-configured CLI spoofing detection functionality. The technology can examine CLIs of incoming calls to identify inaccuracies that may indicate spoofing, such as CLI lengths of the incorrect length or format, or from an unallocated number range or fixed area code.[126]

Operators would deploy the firewalls within their networks. The feasibility of additional adjustments to a firewall (e.g. to detect CLI spoofing) could depend on the ease with which the firewall can be integrated with an operator's communications fraud analytics system operational processes. Deployment of voice firewall would require integration with existing network elements and is therefore more of a technical challenge. The intervention would rely on operators to implement (or purchase) the new technologies and systems, which will ultimately benefit consumers and businesses who receive CLI-spoofed calls and potentially other forms of scam calls.

In the UK, EE recently implemented AI-powered voice firewall technology which has blocked 200m scam calls since its inception in 2021 and up to 1m calls daily.[127] The EE firewall detects all inbound calls from

[124] Mavenir (n.d.) 'CallShield: Voice Fraud, Voice Spam, and CLI Spoofing Protection', solution brief, p.4.
[125] Mobileum (n.d.) 'Superior level of fraud protection when integrated with FMS analytics' [online]
[126] Mavenir (n.d.) 'CallShield: Voice Fraud, Voice Spam, and CLI Spoofing Protection', solution brief, p.4.
[127] EE (2022) 'EE takes stand against scammers with latest international call-blocking technology' [online].

international locations using UK CLIs and stops them from being forwarded to other networks, thus benefiting some phone users on those other networks.

5.7.2 Impacts

The drivers of harm it could address

A voice firewall would support the reduction of spoofed CLI calls reaching consumers and businesses. This would leave them less at risk of receiving these calls, and hence reduce the prevalence of losing money and the associated indirect harms (e.g. losing trust in voice calls such that they miss important calls, opportunity costs of being on the calls, emotional distress).

The ability to adapt to evolving threats from scammers gives this intervention the potential to improve consumer and business trust in voice communication in the longer term. Knowing that a voice firewall is in place to respond to CLI spoofing and potentially other forms of threats could imbue call receivers with trust that the calls they receive are legitimate.

Effectiveness

The dynamic nature of this intervention gives operators the potential to considerably enhance the scam call protections that they provide to their customers in the medium to long term.

The use of AI and machine learning gives this intervention a high level of adaptability. It would protect consumers and businesses by layering additional capability in addition to the other voice interventions. One vendor estimates that a voice firewall could block around 90 per cent of all scam calls.[128]

In the UK, EE, which is part of the same group as BT Ireland, has implemented a voice firewall that has been blocking approximately 1m calls per day.[129] This amounts to approximately 200m blocked calls in a year, which is 25 per cent more than was originally predicted. The experience of EE's anti-spam filter suggests that a voice firewall implemented by one operator has the potential to benefit the users on the networks of other operators. The EE firewall prevents calls from abroad presenting with UK numbers from being forwarded to other networks.[130] This is a spillover effect which might mitigate any lags in the implementation of voice firewalls across operators in Ireland.

Costs

Envisaged as an operator-implemented intervention, the up-front costs largely fall on individual operators, and consist of vendor software costs as well as project cost for the operators to implement the software.

Similarly, ongoing operating costs may be material, as new staff/services would be expected to manage the technology on an ongoing basis, including ongoing service payments to vendors.

Monitoring metrics

As with any system with machine learning capabilities, it is important for humans to monitor what new patterns are identified and how the system adapts. In this case, operators would need to keep track of the distinct threats being identified, and whether and how the firewall adapts. Thus, an important metric would be the volume of calls that the firewall strips of CLIs or blocks for each distinct type of threat. By doing so, this intervention benefits from being able to keep track of the volume of potential scam calls identified even after scammers adjust their techniques – one of the criticisms of interventions considered previously is that they would not do this. This is an area that will occupy some of (or add to) the minimal element of human intervention envisaged.

[128] Informed by discussions with ComReg.
[129] EE (2022) 'EE takes stand against scammers with latest international call-blocking technology' [online].
[130] EE (2022) 'EE takes stand against scammers with latest international call-blocking technology' [online].

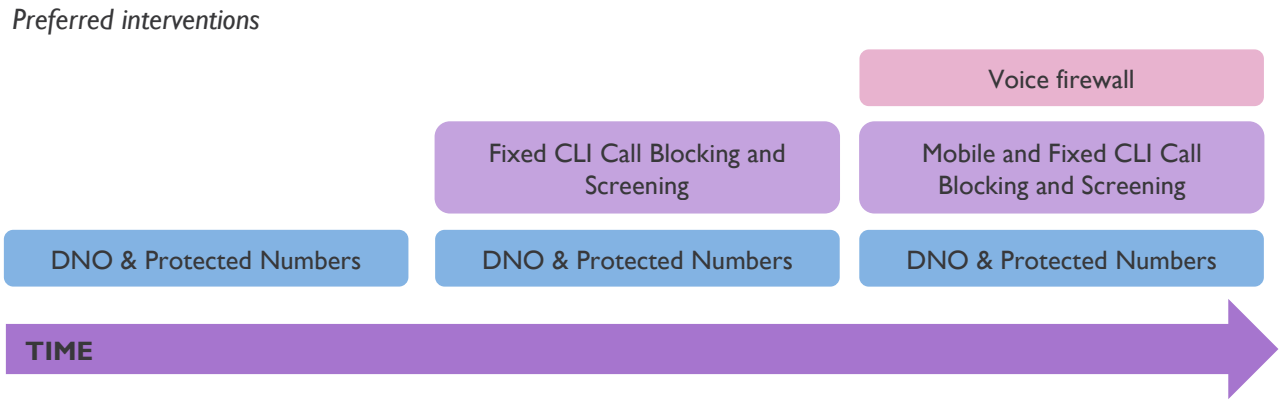
Similarly, it would be worth investigating how the extent of false-positive call blocks could be measured. As scam threats evolve, machine learning systems could have a limited time to train itself on the types of calls that it needs to block before the illegal calls evolve, during which time there may be scope for error.

The complaints received by operators (and by others, such as ComReg) could be monitored to identify whether their implementation of voice firewalls affects the level of consumer/business disruption caused by nuisance calls and their overall satisfaction with their operators.

5.8 Combinations of voice interventions

The complementarities and different complexities of the voice interventions implies that combining them over time would be necessary to achieve the best defence against scam communications. Interventions with relatively low set-up costs and that exploit existing technologies could be implemented in the short term to begin addressing harm immediately. The more complex interventions that require additional specifications or time to put in place could be implemented later. The figure below presents the core option for a combination of voice interventions that could be implemented over time.

Figure 5.1: Potential layering of voice interventions over time



The DNO database and the protected numbers intervention would be combined in the first instance. This would prevent fraudsters from using both numbers that cannot originate calls and numbers that have not yet been legally allocated. However, this still leaves society open to scam calls from abroad that present with Irish CLIs not on the DNO database and Protected Numbers list, which we understand from operators accounts for the majority of scam calls. Implementing the two interventions together is achievable in the short term and will prevent fraudsters from using numbers that cannot send outgoing calls *and* numbers that have been withdrawn or not been allocated.

The Fixed CLI Traffic Blocking and Screening intervention would be introduced in the short to medium term. Together with the DNO database and Protected Numbers list, this would address the majority of scam calls entering Ireland that spoof fixed CLIs.

Fixed CLI Traffic Blocking and Screening intervention does not directly stop scammers from spoofing all numbers of trusted organisations – only those that attempt to spoof fixed Irish CLIs. This reinforces the benefits of bundling this intervention with the DNO database, which could stop scammers calling from abroad using spoofed Irish CLIs whilst also stopping scammers spoofing their CLIs with trusted business/organisation numbers which cannot make outgoing calls in country.

Mobile CLI Traffic Blocking and Screening would be the next intervention to introduce. Implementing this alongside Fixed CLI Traffic Blocking and Screening would combine the ability to limit scams resulting from impersonating fixed CLIs and mobile CLIs, and would account for a significant proportion of scam calls. The mobile intervention could be implemented gradually, beginning with an 'on-net' version (where each mobile

operator checks inbound calls to its own customers to determine that a call from what appears to be a CLI of one its own customers is actually from that customer who is either originating the call in the home network or from a visited network). The full network solution would take longer to be developed and implemented among operators.

In the longer term (after a year) the voice firewall could be implemented, which would enhance the benefits of the other interventions by adding a more dynamic element. As scammers become confronted by the blocks on their activities caused by those interventions in the shorter term, they will likely evolve their methods to maintain access to the pool of potential victims in Ireland. A voice firewall has the potential, in the longer term, to help combat the problems more dynamically and address scam calls that get around the previous interventions.

As the firewall intervention would take some time to develop and implement, the previous interventions would be valuable in preventing the harm caused by scam calls sooner.

5.9 Sender ID registry and blocking

5.9.1 Description

This intervention would require businesses wishing to use an alphanumeric senderID to register their SMS senderID(s) with ComReg. The SMS aggregators that carry such messages ("Participating Aggregators") would be required to follow a code of practise necessitating the authentication of the source of such messages. The mobile operators would then be responsible for blocking any message bearing a senderID from any unregistered source. This would mean that and senderIDs coming from an unauthenticated (scam) source would be blocked.

Messages with any senderID would only be allowed via approved aggregators who have signed up to the code of practise. Mobile operators could be required to initially convert (or 'translate') all unregistered senderIDs to a defined senderID (such as "Unregistered", "Untrusted" or "Likely-Scam") for a period, and thereafter block unregistered senderIDs.

The registry would require all senderIDs to be registered with ComReg and subject to authentication;

Stakeholders directly impacted by this intervention are the operators and SMS aggregators, which would need to implement the sender ID registry and update (or implement) SMS-blocking facilities. ComReg would maintain the register, and sender ID owners would be responsible for organising for their outbound SMSs to be sent through the directly-connected aggregators.

As of early 2023, the Singaporean NRA, the IMDA, is rolling out a full sender ID registry regime.[131]

5.9.2 Impacts

The drivers of harm it could address

This intervention would entirely block texts spoofing the alphanumeric sender IDs of organisations not listed on the ID registry, while protecting the integrity of messages from organisations that are listed on the registry. This would alleviate potential harm coming to consumers who may otherwise open the texts, click on links and/or unknowingly download malware (and become the source of further malware-infected texts). This would also stop such scam texts being bundled with legitimate texts in consumers' SMS inboxes, which can cause confusion and the loss of trust in SMS communications.

[131] IMDA (2022) 'Full SMS Sender ID Registration to be required by January 2023' [online]

Reduced spoofing of sender IDs means consumers may maintain more trust in legitimate communications from these organisations. Alternatively, a warning that a text is not from a trusted source in the form of a translated senderID, maintains the agency of recipients and provides them with the information needed to make an informed decision regarding the texts they receive. Either way, this could lead to a reduction in costs for businesses and government agencies who otherwise may need to adjust their communications to convince customers of their legitimate identity.

The intervention could also address consumers losing trust in SMS communications from businesses and government organisations. This could lead to consumers acting on information sent from legitimate organisations more reliably, reducing the potential costs these organisations face from missed appointments and rescheduling.

Effectiveness

Finally, this intervention deals solely with scam SMSs that seek to spoof sender IDs via 'application originated' rather than 'mobile originated' sources. It would not address scam SMSs using 'regular' mobile numbers which can be addressed using other interventions.

In Singapore, the introduction of a comprehensive SMS SenderID registry appears to have been moderately successful in its infancy, having led to a 64 per cent reduction in scam texts between Q4 2021 and Q2 2022.[132] This has been reflected in customers' experience of scams, with just 8 per cent of scam reports concerning scam texts in Q2 2022, down from 10 per cent in 2021. This intervention was a voluntary regime in Singapore for the period being reported, so it is likely that its effectiveness will increase as it becomes mandatory.

Costs

As an extension of existing SMS firewall capabilities, the blocking component would entail some costs to operators to implement, such as internal project activities i.e. design, implementation, testing. Further software and project costs would be incurred if operators need to extend their SMS filtering capacity. Operators would need to implement new connections from new participating aggregators, and have in place ongoing maintenance to allow newly registered sender IDs and subsequent updates (e.g. change of aggregator).

Aggregators would incur costs of setting up new connections to local MNO(s), if not in place already. They would also incur business costs of onboarding and authenticating new senderID owners, and implementing and validating the required sender ID filtering. A key impact is that non-participating aggregators may lose business as only sender IDs sent through authenticating participating-aggregators would remain unblocked by operators.

The relevant sender ID owners would bear the costs of organising for their outbound SMSs to be sent through the directly-connected aggregators – many of these costs would be pass-through costs from aggregators. Sender ID owners may also forgo the ability to use cheap SMS aggregator services e.g. via offshore aggregators and so-called 'grey routes'. This would depend on how competition between participating aggregators and operators evolves.

Monitoring metrics

The NCIT suggests key metrics for this intervention:

- The number of SMS texts blocked based on sender IDs appearing on irregular routes.
- The number of valid messages with sender IDs appearing over allowed routes.

[132] IMDA (2022) 'Full SMS Sender ID Registration to be required by January 2023' [online]

5.10 SMS Scam Filter

5.10.1 Overview

SMS scam filtering typically analyses the metadata of an SMS message to detect suspicious details (e.g. sender, recipient, source). Some advanced firewalls also go further and inspect the message text itself, looking for scam message patterns or weblinks that may contain viruses and other forms of malware. Once detected, suspicious messages can be blocked, have their text content modified to include a warning, or have the sender ID modified to indicate an untrustworthy source. The intervention considered here is a content-scanning firewall.

Stakeholders directly impacted by this intervention are the operators, which would need to update their SMS firewall platforms. This could be facilitated by existing firewall products already available in the market.

A firewall that inspects SMS messages – either the metadata or the content[133] – raises privacy implications and some consumers may feel that such an intervention encroaches on their communication privacy. This could temper the effectiveness of the intervention at retaining trust in SMS communication is consumers feel that their incoming texts are being monitored.

Despite the potential privacy issues associated with SMS scam filtering, a number of European countries have sought to implement similar interventions. Belgium and Poland intends to standardise legislation to allow the screening of inbound texts based on a variety of rules, some of which may be derived from artificial intelligence (AI) analysis of the message content of SMS traffic. This could lead to suspicious texts being blocked or potentially originating numbers being removed or changed to flag suspicious texts.

5.10.2 Impacts

The drivers of harm it could address

An advanced SMS filter which inspects SMS message content could prevent the spread of scam texts *and* the spread of malware through texts. The former effect would be due to the outright blocking of suspicious texts. Alternatively, flagging suspicious texts and giving consumers the choice of whether to interact with the texts they receive could reduce the prevalence of harms resulting from engaging with scams while mitigating the effects of false-positive detection. The latter effect would occur as the message text could be modified, thus limiting the risk of downloading malware that directly affects recipients' devices or that uses recipients' devices as a platform to spread further fraudulent messages.

Effectiveness

An advanced SMS filter, which actively inspects messages for harmful content, is likely to be most effective at preventing scam texts For instance, scammers may be able to evade an intervention preventing scams at the aggregator node (e.g. sender ID screening) by sending texts directly to a short message service centre (SMSC) and then onto operators, thus bypassing the aggregators. In this instance, operators would not be able to

[133] The Explanatory Memorandum for the new proposed E-Privacy Regulation (that summarises relevant law in this area) that are relevant here notes "The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views, the disclosure of which could result in personal and social harm, economic loss or embarrassment. Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc., allowing precise conclusions to be drawn regarding the private lives of the persons involved in the electronic communication, such as their social relationships, their habits and activities of everyday life, their interests, tastes etc." See here- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

block these messages and thus an advanced SMS scam filter would be needed to reduce the scam risk (SenderID screening can also deal with this).

The SMS scam filter would be a dynamic solution and could quickly react to new scams based on analysis of all messages being sent as well as evolve to identify new and emerging SMS scam message types. This would be particularly valuable if scammers find ways of working around the sender ID registry intervention.

International evidence on similar interventions suggests that a SMS scam filter has strong potential. In the UK, a number of operators have implemented AI based SMS firewalls. EE's 'anti-spam filter' proactively blocks scam texts by analysing content patterns.[134] This intervention blocked 42m scam texts between July and October 2021 and reduced customers' reports of scam SMS by 85 per cent. Real-time monitoring of new and emerging scams is predicted to block over 150m scam texts per year. Vodafone's SMS firewall cut the average volume of scam texts by 76 per cent in December 2021 compared to May 2021.[135] In Australia, Telstra's text-blocking feature blocked 185m scam texts between April and June 2022, approximately 61m per month,[136] whilst Optus's machine-learning firewall blocks an average of 10m texts every month.[137]

Costs

The extent to which operators need to update their firewalls to accommodate this intervention is a key determinant of the implementation cost – which is likely to vary by operator as a result. Our understanding is that operators would most likely purchase software from vendors, and incur additional project costs of embedding this in their systems (e.g. design, governance, testing). Ongoing costs would also be incurred (e.g. paid to vendors) for maintaining and updating the firewall. For example, random samples of blocked/adjusted texts could be spot-checked by the vendor as a service to ensure that automated rules are being followed and that the number of false-positive blocks is kept to a minimum.

Monitoring metrics

The success of this intervention can be measured by monitoring the number of messages that have been blocked and the number of warnings attached to recipients' incoming texts. The spot checks of the blocked texts would be important for estimating the number of texts that are blocked erroneously.

5.11 Combinations of SMS interventions

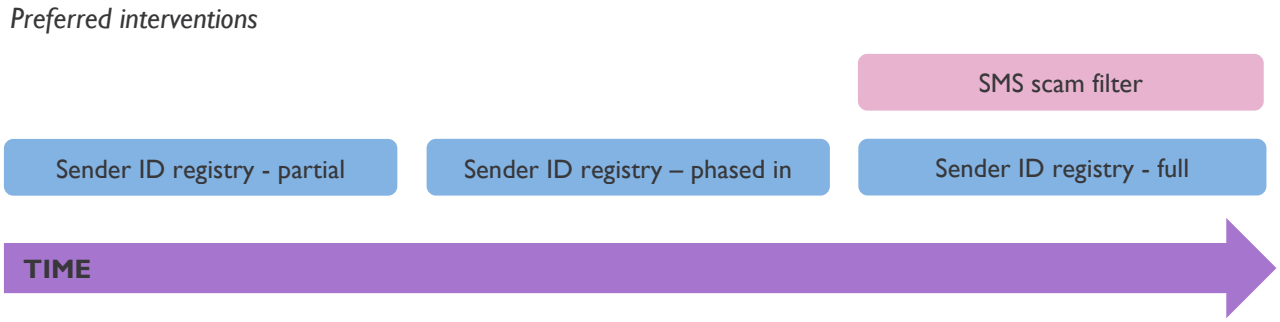
As with the voice interventions, there is value to layering the SMS interventions. For example, a partial sender ID registry could be implemented to first capture the key organisations that are most likely to have their sender IDs spoofed by scammers, followed by the full registry, allowing time for other businesses to register.

Given the complexities of specifying a SMS scam filter intervention, this would take more time to implement and would serve as a medium to longer term, dynamic intervention.

Combining the two interventions would enable operators to identify and block a wider range of potentially harmful texts getting through to mobile users and would also add an extra layer of protection for consumers if any did – through flagging untrustworthy sources, for example. These methods combined are likely to have a high impact on reducing the harm caused by scam texts.

[134] EE (2022) 'EE's taking a stand against scams blocking 42 million scam texts' [online]
[135] ISPreview (2022) 'Vodafone UK's New SMS Firewall Dramatically Cuts SCAM Texts' [online]
[136] Tesltra Exchange (2022) '185 million malicious texts blocked and counting' [online]
[137] Optus (2022) 'Optus' fight against fraud' [online]

Figure 5.2: Potential layering of SMS interventions over time



Source: Europe Economics

6 Cost and Benefits of the Interventions

6.1 Introduction

We now present the costs and benefits of the interventions.

The costs are informed by discussions with operators we interviewed for this research and information gathered from vendors and desk based research. The benefits are estimated as the amount by which each intervention reduces the harms to consumers and businesses quantified in Chapter 4.

The costs and benefits have been modelled over seven years (the implementation period), which represents the time horizon over which the majority of the interventions are likely to be effective and recognises the risk that technological change makes them less effective over time. (The exception being the voice firewall and SMS scam filter interventions, which are dynamic and thus intended to return benefits beyond the implementation period.) The final costs and benefits are then discounted to today's value.

The costs and benefits have been estimated in relation to the central counterfactual harm scenario, as described in Section 4.8.1. This represents a view of how the harm from scam calls and texts might evolve in the future in the absence of any interventions.

The chapter is structured as follows:

- Section 6.2 presents the costs of the interventions.
- Section 6.3 outlines the assumptions regarding the effectiveness of each intervention and the framework for estimating benefits.
- Section 6.4 presents the net present value results. A detailed description of these steps can be found in the associated Appendix.

6.2 The costs of the interventions

We estimate the one-off and ongoing costs of implementing the proposed interventions over the implementation period. One-off costs include capital costs for vendor software, additional vendor costs that could be mandated by ComReg, and the cost to stakeholders of staff time involved in designing, testing and implementation projects. The ongoing costs are those costs associated with annual vendor subscriptions/updates, and monitoring and ongoing intervention delivery.

The cost estimates draw on input from our fieldwork and ComReg technical experts, based on descriptions provided in Chapter 5. Some of the interventions had not been fully specified at the time of writing and thus we use broad estimates of the costs.

The estimates include assumptions about the number of stakeholders affected. Our central estimates assume a large group of telecommunications operators for certain of the interventions who would bear the costs (namely, five for the Voice firewall, and four for the SMS scam filter). Our Appendix presents the results for a smaller grouping (three large MNOs respectively) which results in lower overall costs and higher net benefits.

The table below summarises the cost descriptions across the interventions.

Table 6.1: Description of intervention costs

Intervention	One-off costs	Ongoing costs	Affected stakeholders
DNO / PN blocking	Internal costs to implement the blocks – business case design, testing, configuration.	Updating the lists and change requests.	Around 30 operators
Fixed CLI blocking	Internal project costs to implement and test the solutions.	No material ongoing costs identified.	Around 10 International Gateway Operators (IGOs)
Mobile CLI blocking	V1 – internal costs to design and test on-net roamer checks, plus software costs to extend roamer checks to other operators' customers. V2 – costs of shared solution between main operators (including proxy servers) and solutions for VoLTE roaming. Internal project and infrastructure costs plus software costs.	Ongoing software costs (20%)	Three main MNOs plus one large IGO. Other operators assumed to be able to route traffic over the proxy server solution.
Voice firewalls	Vendor costs and internal project costs to implement the solutions.	Ongoing vendor costs (20%)	Three main MNOs plus two large fixed operators. (Appendix shows results of just 3 MNOs).
Full and partial sender ID registry	Operators – internal development costs to update filtering (design, configuration, testing); costs of new connecting aggregators.	Updating connections to new aggregators and new IDs.	3 enabling operators
	Aggregators – internal development costs to make new connections to operators; business costs of onboarding ID senders.	Updating connections to new aggregators and new IDs.	10 large and 20 smaller aggregator
	ComReg – IT development to set up registry and portal	Assume all connections made up-front so minimal ongoing costs. Updating registry	ComReg
	Sender ID owners – costs of connecting to aggregators and registry fees to ComReg. Note that sender ID costs would represent transfers from aggregators and ComReg, so not modelled explicitly.		500 in total. 100 classified as 'large' senders.
SMS scam filter	Vendor costs and internal development costs.	Ongoing vendor costs (20%)	3 main MNOs plus 1 large fixed operator. (Appendix shows results of just 3 MNOs).

The one-off costs are assumed to be incurred in the first year of implementation, which is "Year 1" for most of the interventions. The exceptions are the VoLTE stage of the Mobile CLI blocking intervention and the Full Sender ID registry (both standalone and phased-in variants). For these, initial costs are split between Year 1 and Year 2, reflecting their longer-term implementation schedule. The ongoing costs of each intervention are incurred in the subsequent years and do not vary from year to year. For simplicity, we have assumed that costs are incurred at the beginning of the year.

We model three versions of the SMS registry for completeness – a full and partial model in isolation, and then a phased-in approach whereby the partial model is first implemented followed by the full model.

The tables below present the one-off and ongoing costs per stakeholder and in aggregate.

Table 6.2: The one-off and ongoing costs for each intervention per stakeholder (€000s)

Intervention	One-off costs per stakeholder €000s	Ongoing costs per stakeholder (1 year) €000s
DNO/PN	Operators – 33	Operators – 3
Fixed CLI blocking	Operators – 46	nil
Mobile CLI blocking (without VoLTE)	Operators – 356	Operators – 60
Mobile CLI blocking (with VoLTE)	Operators – 856	Operators – 160
Voice firewall	Operators – 1,184	Operators – 223
Sender ID Registry (Partial)	Operators – 150 Aggregators – 107 ComReg – 211	Operators – 20 Aggregators – nil ComReg – 360
Sender ID Registry (Full)	Operators – 150 Aggregators – 123 ComReg – 211	Operators – 20 Aggregators – nil ComReg – 360
Sender ID Registry (Full phased-in)	Operators – 150 Aggregators – 123 ComReg – 371	Operators – 20 Aggregators – nil ComReg – 360
SMS scam filter	Operators – 1,096	Operators – 98

Note: The number of stakeholders for each cost category maps onto Table 6.1 above. Only key stakeholders who would bear the material costs of the interventions are considered.
Source: Europe Economics analysis. Values not discounted.

Table 6.3 : Total costs: total one-off and ongoing cost over the 7-year implementation horizon (€000s)

Intervention	Total one-off cost	Total ongoing cost
DNO/PN	981	605
Fixed CLI blocking	462	nil
Mobile CLI blocking with VoLTE after 2 years	3,424	3,440
Voice firewall	5,919	5,340
Sender ID Registry (Partial)	3,861	2,523
Sender ID Registry (Full)	4,361	2,102
Sender ID Registry (Full phased-in)	4,521	2,523
SMS scam filter	4,384	2,352

Source: Europe Economics analysis. Values not discounted.

6.3 Estimating the benefits of the interventions

As described in Chapter 5, the benefits of the interventions can be articulated in terms of how they reduce the harms from scam calls and texts. There are two main drivers here – how the interventions reduce the *volume* of scam calls and texts, and how they reduce the *likelihood* of recipients being scammed by calls and texts that are still received – for example, by forcing scammers to employ workarounds such as using 'plain' international numbers to make scam calls, or to send SMSs with a phone number rather than a recognisable

sender ID. For simplicity, our model focuses on the first driver – how the volume of scam communications is reduced.

Estimating the benefits of interventions in reducing the harm from scam communications is challenging, given uncertainty around the precise number of scam calls and texts and the associated harms, the newness of the interventions and the associated lack of data on their effectiveness. To our knowledge our report represents the first thorough attempt to do this for any country, and is based on a robust empirical estimation of the harms from scam communications along with informed estimates and logical modelling of the effectiveness of each intervention.

In order to estimate the impact of each intervention over time, we determined the percentage reduction in scam calls and texts that each intervention would have over the intervention period. This is based on information gathered from operators and other regulators where available, and our understanding of scammers' behaviour set out in Chapter 3. For simplicity we assume that the benefit of each intervention will be realised at the beginning of each year.

To examine what possible combination of interventions brings the greatest benefit to Irish consumers and businesses, we assess the impact of the interventions in two scenarios.

- Scenario 1: Cumulative benefits: where interventions are applied in sensible "layers" starting with the least onerous interventions before adding additional interventions. The two dynamic interventions (Voice firewall and SMS scam filter), as well as the Fixed CLI block target the *remaining harm* from the scam calls or texts not picked up by the preceding interventions. Therefore as the effectiveness of the preceding interventions decays, the benefits of these interventions grow. The preceding interventions are modelled as being applied one after the other.
- Scenario 2: Interventions in isolation: where each intervention is implemented individually. This scenario informs the raw cost-vs-benefit of each intervention as though they were each implemented independent of one another. This also allows us to examine the effect of the dynamic interventions were scammers to circumvent the static interventions perfectly (such that they had no benefit). In each scenario, the benefits are modelled as the reduction in harm relative to the counterfactual harm scenario over time.

In either case, the key variable in assessing the impact of each intervention is an assumption of the share of scam calls and texts they affect. For example, the DNO and PN blocking interventions would only be effective in blocking scam calls that spoof DNO and PN numbers – the smaller this proportion of scams the smaller the effectiveness of the intervention.

Besides the obvious voice call/SMS split across interventions, within the voice call category there is further disaggregation between scam calls presenting with fixed and mobile CLIs. We assume that the DNO and PN lists and the fixed CLI blocking interventions are effective against scam calls presenting with fixed CLIs.[138] Within this, based on operator data we assume that scam calls spoofing DNO/PN numbers make up a relatively small shared of fixed CLI spoofs (around five per cent). The mobile CLI blocking intervention would be effective against scams that spoof mobile CLIs from outside Ireland. We assume that voice call scams are split broadly 50-50 between fixed and mobile CLI spoofs.

The SMS registry interventions would be effective against any scam SMSs based on spoofed senderID, with the full registry capturing more scams than the partial. As the partial registry would begin with the most well-known organisations, we assume that this intervention would only be somewhat less effective than the full registry model.

By their nature, the two dynamic interventions – the Voice firewall and the SMS scam filter – are assumed to target all scam calls and texts respectively, and they would act upon the scams that remain *after* the effects

[138] In reality we understand that PN may also affect mobile numbers, but given the likely small scale and for simplicity we bundle it with DNO as a fixed call solution.

of the other interventions have been realised. By comparing the results under the two scenarios, we measure the range of benefits provided by the dynamic interventions in reducing all harms. This is because in Scenario 2 (individual impact), we examine the effect of the voice firewall on scam calls and SMS scam filter on scam texts on their own, which is equivalent to assuming the static interventions to be wholly ineffective (i.e. scammers adapt perfectly to the interventions).

6.3.1 Summary of key timing assumptions

The timing of the interventions is important when calculating their net present value. Costs incurred further into the future will have a lower value when discounted to the present time. We use the standard social discount rate for Ireland of 4 per cent following the DPER Public Spending Code.

For the simpler interventions, we assume that the benefits begin to be realised in the same year as the costs are incurred. For others, there is a delay between when the intervention is first implemented and then the benefits begin to be realised given the time taken to develop the intervention (nearly a year or more)

Three interventions are assumed to have staggered implementation phases such that the costs are split over two years. These are:

- Mobile CLI blocking, with the costs of the shared solution and provisions for VoLTE roaming being incurred in year 2.
- Full SMS registry, with the costs of connecting all sender IDs being spread over two years.[139]
- Phased-in registry, with the costs of the partial element being incurred in year 1 and the costs of the full element in year 2.

The table below summarises the timing assumptions of costs and benefits for each intervention.

Table 6.4: Summary of key timing assumptions

Intervention	Year (Y) in which fixed costs are incurred	Year in which benefits begin
DNO/PN	1	1
Fixed CLI blocking	1	1
Mobile CLI blocking	VoLTE stage: Split between Y1 and Y2	2
Voice firewall	1	2
SMS registry - partial	1	2
SMS registry - full	Split between Y1 and Y2	3
SMS scam filter	1	2
Full (phased-in) sender ID registry	Split between Y1 and Y2	2: effects of Partial registry. 3: Effects of Full registry.

Source: Europe Economics analysis.

6.3.2 Effectiveness of interventions

Table 6.5 summarises the rationale for our assumed effectiveness for each intervention (based on evidence reported in Chapter 5), along with the percentage reductions in harm that form the basis of our modelling – both the initial impact and the impact after some decay in effectiveness as scammers work around the interventions.

[139] For our modelling purposes we assume that the largest senderID owners would be connected first. It may be that aggregators and operators are able to connect all ID owners sooner than two years.

Given the uncertainties inherent in estimating the effectiveness of the interventions, we also conduct critical-value analysis to determine the lowest value of effectiveness that would be required to generate a net-beneficial value of each intervention.

Table 6.5 : Intervention effectiveness evidence and assumptions

Intervention	Country	Source	Evidence	Our assumptions	Initial impact (%)	Decay impact (%) (after 2 years)
DNO/PN	UK	Talk Talk	TalkTalk has seen a 65 per cent reduction in complaints about scam calls since it introduced the measures. Ofcom estimated that about 700,000 people received spoof calls in the three months to August 2022. [online]	We assume 5 per cent of fixed CLI scam calls. Effectiveness would decay over time as scammers shifted away from spoofing DNO/PN numbers towards other fixed CLIs.	-5	-3
	Ireland	Large IGO	Irish operator data shows that DNO number spoofs are low in Ireland (1-2% of calls), but that list is currently very small. May increase as list expands			
Fixed CLI blocking	Australia	Regulator	The Australian Competition and Consumer Commission's Scamwatch says that between 1 January and 13 November this year, reports about phone scams decreased by 61% from 135,400 in 2021 to 57,400 this year. The reduction is being credited to the scam calls code the industry brought in to identify, block and trace incoming calls from scammers in 2020. More than 549m calls have been blocked by telcos since the scam code was introduced.[online]	Intervention would initially address 90% of fixed CLI scam calls. Decay in effectiveness due to scammers shifting towards non-spoofed international numbers or spoofed UK CLIs which Irish consumers may still trust.	-90	-80
	Norway and Other Scandinavian countries	Telia	Millions of calls being blocked by Telia in Norway and other Scandinavian countries due to Fixed CLI blocking [online]; [online]; [online]			
	Ireland	Large IGO	Majority of scam calls coming from international fixed and mobile CLIs			
Mobile CLI blocking	Finland		Little experience with this intervention in other jurisdictions. Finnish regulator expects intervention to be largely effective against spoofed mobile CLIs from international sources.	Intervention would address 90% of spoofed mobile CLI calls. Decay would arise if scammers used legitimate Irish SIM cards	-90	-80

				to make scam calls. Assume equivalent decay to fixed intervention.		
Voice firewall	International	Vendor	- International vendors tell ComReg they expect firewall to be highly effective at blocking voice scam calls ("in the 90s")	The firewall would address 90% of remaining scam calls, after the preceding interventions. No decay in effectiveness assumed given dynamic solution.	-90	-90
	UK	Operator	Everything EveryWhere (EE) in the UK is blocking as many as two hundred million scam calls in a year, following the introduction of an artificial intelligence based "anti-spam filter" in 20211.			
SMS registry (full)	Singapore		The IMDA's registry appears fairly successful to date. There has been a 64% reduction in scams through SMS from Q4 2021 to Q2 2022. Scam cases perpetrated via SMS make up around 8% of scam reports in Q2 2022, down from 10% in 2021.	Intervention would apply to all scam texts spoofing sender IDs (assumed to represent the bulk of scam texts causing harm). Some decay as scammers shift to non-sender ID scams.	-65	-60
SMS registry (partial				Same as above, with adjusted effectiveness to represent partial registry consisting of the most commonly spoofed organizations' IDs.	-55	-50
SMS scam filter	UK	EE	- SMS scam filter technology has blocked over 11 million scam texts since its inception in July 2022.[online]	The firewall would address 85% of remaining scam texts, after the preceding interventions. No decay in effectiveness assumed given dynamic solution based on machine learning and ability to adapt to scammers' workarounds.	-85	-85
		VF	- International experience shows firewalls blocking millions of scam texts per month, with Vodafone reporting a 76% reduction in scam texts.			

	Australia	Telstra	In April 2022, technology had blocked over 185 million scam text messages in the three months to July and 225 million to December.			
		Optus	Between 1 December 2020 and 31 March 2022, Optus blocked more than 232 million scam calls and now block an average of ten million texts every month.			

6.4 Results : The net present benefit of the interventions

The costs and benefits are estimated over the implementation period. The net benefits (benefits less costs) are calculated for each year and then discounted to present values.

Scenario 1: Interventions implemented cumulatively

This section presents the results, showing the incremental impacts of each intervention as it is added to the preceding ones, and the cumulative benefits of the all interventions. In this scenario, the dynamic interventions are assumed to target the harm from scam calls or texts that *remain* following the implementation of the preceding interventions. The Fixed CLI block also works incrementally upon the DNO/PN lists (since they target the same type of scam calls), but this is less consequential given the low assumed impact of the DNO/PN lists, as a result of the small share of scams using CLI spoofing.

The results show that the incremental reduction in harm caused by the Voice firewall and SMS scam filter interventions is lower if the interventions implemented before them are still working well and scammers have not yet found new means of reaching Irish consumers (i.e. without CLI spoofing). Consequently, in this scenario the incremental Voice firewall net present benefit is just €142m after seven years – much lower than the two CLI blocks. Despite these highly conservative assumptions, the Voice firewall is still great value, with over €15 in benefits for every €1 cost. In contrast, the value of the Fixed CLI block is reduced marginally from €485m when implemented in isolation, to €469m.

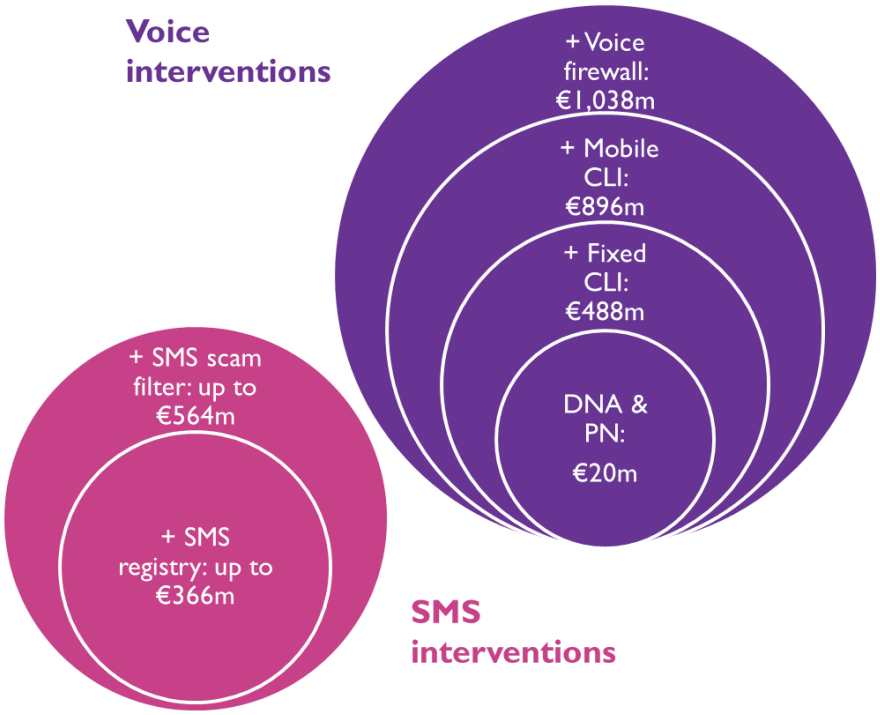
The incremental benefits of the SMS scam filter are predictably lower if implemented following the Full SMS registry, assuming that it is working well and that scammers have not yet found new means of reaching Irish consumers (i.e. without SMS ID spoofing). This is despite the Full SMS registry only beginning to reduce harm in year 3 as a Partial registry would be functioning in year 2, thus reducing the incremental benefit of the SMS scam filter intervention in this year in particular. Despite these highly conservative assumptions, the SMS scam filter is still great value, with over €33 in benefits for every €1 cost.

Table 6.6: Scenario 1: Estimated cumulative reduction in harm and net present benefit across the interventions (€m); cumulative NPV shown

Intervention	Present-value incremental reduction in harm (€m)	Incremental NPV (€m)	Cumulative NPV (€m)
VOICE INTERVENTIONS			
DNO and PN	21	20	20
Fixed CLI blocking	469	469	488
Mobile CLI blocking	414	408	896
Voice firewall	152	142	1,038
SMS INTERVENTIONS 1			
SMS registry - partial	317	311	311
SMS scam filter after Partial	251	245	555
SMS INTERVENTIONS 2			
SMS registry - full	312	306	306
SMS scam filter after Full	255	248	555
SMS INTERVENTIONS 3			
SMS registry - full (phased-in)	372	366	366
SMS scam filter after Full (phased-in)	204	197	564

Source: Europe Economics analysis. Note: The difference between the Cumulative NPV may not exactly equal the Incremental NPV due to rounding.

Figure 6.1: Scenario 1: cumulative net present value benefit across the interventions (€m)



Source: Europe Economics analysis.

Scenario 2: Interventions implemented in isolation

Table 6.7 presents the results of this scenario both in terms of benefits (reduction in harm) and net present benefits (benefits less costs over time). The Voice firewall would have the most significant impact of all the voice interventions, with a net present benefit of €881m over the period. This is driven predominantly by the fact that the Voice firewall is assumed to cause a non-decaying 90 per cent reduction in all scam calls.

Despite the Fixed CLI and Mobile CLI blocking interventions targeting equal shares of scam calls, the net present benefit of the Mobile CLI block is slightly less than that of the Fixed CLI block. This is driven by the fact that it is considerably costlier, and its effects on reducing harms are experienced a year after implementation commencement.

For the sender ID options, the phased-in variant of the full SMS registry scores the highest, with a net present benefit of €366m. This is because it begins to stem the harm from scam texts in year 2 in line with the effectiveness of the Partial registry, before realising the effects of the Full registry in year 3. In turn, the registry begins to decay in year 5, giving it the longest period of 'original' (or full strength) impacts.

The SMS scam filter intervention would be the most effective intervention for SMS scams, with a net present benefit of €514m over the seven years. We assume that the SMS scam filter is implemented without any delay due to the need for supporting legislation. This is necessary to simplify our analysis, given the uncertainty inherent in predicting the passing of legislation. However, we note that any such delay results in continued harm to Irish consumers and businesses, with a 1-year delay resulting in a €93m cost of uncaptured harm over the seven years.

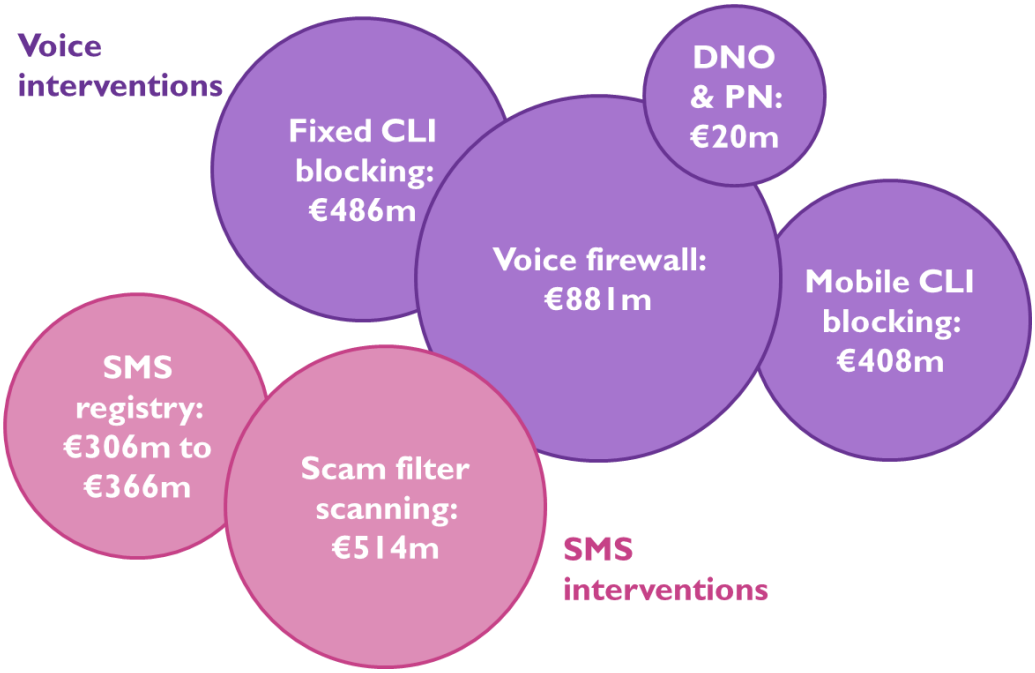
The Voice Firewall has a much greater NPV than the SMS scam filter primarily because harm from voice scams across consumers and businesses is much greater than harm from SMS scams. It is also expected to be more effective (addressing 90% of calls as opposed to 85% of texts).

Table 6.7: Scenario 2: Estimated present-value reduction in harm and net present benefit per intervention in isolation (€m)

Intervention	Present-value reduction in harm (€m)	Net present benefit (€m)
DNO and PN	21	20
Fixed CLI blocking	487	486
Mobile CLI blocking	414	408
Voice firewall	892	881
SMS registry - partial	317	311
SMS registry - full	312	306
SMS registry - Full (phased-in)	372	366
SMS scam filter	520	514

Source: Europe Economics analysis.

Figure 6.2: Scenario 2: net present value benefit, per intervention (€m)



Source: Europe Economics

Scenarios 1 and 2: Discussion

As noted in the "static" view of harm, Scenario 1 would vastly understate the benefits of the dynamic measures on their own (the Voice Firewall and SMS scam filter), as it assumes that scammers blocked by static measures such as CLI Blocking will not find new routes to customers or develop scams that sidestep the static interventions altogether.[140] While we do not know the degree to which scammers will circumvent such interventions, we do know they will try and there is emerging evidence of such practices both in Ireland and abroad.

To account for this, Scenario 2 can be interpreted as the impact of the dynamic interventions on reducing dynamic harm, assuming that the same level of harm prevails in spite of the static interventions (e.g. if scammers were to fully circumvent these interventions such that their benefits were zero). This is equivalent to assessing the impact of the dynamic interventions in isolation (e.g., on overall harm). Therefore, these figures can be considered upper bounds for the potential benefits of the Voice Firewall and SMS spam filter.

[140] While our models do build in a "decay rate" in interventions effectiveness, the real issue is whether scammers will be able to circumvent the static interventions altogether.

This approach enables us to capture the potential benefits of the dynamic interventions,[141] in light of scammers' adaptability.

We find that the voice firewall and SMS scam filters are important and provide benefits of €142m and €197m even where scammers do not adapt to the static interventions, because they offer additional protection (e.g., against scams originating in Ireland). However, they become increasingly more important the more scammers adapt to the static interventions, rising to €881m and €514m respectively when considered in isolation (i.e. akin to a scenario where scammers fully adapt). Again, the exact benefits of each intervention depends on the reaction of scammers to the static interventions, including at what point they adapt. We consider this approach appropriate for estimating the range of potential benefits because assuming a specific level of adaptation (and related timing) by scammers over such a long period would require information that is simply not available.

The table below presents our central scenario where scammers adapt to some extent to the static interventions (such that their effectiveness decays over time) and an extreme scenario where scammers adapt fully to the static interventions, such that their benefits are zero. Whilst this is an unlikely scenario, it nevertheless provides an absolute lower bound to the benefits of the intervention packages.

Figure 6.3: Comparison of costs and benefits assuming different levels of scammers' adaption

Intervention	Cost (€m)	Net Benefit	
		Scammers adapt minimally to static interventions	Scammers adapt fully to static interventions
Voice interventions			
Static interventions (DNO,PN, Fixed & Mobile CLI Blocking)	€8m	€896m	-8m
Voice firewall	€10.2m	€142m	€881m
SMS Interventions			
Static: SMS registry – Full (phased-in)	€6.4m	€366m	-6.4m
SMS scam filter	€6.2m	€197m	€514m
Combined			
Total	**€31m**	**€1.6bn**	**€1.4bn**

Source: Europe Economics analysis. Values may not add due to rounding. Note that the reported costs in the table are present value figures over the 7-year implementation horizon.

[141] The static harm assumes that the value and profile of harm from scams in 2022 (e.g., % from Fixed CLI spoofing, Mobile CLI spoofing) is forecast into the future, whereas dynamic harm assumes that the same level of prevails but completely circumvents the static measures.

7 Conclusions and Recommendations

7.1.1 The problem of scam communications

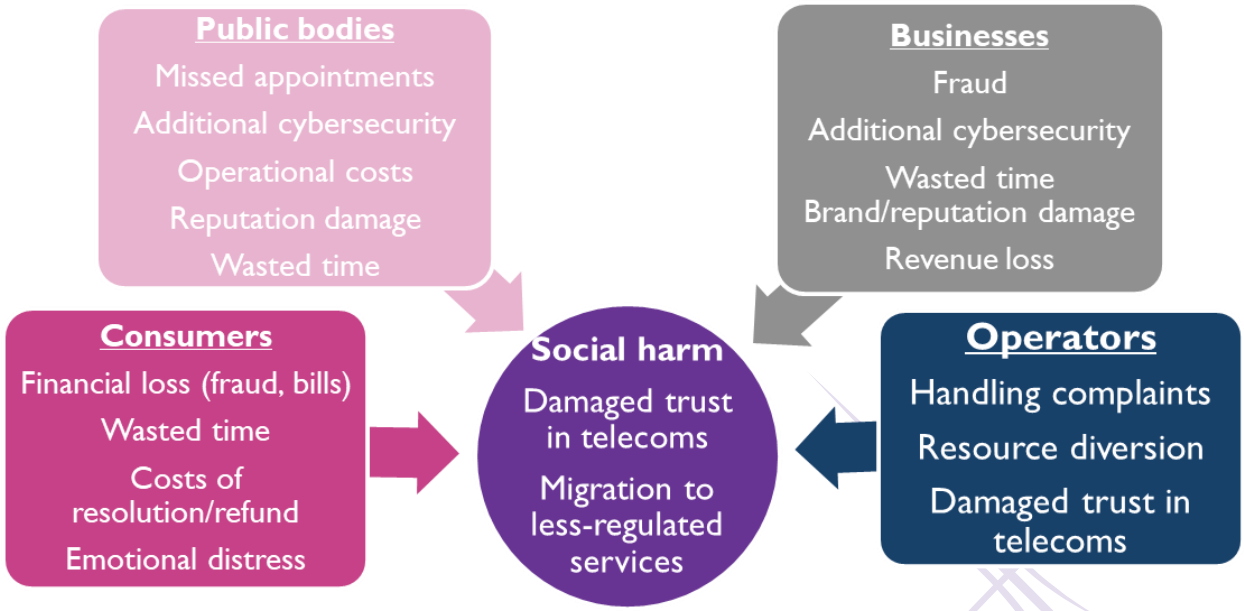
The use of mobile and fixed telecommunications – both voice calls and SMS – is central to the functioning of Irish society and its economy. Around 15 billion calls and 2.5 billion SMS messages are made in a year.[142] Telecommunications are an essential part of businesses and the public sector, in terms of driving business operations and service provision and keeping in contact with customers and service users.

Nuisance communications therefore have wide-reaching impacts both in Ireland and abroad. This report has focused on scam calls and texts that attempt to impersonate well-known organisations (such as banks, courier companies and public services) or personal numbers by 'spoofing' telephone numbers (CLIs) or alpha-numeric SMS sender IDs. The aim is to mislead victims into thinking they are receiving calls or texts from legitimate organisations or people, and illegally obtain sensitive information such as bank details with the view to committing fraud.

As an English-speaking nation, Irish residents are targeted disproportionately compared to their EU counterparts, receiving fraudulent phone calls or emails asking for personal details 10 per cent more often than the EU28 average in 2016-19.[143] Currently the majority of scam calls and texts targeting Ireland originate abroad. Given the opportunistic nature of scammers, they are likely to concentrate their efforts in countries where the defences against scams are (relatively) low. There is thus a risk that if Ireland takes no action in this area, it will increasingly become a target if other countries' defences improve.

Scam communications can cause a host of harms to individuals, businesses and public organisations, and wider society, as summarised below.

Figure 7.1: Harms from scam calls and texts



Source: Europe Economics

[142] ComReg. 'Tabular Information' – [online]
[143] European Union (2019).' Europeans' attitudes towards cyber security (cybercrime)' – [online]

7.1.2 The scale of the problem in Ireland

This report represents the first attempt to estimate the total harms from scam communications in Ireland, and is the most thorough examination of this issue of which we are aware.

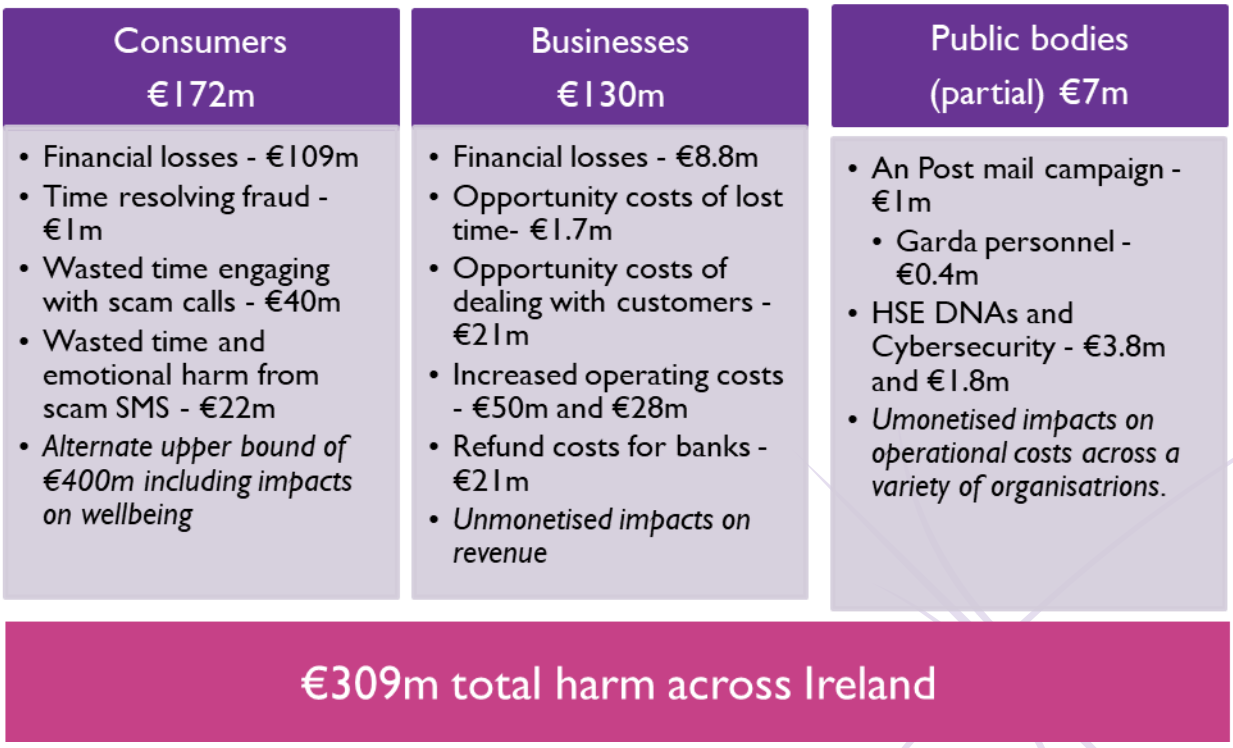
In order to estimate the harms from Nuisance Communications, we gathered evidence from representative surveys of Irish citizens and businesses, interviews with operators, businesses and public bodies, and desk-based research. Based on this work we identified the affected stakeholders and identified key harms they suffer as a result of scam calls and texts. We then developed a comprehensive bespoke and quantitative model to estimate harms across different stakeholders – by far the most thorough of which we are aware.

We then utilised a number of approaches to quantifying harm:

- Bottom-up cost modelling, which used data derived from our consumer and business surveys and estimated tangible costs.
- Willingness-to-pay (WTP) analysis was used to capture intangible harms from scam calls and texts. We obtained two broad estimates: an overall, forward-looking WTP capturing a fuller range of harms including the annoyance or distress recipients might feel, or fears about potential losses from fraud; and a backwards looking WTP analysis capturing just the emotional and time cost element actually incurred.
- Illustrative case studies to provide examples of aspects of harm that were not captured in the above two tools due to their bespoke nature, in particular for businesses and public bodies. Given the great variety across organisations in Ireland it is not possible to extrapolate these examples, and thus the estimates provide just a partial view of the harm to such organisations.

Our research shows that harm in Ireland from scam communications is significant, and **conservatively estimated** at **€309m a year**.

Figure 7.2: Summary of quantified harms from scam communications



Source: Europe Economics

This figure does not capture full extent of harm to public organisations, and also does not capture all elements of emotional harm or forgone business revenue. In particular, it does not fully capture harm to wider society

from a loss of trust in telephone numbers, calls and texts. Trust is difficult for consumers and organisations to define, measure and quantify. However, our Willingness to Pay analysis suggests that the impact of a loss of trust in telecommunications could be in the range of €230m for consumers, and our business survey suggests that as much as €48bn worth of revenue could be at risk from a loss of trust of business-relatred communications among consumers. Without any action to tackle nuisance communications, there is little reason to believe that harm would fall, given the opportunistic nature of scammers and their ability to take advantage of new events or changes in phone users' behaviour. If other jurisdictions continue to improve their security, Ireland may become even more susceptible to scam calls and texts.

7.1.3 Technical interventions

We considered a range of technical interventions that could be implemented by telecoms operators to tackle scam calls and texts. These have been suggested to us by ComReg based on its work with the NCIT and its assessment of what interventions are suitable for consideration given their feasibility. While the interventions that featured in the NCIT will likely be implemented sooner by NCIT members, we find that all interventions should be implemented as soon as possible, as any delay entails a continuation of the significant harm volumes. In particular, delays in implementing the SMS scam filter by even one year are estimated to **reduce the benefits of the intervention by €93m** over the seven-year period.

Figure 7.3: Options for interventions to tackle scam calls

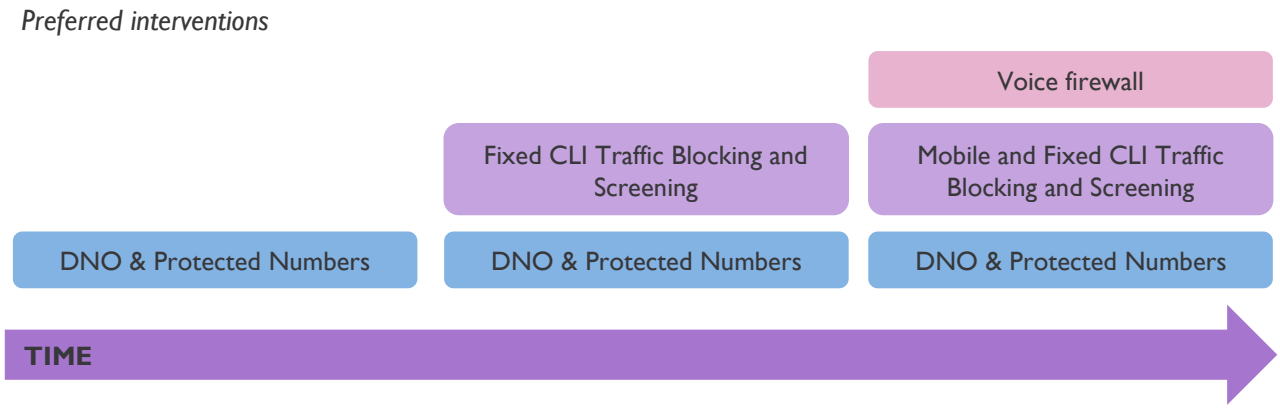
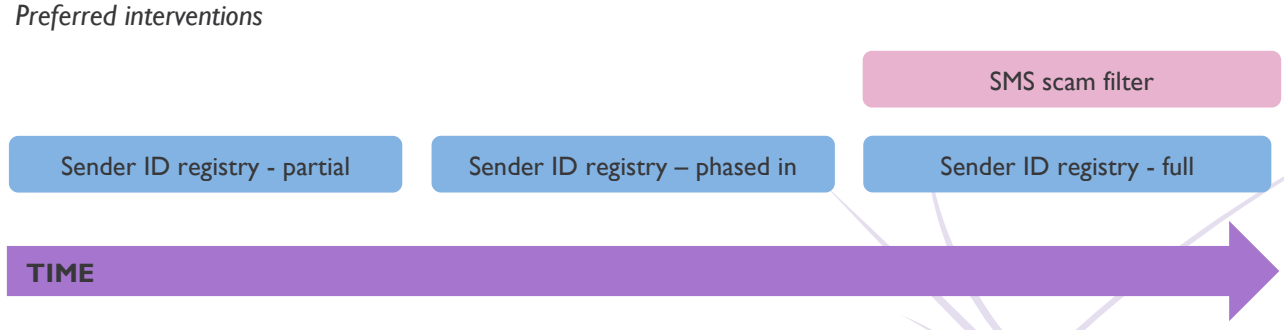


Figure 7.4: Options for interventions to tackle scam calls



Source: Europe Economics

7.1.4 Net benefits of the interventions

We estimated the costs of each intervention based on information received from operators, ComReg and vendors. Benefits were modelled as the extent to which each intervention is assumed to reduce the volume of scam calls or texts, and thus harm. Costs and benefits were modelled over a seven-year period, and

discounted to the present value. We analysed the costs and benefits of each intervention in isolation, and the incremental benefits if the interventions were introduced cumulatively.

All interventions are cost-beneficial at our assumed levels of effectiveness, as shown in the tables below.

Table 7.1: Net present benefit per intervention in isolation (€m over 7 years)

Intervention	Net present benefit (€m)
DNO and PN	20
Fixed CLI blocking	486
Mobile CLI blocking	408
Voice firewall	881
SMS registry - partial	311
SMS registry - full	306
SMS registry - Full (phased-in)	366
SMS scam filter	514

Source: Europe Economics analysis.

For scam calls, the voice firewall would have the most significant impact of all the voice interventions, with a net present benefit of €881m over the period. This is driven predominantly by the fact that the Voice firewall is assumed to cause a 90 per cent reduction in all scam calls. Similarly, the SMS scam filter would be the most effective intervention for SMS scams if implemented in isolation as it is assumed to capture a greater share of scam texts than the registry options, with a net present benefit of €514m over the seven years.

When applied one after the other, the incremental net benefit of each intervention depends on the effectiveness of the preceding interventions in blocking a volume of scam calls and texts. For example, the incremental benefit of the mobile CLI block is the same as its benefit in isolation. This is because the preceding interventions do not tackle mobile scam calls, only those spoofing fixed CLIs. On the other hand, the incremental benefits of the voice firewall and SMS scam filter are much lower compared to their benefit in isolation. This is because the firewalls are assumed to pick up and block scam calls and texts *remaining* after the preceding interventions. However, the benefits of these interventions still outweigh their costs. A further important feature of the two firewall interventions is that these are unlikely to lose their effectiveness over time[144], as they are based on machine learning and designed to adapt to changes in scammers' techniques in a way that the other interventions may not. Our model assumes that all the other interventions would experience some decay in their effectiveness over time as scammers develop workarounds. Therefore, the incremental net benefits of the two firewalls would be even larger if extended beyond the seven year intervention period.

[144] Assuming these are recalibrated with appropriate frequency (similar to keeping firewall/anti-virus products up to date on a personal computer).

Table 7.2: Incremental and cumulative net present benefit across the interventions (€m)

Intervention	Incremental NPV (€m)	Cumulative NPV (€m)
VOICE INTERVENTIONS		
DNO and PN	20	20
Fixed CLI blocking	469	488
Mobile CLI blocking	408	896
Voice firewall	142	1,038
SMS INTERVENTIONS 1		
SMS registry - partial	311	311
SMS scam filter after Partial	245	555
SMS registry - full	311	311
SMS INTERVENTIONS 2		
SMS scam filter after Full	306	306
SMS registry - full (phased-in)	248	555
SMS INTERVENTIONS 3		
SMS registry - full (phased-in)	366	366
SMS scam filter after Full (phased-in)	197	564

Source: Europe Economics analysis. Note: The difference between the Cumulative NPV may not exactly equal the Incremental NPV due to rounding.

However, the approach above assumes that scammers do not merely sidestep static interventions. In reality, the extent to which individual interventions are effective depends on how scammers adapt to the interventions. The voice firewall and SMS scam filters are important and provide benefits of €142m and €197m even where scammers do not adapt because they offer protection that cannot be provided by the static interventions (e.g., against scams originating in Ireland).

These interventions become increasingly more important the more scammers circumvent ComReg's static interventions, rising to €881m and €514m where scammers fully adapt. Again, the exact benefits of each intervention depends on the reaction of scammers to the static interventions. We consider this approach appropriate for estimating the range of the benefits because assuming a specific level of adaptation by scammers over such a long period would require information that is simply not available.

Figure 7.5: Comparison of costs and benefits assuming different levels of scammers' adaption

Intervention	Cost (€m)	Net Benefit	
		Scammers adapt minimally to static interventions	Scammers adapt fully to static interventions
Voice interventions			
Static interventions (DNO,PN, Fixed & Mobile CLI Blocking)	€8m	€896m	-8m
Voice firewall	€10.2m	€142m	€881m
SMS Interventions			
Static: SMS registry – Full (phased-in)	€6.4m	€366m	-6.4m
SMS scam filter	€6.2m	€197m	€514m
Combined			
Total	**€31m**	**€1.6bn**	**€1.4bn**

Source: Europe Economics analysis. Values may not add due to rounding. Note that the reported costs in the table are present value figures over the 7-year implementation horizon.

7.1.5 Sensitivity analysis

Our key finding is that **all potential interventions are cost-beneficial at our assumed levels of effectiveness**, and also at much lower assumptions of effectiveness as shown in our sensitivity analysis in the Appendix. Furthermore, the combined package of all interventions would still have significant net benefits even were scammers to fully adapt to the static interventions such that their benefits were zero.

We also conducted sensitivity analysis to see how the costs and thus net benefits of all the proposed interventions would change if the number of large operators that would incur the costs of the Voice firewall and SMS scam filter were to change from five and four operators respectively to three operators each. This change reduces the one-off and ongoing costs of the two interventions and increases the net benefit on the central adaption scenario marginally by €6m over the 7-year period.

7.1.6 Recommendations

Based on the costs and benefits estimated, it is clear that all the interventions are beneficial. We note that the estimated benefits are conservative as they do not capture the full range of harms such as emotional harm and the variety of harms experienced by public organisations, as well as the intangible harm from a society-wide loss of trust in telephone numbers.

Given the scale of harm incurred every year and the likelihood of this increasing – or at least remaining steady – in the absence of any intervention, we recommend that interventions are implemented as soon as possible, starting with those that can be implemented soonest and incorporating the more complex ones in time.

- **To combat scams texts,** we recommend implementing SMS ID Registry and SMS scam filter. The cumulative net benefits are greatest for the combination of the sender ID registry and the SMS scam filter. The SMS scam filter brings large benefits relative to its costs no matter the scenario used.

Implementing the SMS ID registry absent the SMS scam filter risks undermining the SMS ID registry, were scammers to switch to scams that do not involve SMS ID spoofing. This is clearly already necessary, given the large share of recent scams that do not use SMS ID spoofing.

- **To combat scam calls**, we recommend implementing DNO/PN, Mobile and Fixed CLI Blocking and Voice Firewall. This would bring the greatest reduction in scam calls, no matter how scammers react. The three fixed interventions (DNO/PN and Fixed CLI blocking) should be implemented as these tackle slightly different types of scam call, and have low implementation costs. The Mobile CLI block is needed to address scams that spoof mobile CLIs and also brings large benefits relative to its cost. The Voice firewall brings large benefits relative to its costs no matter the scenario used. Implementing the static measures absent the Voice Firewall risks undermining the static measures, were scammers to switch to scams that do not involve CLI spoofing.

8 Appendix 1: Calculation of Harms

Our approach to estimating the harms from scam calls and texts consisted of three tools, and combined evidence from public data sources, our interviews and results from consumer and business surveys (the fieldwork) and selected case studies, with extrapolation to the relevant Irish population.

- Bottom-up cost modelling used data points derived from our consumer and business surveys to estimate the costs and prevalence of a range of harms, such as losses from fraud, the monetary value of time spent resolving scams; or the monetary value of time spent engaging with scam calls or texts. These individual harm estimates were then added together for consumers and businesses separately. Bottom-up cost modelling cannot capture all harms, such as intangible harms of annoyance or distress, or second-order effects of a loss of trust in calls or SMS.

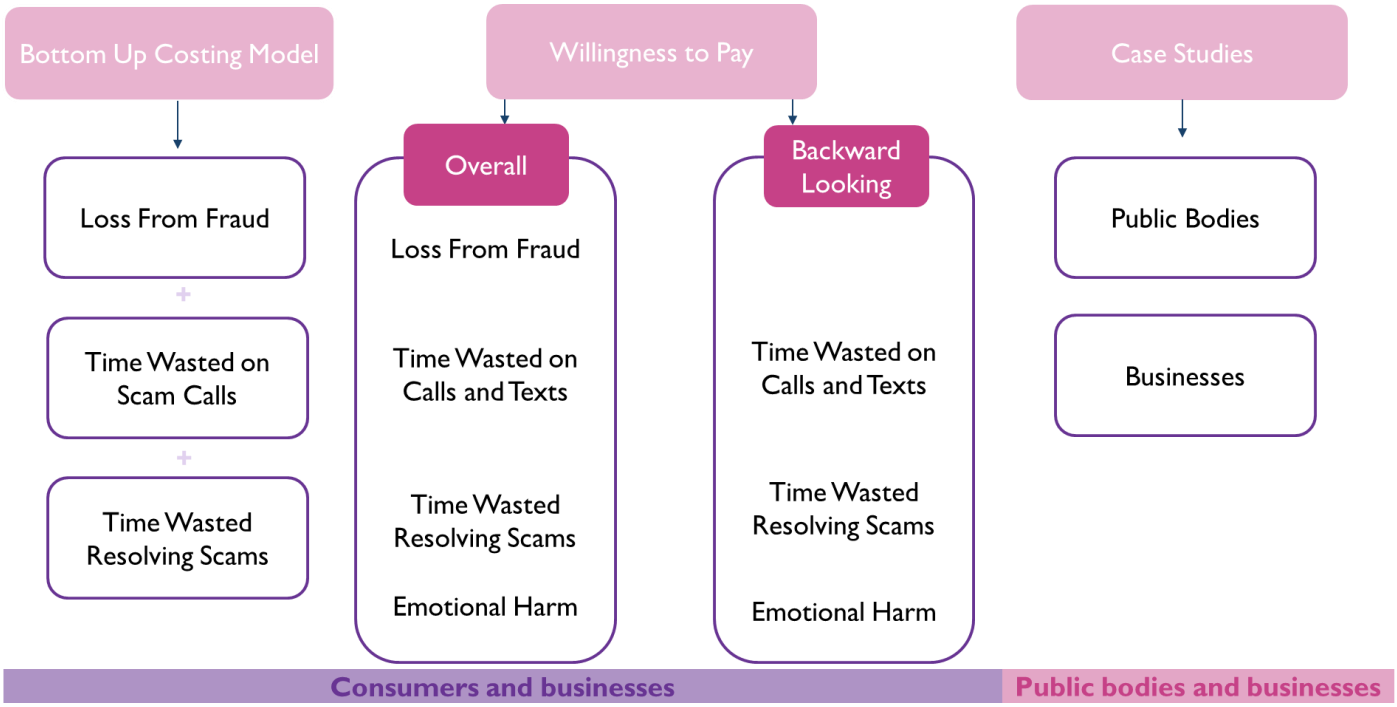
- Willingness-to-pay (WTP) analysis was used to capture intangible harms from scam calls and texts. In our surveys we asked consumers and businesses how much they would be willing to pay to avoid receiving scam calls and texts (using a variety of question formats). This enabled us to estimate a fuller range of harms including the annoyance or distress recipients might feel, or fears about potential losses from fraud (what we term 'overall WTP'). The overall WTP estimates represent a different approach to estimating harm compared to the bottom-up cost modelling, and as such the two sets of harms estimates should not be added together and are instead used in order to act as sense check on each other and produce more reliable estimates of the harm caused by scam calls and texts.

  For consumers, we also included a 'backwards looking' willingness to pay estimation, limited to actual consumer experiences of receiving scam calls and texts.[145] As this only included those who had received scams calls or texts and had not experienced losses from fraud, this WTP estimate captures more accurately just the annoyance/distress and time cost element of the harm. As such, it is possible to add this to different elements of the bottom-up estimates such as losses from fraud.

- Illustrative case studies provide examples of aspects of harm that were not captured in the above two tools due to their bespoke nature, in particular for businesses and public bodies.

[145] Consumers were asked how much they would be willing to pay to not have received the scam calls and texts they received in the past year, rather than being asked what they would be willing to pay to avoid receiving all scams in the future.

Figure 8.1: Summary of our approach



8.1 The consumer and business surveys

The harms calculations have been informed in part by two surveys that were conducted for the project. One survey was targeted at consumers in Ireland and the other at businesses in Ireland. They were designed jointly by Europe Economics and ComReg and conducted by B&A. Many of the questions in these surveys asked respondents to select from a range of values that best represented their answers – or 'bins'. In these instances, references to the 'mean' value throughout this appendix refers to the mean value as calculated by B&A using the weighted proportions of respondents that selected each bin. We were able to calculate the median values for those questions where respondents could report an unrestricted amount.

8.1.1 Consumer survey

The consumer survey involved 1,219 responses from adults aged 16+ across Ireland. All responses were obtained through B&A's online research panel. The gender split of the sample was roughly equal, with 51% female and 49% male. The ages of respondents were also equally distributed between age bands, with 14% aged 18-24, 15% 25-34, 20% 35-44, 17% 45-54, 14% 55-64 and 19% 65+. In terms of the geographic location, 29% are located in Dublin, 27% in Rest of Leinster, 27% in Munster and 18% in Connaught/Ulster. Respondents were also asked about their gross income. The majority of respondents (just under 60%) indicated that they earned €25k-€50k (31%) and €50k-€100k (28%); 18% earned up to €25k and 8% €100k-€150k. Only 3% of respondents earned over €150k.

Table 8.1: Summary demographics of respondents to the consumer survey

Characteristic	Number	Share (%)
Gender	**1,219**	**100**
Male	607	49.8
Female	612	50.2
Age	**1,219**	**100**
17-24	128	10.5
25-34	205	16.8
35-44	235	19.3
45-54	249	20.4
55-64	174	14.3
65+	228	18.7
Region	**1,219**	**100**
Dublin	331	27.2
Leinster	325	26.7
Munster	325	26.7
Connaught/Ulster	238	19.5
Urban/Rural	**1,219**	**100**
Urban	799	65.5
Rural	420	34.5

Source: ComReg consumer survey. Share (%) given as percentage of respondents.

All survey respondents reported having a mobile phone that they use. More than half pay monthly for their mobile contracts ('bill pay'); the rest have prepay setups. The majority of respondents, 60 per cent, stated that they have a landline handset, too.

Table 8.2: Summary device usage statistics (consumer survey)

Characteristic	Number	Share (%)
Mobile use	**1,219**	**100**
Yes	1219	100
No	0	0
Mobile package type	**1,219**	**100**
Prepay	510	42
Bill pay	690	57
Don't know	19	2
Landline use	**1,219**	**100**
Yes	492	40
No	727	60

Source: ComReg consumer survey. Share (%) given as percentage of respondents

Population variables

Table 8.3 summarises the population variables for consumers in Ireland. Each start with an estimate of the population of adults (18+) in Ireland from the World Population Review 2022.[146]

The Mobile phone-owning population and the Landline phone-owning population are calculated by multiplying the Irish adult population by the share of Irish people who use a mobile phone and a landline phone, respectively, based on ComReg's Mobile Consumer Experience 2022 survey.[147] The number of people who own a mobile or a landline is the mobile phone-owning population plus (i) those who owned a mobile but no mobile currently and now use landline instead; (ii) those who never owned a mobile and use landline instead; and (iii) those who use mobile phone belonging to someone else in the house.

The scam call recipient population is hence the product of the number of people who own a mobile or a landline and the share of adults that have received a scam call in the last year, as given by the consumer

[146] World Population Review, Ireland Population Pyramid 2022 [online]. There are 3,839,448 people over 18 in Ireland.
[147] ComReg (2022) 'Mobile Consumer Experience 2022 - Survey results' [online].

survey. The scam text recipient population is the product of the mobile phone-owning population and the share of adults that have received a scam text in the last year, also from the consumer survey.[148]

Table 8.3: Population variables for consumers in Ireland used in harms modelling

Population variable	Estimate
Mobile phone-owning population	3.76m
Landline phone-owning population	1.50m
People who own a mobile or a landline	3.79m
Share of people that received scam calls	92%
Scam call recipient population	**3.49m**
Share of people that received scam texts	84%
Scam text recipient population	**3.16m**

Source: Europe Economics analysis of ComReg consumer survey and other sources.

8.1.2 Business survey

The business survey involved 794 responses from businesses across Ireland. Most of these (501) were obtained through B&A's telephone unit and the rest (293) through an online research panel. The vast majority of respondents represented firms with 1-9 employees (92%). Of the remaining, 6% represented firms with 10-49, 1% 50-249 and 1% 250+. In terms of the geographic, 32% are located in Dublin, 25% are located in Rest of Leinster, 26% in Munster and 17% in Connaught/Ulster. The top five industries respondents indicated activity in are Construction (19%), Professional, scientific & technical (14%), Transportation, storage & communication (13%), Retail Trade & Repairs (10%) and Accommodation & food service activities (6%).

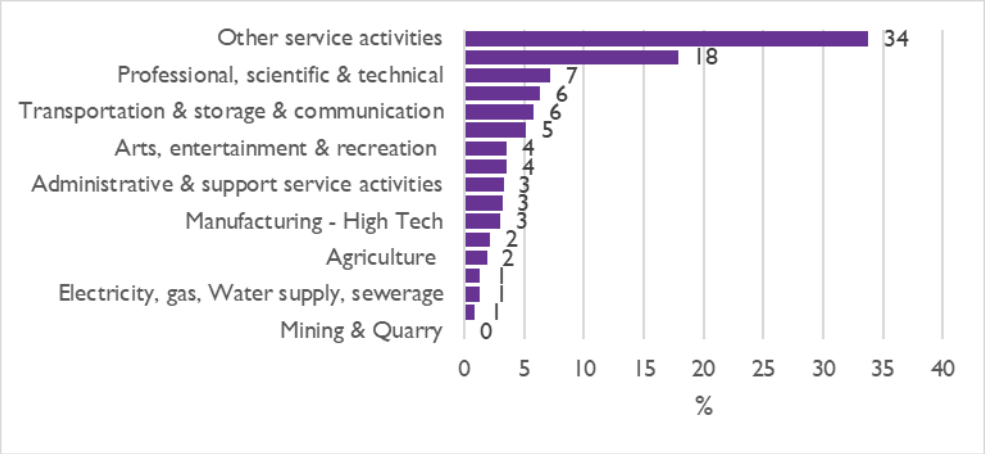
Table 8.4: Summary characteristics of respondents to the business survey

Characteristic	Number	Share (%)
Sector	**794**	**100**
Private	684	86
Public	100	13
Don't know	10	1
Company ownership	**794**	**100**
Irish Owned	690	87
Multinational	89	11
Not Applicable	15	2
Employees	**794**	**100**
1-3	243	31
4-9	225	28
10-19	108	14
20-49	92	12
50-250	69	9
250+	57	7

Source: ComReg business survey. Share (%) given as percentage of respondents

[148] 100% of adults reported having a mobile phone in the consumer survey.

Figure 8.2: Business survey industry representation, % of respondents



Population variables

For the business harm calculations, we relied on the extrapolated numbers of businesses calculated by B&A using the business survey results. We understand that these are estimated based on quota-controlling the sample of responding businesses in terms of size (employee number), region and sector to reflect the profile of the companies in Ireland.

8.2 Harms to consumers

Figure 8.3 illustrates the different methodologies that have been used to quantify consumer harms. For all harms, extrapolation of the survey data and population variables was used. Forward-looking WTP analysis was used to capture intangible harms from scam calls and texts, allowing us to estimate a fuller range of harms (loss from fraud and emotional harm). For consumers, we also included a backwards-looking WTP estimation, limited to actual consumer experiences of receiving scam calls and text (emotional harm). The value of time was used to estimate the opportunity cost of wasted time using the estimates from the Department of Transport.

Figure 8.3 : Methodologies used to quantify consumer harms

Harm/methodology	Extrapolation	Value of time	Backward Looking WTP	Forward Looking WTP
Financial losses from fraud	**Yes**	No	No	**Yes (*overall WTP*)**
Costs of resolving fraud cases	**Yes**	No	No	**Yes (*overall WTP*)**
Opportunity cost of wasted time	**Yes**	**Yes**	No	**Yes (*overall WTP*)**
Emotional harm	**Yes**	No	**Yes**	**Yes (*overall WTP*)**
Lost trust in voice and SMS communications	**Yes**	No	No	**Yes (*overall WTP*)**

We have quantified a range of harms to consumers, set out in the table below. We indicate how these harms have been incorporated into an aggregated figure, bearing in mind overlaps between the bottom-up cost modelling (BUCM) approach and the willingness to pay (WTP) approach.

Table 8.5: Summary of quantified harms to consumers

Harm	Estimate	Approach	How included in total

A	Financial loss from fraud	€109m	Bottom-up cost modelling	Direct harm from fraud. Included in total aggregated harm.
B	Opp. Cost of time engaging with scam calls	€40m	Bottom-up cost modelling	Indirect harm (wasted time) from scams, only relating to scam calls. Included in aggregated total.
C	Opp. Cost of time resolving scams	€1m	Bottom-up cost modelling	Indirect harm (wasted time) from fraud. Included in aggregated total.
D	Overall WTP	€399m	WTP (all respondents)	Direct and indirect harm from scam calls and texts (perceived and actual). Overlaps with above and represents upper bound. Excluded from aggregated total.
E	Backward looking WTP (calls)	€25m	WTP (those receiving scam calls in past year, not victims of scam)	Indirect harm from scam calls (actual – assumed wasted time and emotional harm). Overlaps with B. Excluded from aggregated total.
F	Backward looking WTP (SMS)	€22m	WTP (those receiving scam texts in past year, not victims of scam)	Indirect harm from scam SMS (actual – assumed wasted time and emotional harm). No overlap with BUCM. Included in aggregated total.
Aggregated harm (A + B + C + F)		**€172m**		

8.2.1 Financial loss from fraud

We estimated the financial loss from fraud as a result of scam calls and scam texts separately. Table 8.6 provides key estimates and sources for variables used to quantify this.

For scam calls, we started with the number of Irish people who have suffered financial loss in the last year, as given by the product of the scam call recipient population and the share of adults who have received scam calls to either mobile or landline and lost money as a result (5%). The gross defrauded loss (or the scammers' gain) is then the product of this figure and the average financial loss incurred in the last year, based on the mean of consumer survey responses (€494). The gross defrauded loss per annum is hence €86.2m. As the survey data were collected in bins, it is not possible to estimate the exact median, and this method also protects against extreme outliers. We therefore rely on the mean wherever this is the case.

We account for people who were able to recover some of their loss according to the consumer survey (49% of those who suffered a loss) and the average share of the loss that was recovered (28%). The net defrauded loss is therefore €75m. The survey did not enable us to identify from whom losses were recovered; our working assumption is that the reported recovered loss amounts were recovered from banks, rather than from the scammers themselves.

Following the same steps as above and using the estimates applicable to scam texts (mean loss of €230) we estimate a gross defrauded loss (scammers' gain) per annum of €44m. Accounting for some recovery (62% recovered 34% of the loss, on average), the net harm to consumers is estimated at €35m.

The total financial loss to consumers from fraud caused by scam calls and texts is therefore estimated to be €109m in one year. The gross loss, without any recovery, is €130m.

Although there are examples of large fraud amounts being recovered from scammers, it is likely that the vast majority of recovered funds reported in our survey (given the relatively small amounts scammed) were recovered from the banks, rather than from the scammers. We therefore assume that the gross defrauded loss figure across calls and texts (€130m) represents the total welfare loss to Irish society. We report the recovered amount (€21m) in the harms to businesses (banks) section.

Table 8.6 : Key assumptions for harm: financial loss from fraud

Variable description	Estimate	Consumer survey question
Scam calls		
Share of scam call recipient population who suffered financial loss due to fraud.	5%	Q11a
Average financial loss as a consequence of scam calls.	€ 494	Q12 (mean)
Share of defrauded people who managed to recover at least some loss.	49%	Q16
Average proportion of financial loss that is recovered.	28%	Q16
Scam texts		
Share of scam text recipient population who suffered financial loss due to fraud.	6%	Q28a
Average financial loss as a consequence of scam texts.	€ 231	Q29 (mean)
Share of defrauded people who managed to recover at least some loss.	62%	Q33:
Average proportion of financial loss that is recovered.	34%	Q33 (mean)

Source: Europe Economics analysis of consumer survey.

8.2.2 The opportunity cost of time engaging with scam call

This harm is assumed to be specific to scam calls and thus we do not calculate a scam text equivalent (although we recognise that navigating around a scam text would take some seconds, and thus our estimates of the opportunity cost can be considered a lower bound). We estimate the time spent by multiplying the mean number of scams calls received per year by an individual (17), by the mean time spent on call with a scammer (1.93 minutes, or 0.03 hours).

We turned this time into a financial value by assigning established estimates of the values of leisure and work time[149] to an assumed split of when consumers receive scam calls. We assume that consumers receive scam calls in both their work and leisure time, and that they may receive calls at any hour of the day. Assuming an 8-hour work day, we calculate the opportunity cost of the wasted time at €40m in one year. It may be that some proportion of these costs is borne by businesses, if such time is incurred during a working day. For simplicity we incorporate all these costs into the consumer section to minimise the risk of double-counting with our business harms.

[149] An hour of leisure: €12.75; work: €34.33. ComReg 22/48, p.66 FN 54 [online]. Figures uplifted to 2021 prices.

Table 8.7 : Key assumptions for harm: the opportunity cost of time engaging with scam call

Variable description	Estimate	Consumer survey question
The number of scam calls received on mobile or landline per year by an individual.	17	Q7 (mean)
The time spent on the line with scammer, in seconds.	116	Q14 (mean)
Average share of leisure time in a typical day.	67%	Assumes 8 hours of work per day.

Source: Europe Economics analysis of various sources.

8.2.3 The opportunity cost of time resolving issues associated with scam calls and texts

To calculate the opportunity cost of time resolving scams (from calls and texts), we start with shares of scam call recipients and scam text recipients who have attempted to resolve the associated issues. The total time wasted is calculated by multiplying this by the mean time spent resolving the issues (428 seconds, or 0.12 hours).

We turn the time value into a financial value by applying the same methodology as previously outlined for the opportunity cost of time engaging with scam calls. The total time wasted is multiplied by the value of time. The total harm of resolving issues associated with scam calls is thus €776,000 in one year and scam texts is €248,000. Together this yields a total harm of approximately €1m in one year.

Table 8.8 : Key assumptions for harm: the opportunity cost of time resolving scam

Variable description	Estimate	Consumer survey question
Scam calls		
Share of scam call recipient population who attempted to resolve scam (successful or attempted).	9%	Consumer survey Q15a
The time spent resolving problems caused by scam call, in hours.	0.12	Consumer survey Q15a. (Mean)
Average share of leisure time in a typical day.	67%	Assumes 8 hours of work per day.
Scam texts		
Share of scam text recipient population who attempted to resolve scam (successful or attempted).	3%	Consumer survey Q32
The time spent resolving problems caused by scam text in hours.	0.11	Consumer survey Q32a. Mean
Average share of leisure time in a typical day.	67%	Assumes 8 hours of work per day.

Source: Europe Economics analysis of various sources.

8.2.4 Emotional harm

To illustrate this harm, we quantified the number of annoying/irritating and distressing communications received as a result of scam calls and texts. To do so, we multiplied three components together: the number of scam call (text) recipients, the share of scam call (text) recipients that found the calls (texts) 'annoying/irritating', and the mean number of scam calls (texts) received over the past year.

The survey results imply that there were 51m annoying/irritating communications due to scam calls and 38m due to scam texts in the last year. Following the same methodology and substituting with the share of communications that are 'distressing', the survey results imply that there were 17m distressing communications due to scam calls and 14m due to scam texts.

Importantly, a respondent in the consumer survey could indicate whether they found a given scam communication to be 'annoying/irritating', 'distressing', or both. This means that the numbers described above are not independent events and so should not be added together.

Table 8.9 : Key assumptions for harm: emotional harm

Variable description	Estimate	Consumer survey question
Scam calls (annoyance/irritation & distress)		
Share of people who received scam calls and have found them to be annoying/irritating.	86%	Consumer survey Q8
Share of people who received scam calls and have found them to be distressing.	29%	Consumer survey Q8
Number of scam calls received	17	Consumer survey Q7: Mean
Scam texts (annoyance/irritation & distress)		
Share of people who received scam texts and have found them to be annoying/irritating.	81%	Consumer survey Q26
Share of people who received scam texts and have found them to be distressing.	29%	Consumer survey Q26
Number of scam texts received	15	Consumer survey Q25: Mean

Source: Europe Economics analysis of various sources.

8.2.5 Willingness to Pay (WTP)

This section outlines the methodology for calculating harm to consumers through WTP analysis. We developed three variations to estimating harm from a WTP approach, with different questions in the consumer survey:

- Variation 1: Contract difference method. This asked respondents to place a value on their current mobile contract and then consider what they would pay for their current mobile contract plus the guaranteed blocking of all scam calls and texts. The harm caused by scam calls and texts is then inferred from the difference between the two contract valuations. The reported values are monthly amounts.
- Variation 2 ("Overall WTP"): Product purchase method. This asked respondents how much they were willing to pay per month for a product/app that would block all scam calls and texts received on mobiles and landlines. The harm is interpreted as the value respondents place on such a product. The reported values are monthly amounts.
- Variation 3 ("backward looking WTP"): This prompted respondents to consider the scam calls and texts they reported having received over the past year, and asked how much they would pay to have not received any of them. The reported values are annual amounts.

Variation 1 – Contract difference method

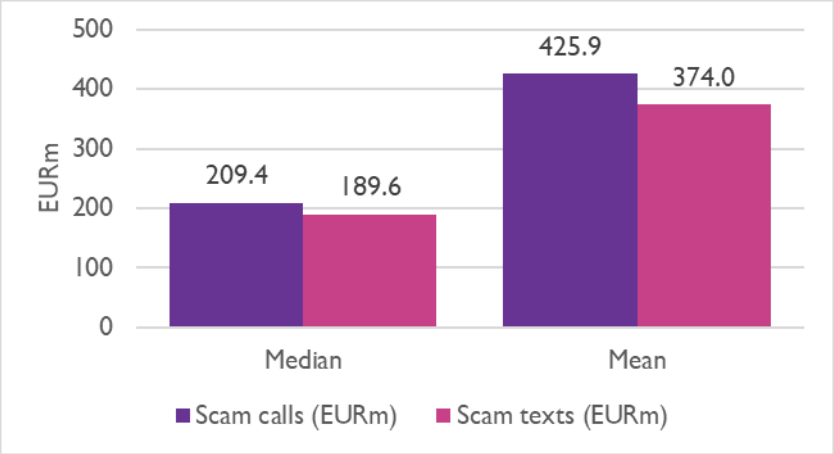
The results to this question suggest that different respondents interpreted the question differently. For example, there were a number that provided a lower value for the hypothetical contacts including scam blocking compared to the current contract, which suggests they may have misunderstood the question and considered that the hypothetical contract value should be in *addition* to the current contract. The responses may also reflect reactions to how the question was framed. Asking respondents to value scam blocking in addition to the value of their current contract may have caused some to react on the perception that their mobile operators ought to already be providing a scam blocking service, and hence they would be unwilling to pay any more for this service. Given the issues in interpretation, we consider that the results of this particular formulation of WTP are not sufficiently robust for include in our analysis.

Variation 2 – Product purchase method (Overall WTP)

This variation involves identifying the value consumers would pay each month to have a product/app/subscription that could guarantee the blocking of all scam calls and texts. This perfect product does not exist; the aim is to observe how much consumers value this hypothetical scenario and hence understand the amount of harm that could be avoided with the product. It takes inspiration from Ofcom's

(2015) willingness WTP approach to estimating the harm caused by nuisance calls.[150] We multiply the scam call (text) recipient population by the monthly average value of a product that could block scam calls (texts) to generate an aggregate willingness to pay to avoid them. The results are shown in Figure 8.4 for the mean and median values given by respondents.

Figure 8.4: Results of WTP Variation 2 – Product purchase method (main estimates)



Source: Europe Economics analysis.

Table 8.10: Key assumptions for harm: WTP Variation 2 – Product purchase method

Variable description	Estimate	Consumer survey question
Average value of a product for your mobile/landline that could block scam **calls** (monthly).	€5.00	Q23 - median of actual values
	€10.17	Q23 - mean of actual values
Average value of a product for your mobile/landline that could block scam **texts** (monthly).	€5.00	Q39 - median of actual values
	€9.86	Q39 - mean of actual values

Source: Europe Economics analysis. Q.23(Q39) If you could buy a product for your mobile and landline (mobile) that could block scam calls (texts) without you having to take any further action, how much would you pay per month for this?

The minimum value respondents provided for a scam-blocking product was zero in respect of both scam calls (25% of responses) and texts (27%). This shows that a notable minority were not prepared to pay extra for scam blocking. The maximum value in respect of scam calls was €200 (given by two responses) and €260 (given by one) in respect of scam texts. In both cases, the values above €200 are around double the next highest values (see Table 8.11).

Table 8.11: Highest five values given for the monthly payment for a product to block scam calls and texts

Highest values	Scam calls (€)	Scam texts (€)
First (maximum)	200	260
Second	200	200
Third	100	200
Fourth	90	109
Fifth	80	100

This shows that there are some clear outliers and this is reflected in the median values being significantly less than the mean. Nevertheless, more than a third of respondents provided values of more than €10 per month for the product (in respect of both scam calls and texts) and around 10% of more than €30 per month, suggesting that many consumers assign a material value to the ability to block scam calls and texts. We use

[150] Ofcom (2015). 'Review of how we use our persistent misuse powers' [online]

the median as our central value in our reporting, which generates an overall harm from this approach across calls and texts of just under €400m.

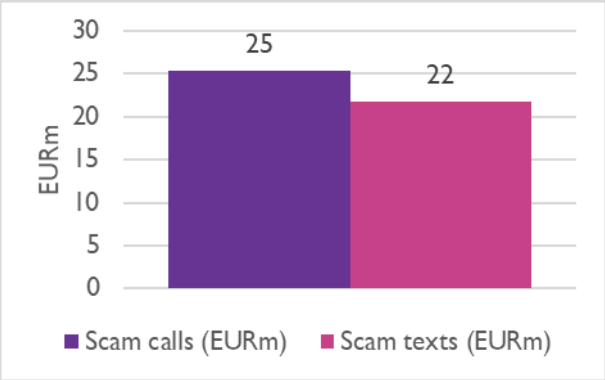
Variation 3 – Scam calls and texts actually received, restricted values (Backward looking)

In this variation, the question asked respondents to select a bin containing the value they place on not receiving the scam calls and texts they reported receiving over the last year. This approach is a backward-looking one as it focuses on the scam calls and texts survey respondents actually received in the past year only, whereas the previous approach would have included respondents' perceptions about scam calls and texts they might receive in any year. We estimate the harm by assuming that survey respondents would pay the midpoint value of the value bin they selected to pay per year. For the final bin, '€50+', we take the standard approach of using €50 as the point value, recognising that this is conservative. This value is multiplied by the scam call recipient population (and the scam text recipient population) that fell between each range by using the share of respondents in each bin. The sum of harm for each bin gives the total annual harm. We excluded from the estimation those respondents who had been victims of a scam, such that the resulting WTP represents only the 'indirect' harm from scam calls and texts such as wasted time and emotional distress.

We estimate total harm from scam calls of €25m and €22m from scam texts, in one year.

This WTP variation differs from the first two in two key ways: it asks respondents to only consider scam calls and texts they have actually received (rather than their willingness to avoid all potential / future scams); and it asks respondents to estimate an annual, rather than a monthly, figure.

Figure 8.5: Results of WTP Variation 3 – Scam calls and texts actually received, restricted values



Source: Europe Economics analysis.

Table 8.12 : Key assumptions for harm: WTP Variation 3 – Scam calls actually received

Amount bin	Share of respondents	Bin midpoint amount	Affected population	Harm (€)
0	0.27	0	962,000	0
<1c	0.03	0.01	99,000	1,000
2-99c	0.11	0.5	365,000	182,000
€1-4	0.16	2.5	531,000	1,326,000
€5-9	0.18	7	564,000	3,946,000
€10-19	0.11	14.5	365,000	5,289,000
€20-29	0.07	24.5	232,000	5,686,000
€30-49	0.03	39.5	99,000	3,929,000
€50 +	0.03	50	99,000	4,974,000

Source: Europe Economics analysis. Q.42 Thinking of all the scams calls you received in the past year, how much would you have been willing to pay per year to not receive any of them?

Table 8.13: Key assumptions for harm: WTP Variation 3 – Scam texts actually received

Amount bin	Share of respondents	Bin midpoint amount	Affected population	Harm (€)
0	0.27	0	832,000	0
<1c	0.03	0.01	89,000	1,000
2-99c	0.11	0.5	297,000	149,000
€1-4	0.18	2.5	564,000	1,411,000
€5-9	0.17	7	505,000	3,535,000
€10-19	0.1	14.5	297,000	4,308,000
€20-29	0.07	24.5	178,000	4,367,000
€30-49	0.03	39.5	89,000	3,521,000
€50 +	0.03	50	89,000	4,456,000

Source: Europe Economics analysis. Q.43 And thinking of all the scam texts you received in the past year, how much would you have been willing to pay per year to not receive any of them?

Responses to each WTP question

The table below presents the numbers of respondents informing each WTP variation.

Table 8.14: Responses informing each WTP variation

Variation	Responses
1 – contract difference	All: 1,219
2 – product purchase	1,219
3 – Scam calls and texts actually received (excl. scammed respondents)	Calls: 1,073 Texts: 969

Note: Unweighted bases of the number of responses to each question.

8.3 Harms to businesses

We estimated a range of harms for businesses as summarised in the table below. Given uncertainties around the interpretation of the WTP results, we only include estimates from our bottom-up cost modelling approach in the aggregated total. We also exclude some illustrative harms.

Table 8.15: Summary of harms to businesses

	Harm	Estimate	Approach	Inclusion in aggregated total
A	Financial loss from fraud	€8.8m	Bottom-up cost modelling	Direct costs from fraud. Included in aggregated total.
B	Opp. cost of engaging with scam calls and texts	€1.7m	Bottom-up cost modelling	Direct harm from scam coms. Included.
C	Operational cost – responding to customer queries on legitimacy	€21m	Bottom-up cost modelling	Indirect harm from scam coms. Included
D	Operational costs – Mitigation costs	€50m	Bottom-up cost modelling	Indirect harm from scam coms. Included
E	Operational costs – rearranging services	€28m	Bottom-up cost modelling	Indirect harm from scam coms. Included
F	Revenue impacts	€2.4bn	Case study, using survey results	Illustrative indirect impacts. Excluded.

G	Willingness to pay	€37m	WTP	Overlaps with BUCM. Excluded.
H	Bank refunds (amount reimbursed)	€21m	Bottom-up cost modelling (consumer survey)	Indirect costs from fraud based on consumer recovered losses. Included.
I	Bank refunds (processing)	€63	Case study, using survey results	Illustrative indirect impacts. Excluded.
Total aggregated harm (A to E + H)		**€130m**		

8.3.1 Financial loss from fraud

Table 8.16 provides the key estimates and sources for the variables used to estimate the financial loss from fraud as a result of scam calls and scam texts.

Using the business survey to calculate the total financial loss, we multiplied the estimated number of businesses that lost money by the average financial loss reported. The total harm is €8.8m in the past year. This estimate assumes no loss is recovered by businesses because the survey did not ask about how much may have been recovered.

Table 8.16 : Key assumptions for harm: financial loss from fraud

	Variable description	Estimate	Source of estimate
A	Number of businesses that lost money due to scam calls or texts	5,164	Q7b/c - base of businesses that lost money due to scam calls and texts.
B	Average financial loss as a consequence of scam calls or texts in the past year	€ 1,707	Q7b/c - Mean.
	Harm (calls and texts) = A * B	€8.8m	Assumes no loss recovered

Source: Europe Economics analysis of business survey

8.3.2 Opportunity cost of time engaging with scam

Table 8.17 provides the key estimates and sources for the variables used to estimate the harm of the opportunity cost of time engaging with scam calls and texts.

We estimated the time spent by multiplying the sum of the mean numbers of scams calls and texts received per year (51), the mean time spent engaging with an individual scammer (23.3 seconds), and the hourly wage of an employee / call handler. This was scaled to the Irish business population using the estimated number of businesses that received a scam call or text to give a total harm of €1.7m in the past year.

Table 8.17 : Key assumptions for harm: opportunity cost of time engaging with scam

	Variable description	Estimate	Source of estimate
A	Number of scam calls and texts received by an average business, in the past year	51	Q4a/4b – sum of means (29.38 + 21.65)
B	Time spent engaging with individual scam, in hours.	0.0065	Q5 - mean amongst businesses that received scam calls and texts (Q3).
C	Hourly wage of employee/call handler	€ 21.51	CSO, hourly wages for Administrative and support services, Q4 2021.
D	Number of businesses that received scam call and text in the past year	239,057	Q5 - Base of businesses that received scam calls and texts (Q3).
	Harm (calls and texts) = A * B * C * D	€1.7m	

Source: Europe Economics analysis of business survey

8.3.3 Operational cost of responding to customer queries regarding communication legitimacy

Table 8.17 provides the key estimates and sources for the variables used to estimate the cost of time engaging with customer queries regarding the legitimacy of the communications customers receive.

We multiplied the estimated number of businesses that have been impersonated as a result of scam calls and texts by the mean amount of time they spent resolving customer problems in the past year (59.2 hours) and the hourly wage of an employee / call handler (€21.51). This gives a total harm of €21m in the past year.

Table 8.18 : Key assumptions for harm: opportunity cost of time responding to customer queries

	Variable description	Estimate	Source of estimate
A	Number of businesses that have been impersonated as a result of scam calls/text	16,102	Q18 - base of businesses that have been impersonated by a scam call/text (Q16).
B	Total time spent by businesses resolving customer problems caused by impersonation scam calls/texts in the past year, in hours.	59.20	Q18 - Mean
C	hourly wage of employee/call handler	€ 21.51	CSO, hourly wages for Administrative and support services, Q4 2021.
	Harm (calls and texts) = A * B * C	€21m	

Source: Europe Economics analysis of business survey

8.3.4 Cost of mitigating against scams

Table 8.19 provides the key estimates and sources for the variables used to estimate the total cost incurred by businesses through implementing measures to prevent scam calls and texts.

We multiplied the estimated number of businesses that have implemented scam-prevention measures in the past year by the mean total cost incurred implementing these measures. This gives a total harm of €50m in one year.

Table 8.19 : Key assumptions for harm: cost of mitigating the harm caused by scam calls and texts

	Variable description	Estimate	Source of estimate
A	Number of businesses in Ireland that have implemented scam-prevention measures in the past year	96,666	Q11 - base of businesses that have put in place any scam-prevention elements against scam calls and texts (Q10).
B	Approximate total cost of implementing the various scam-prevention elements over the past year.	€ 519	Q11 - Mean
	Harm (calls and texts) = A * B	€50m	

Source: Europe Economics analysis of business survey

8.3.5 Additional expenditure on contacting customers and arranging appointments and services

Table 8.20 provides the key estimates and sources for the variables used to estimate the additional cost to businesses when reaching out to customers and conducting other tasks in the context of scam calls and texts.

We multiplied the estimated number of businesses that have experienced difficulties communicating with customers and arranging appointments and services (and have thus seen an increase in their direct costs) by the mean direct cost for businesses. The total harm is €28m in one year.

Table 8.20 : Key assumptions for harm: additional expenditure on contacting customers and arranging appointments and services

	Variable description	Estimate	Source of estimate
A	Number of businesses that have experienced difficulties communicating with customers, attributed to scam calls and texts, and have seen an increase in their direct costs.	13,838	Q24 - base of businesses that reported incurring direct costs (Q23) related to difficulties encountered due to scam calls/texts (Q21).
B	Average direct cost for businesses that have experienced direct costs in the past year	€ 1,997	Q24 - Mean amongst businesses that reported incurring direct costs (Q23) related to difficulties encountered due to scam calls/texts (Q21).
	Harm (calls and texts) = A * B	€28m	

Source: Europe Economics analysis of business survey

8.3.6 Potential impacts on revenue

Revenue at risk due to scam calls and texts

We first calculated the monetary value of revenue supported by mobile communication by multiplying the share of revenue that survey respondents said is supported by mobile communication in the last year by an estimate of the average turnover of businesses in Ireland in 2021 (see Table 8.21). This was then multiplied by the number of businesses that use calls and texts as part of their telecommunication strategy. This results in €48bn in 'revenue at risk' due to scam calls and texts in the past year. We recognise that using the 'average turnover' is a very broad measure, and therefore consider this estimate of revenue at risk to be illustrative only.

Table 8.21 : Key assumptions for harm: revenue at risk

	Variable description	Estimate	Source of estimate
A	Number of businesses that use calls/texts as part of their telecommunication strategy in the past year	161,176	Q20 - base of businesses that use mobile calls or texts as part of their telecommunications strategy (Q19/Q19a)
B	Average turnover of firms in Ireland.	€ 2.9m	CSO, Enterprises in 'total business economy', 2020: Average turnover uplifted to 2021 prices.
C	Approximate share of revenue supported by mobile communication in the past year	10%	Q20 - mean
	Harm (calls and texts) = A * B * C	€48bn	

Source: Europe Economics analysis of business survey

Revenue losses attributed to scam calls and texts

The survey asked businesses to report the approximate share of revenue lost over the past year that they attributed to scam calls and texts (referred to as 'indirect costs' in Table 8.22).

We multiplied the estimated number of businesses that reported incurring indirect costs by the mean stated share of revenue loss attributed to scam calls and texts (3.8%). Again using an estimate of the average turnover of businesses in Ireland in 2021, the revenue loss attributed to scam calls and texts is €2.4bn in the past year. This figure is subject to uncertainty, not least as it would be difficult for respondents to verify how much revenue they might have lost as a result of changing usage of calls and texts and to disentangle changes in revenue over a year from many other factors. It may also be that some of this 'lost' revenue is in fact earned through other channels. Nevertheless, this exercise provides a useful illustration of the potential scale of harm to businesses from scam calls and texts.

Table 8.22 : Key assumptions for harm: revenue loss

	Variable description	Estimate	Source of estimate
A	Number of businesses that have experienced difficulties communicating with customers, attributed to scam calls and texts, and have experienced increased indirect costs in the past year	22,143	Q25 - base of businesses that reported incurring indirect costs (Q23).
B	Share of revenue loss amongst businesses that have experienced indirect costs in the past year	3.8%	Q25 - Mean amongst businesses that reported incurring indirect costs (Q23).
C	Average turnover of firms in Ireland.	€ 2.9m	CSO, Enterprises in 'total business economy', 2020: Average turnover uplifted to 2021 prices.
	Harm (calls and texts) = A * B * C	€2.4bn	

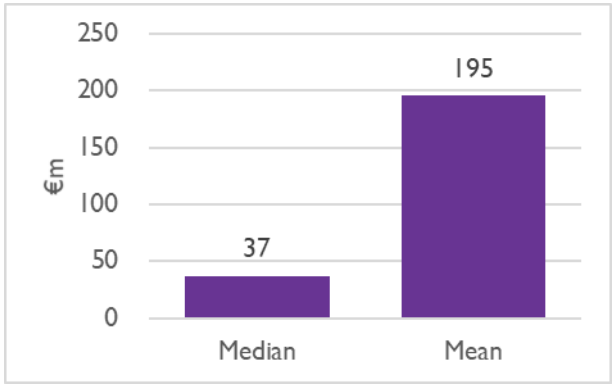
Source: Europe Economics analysis of business survey

8.3.7 Willingness to pay

The business survey included one question on the willingness to pay to avoid scam calls and texts. It asked how much firms would be prepared to pay, per month, for a product/service for its mobiles and landlines that guarantees to stop all scam calls and texts without having to take any further action. This question was asked of all businesses, regardless of whether they had received scam calls or texts.

Using the estimated number of businesses in Ireland and the mean WTP amount (€53 per month), we estimate that businesses would pay €195m per year to avoid scam calls and texts. However, the mean WTP incorporates the effects of some very high amounts, including three values of €5,000 or more. The median is a better measure of what the more typical firms will be prepared to pay. That figure is €10 per month.[151] Using the median WTP in place of the mean WTP gives a total WTP result of €37m.

Figure 8.6: Results of willingness to pay analysis, by averaging method



[151] The median WTP amongst firms that actually use calls and texts was €20 in respect of both.

Table 8.23: Key assumptions for harm: willingness to pay (all businesses)

	Var description	Estimate	Source of estimate
Base	Number of businesses in Ireland	309,057	Business survey (Q14): weighted base.
A	WTP amount	€10	Business survey (Q14): amount per month. Median
Harm	Harm = Base * A * 12	€37m	

Source: Europe Economics analysis of business survey.

8.3.8 Banks

Cost of processing refunds

The cost of processing a scam comes from our interviews with banks for this project, which suggested that the cost of processing a scam could be four-times the loss faced by the consumer, as it accounts for refunding the customer as well as other administrative work undertaken by bank staff. We apply this multiple to the value of the consumer loss that is recoverable by banks (€21m, based on results in Table 8.6), assuming that banks accept liability to recover the whole loss. We hence estimate the total cost of refunds to be €84m in one year, of which €21m is the refund itself and the remaining €63m the administration and processing costs. Given the likely differences across banks we consider the costs of processing claims sufficiently uncertain to exclude this from the aggregated total. However, the costs of the actual refunds (€21m) is based on our consumer survey and is therefore included in the total.

Table 8.24 : Key assumptions for harm: cost of processing refunds (banks)

	Var description	Estimate	Source of estimate
A	Value of total financial loss to consumers that is recovered	€21m	Value of loss recovered (calls and texts together)
B	Cost of processing refund/other admin tasks as a multiple of the recovered loss.	4	Cost of processing a scam could be 4x the loss.
	Harm = A * B - A	€63m	Assumes consumer loss is recovered from banks

Source: Europe Economics analysis of various sources.

Banks Case study: Cost to banks having to respond to customer fraud alerts

Our interviews with banks found that banks typically engage both call centre and fraud team resources to deal with waves of scams. This case study is concerned specifically with the opportunity cost of time responding to customer queries regarding the communications they receive purportedly from banks. The interviews provided a case study of a scam wave in which 10,000 calls were alerted to the bank's call centre, 400 of which were relayed to the fraud team.

We conservatively assume that call handlers – both in the call centre and the fraud team – take 5 minutes to respond to each issue. It is likely that the fraud team will spend more time beyond the initial call processing an actual fraud case, but this is in part quantified in the previous harm (the cost of processing refunds). Finally, we take estimates of average hourly earnings of call centre and fraud team resource to estimate a cost of €19,000 per scam wave. If we were to scale this up to all banks in Ireland using an approximate market share of the bank from which this case study was drawn the cost multiplies to €57,000 per scam wave.

Table 8.25 : Key assumptions for harm: cost to banks having to respond to customer fraud alerts (banks)

	Variable description	Estimate	Source of estimate
A	Number of customer scam alerts to bank's call centre in one wave of scam calls and texts.	10,000	In one wave, there were 10,000 calls in one week.
B	Number of customer scam alerts that are directed to the bank's fraud team.	400	400 of the 10,000 calls were relayed to the fraud team
C	Time allocated per customer call (hours)	0.08	Assumption: 5 minutes.
D	Cost of call handler resource (hourly).	€ 22	CSO Earnings and Labour Costs Quarterly (2021), table 2 (NACE sectors): avg hourly wages for Administrative and support services, (q4 2021)
E	Cost of fraud team resource (hourly).	€ 37	CSO Earnings and Labour Costs Quarterly (2021), table 2 (NACE sectors): avg hourly wages for information and communication, (q4 2021)
F	Value of call centre resource dedicated to responding to a scam wave = A * C * D	€ 17,925	Calc, per major bank
G	Value of fraud team resource dedicated to responding to a scam wave = B * C * E	€ 1,239	Calc, per major bank
	Harm to one bank = F + G	€19,000	Calc, per scam wave

Source: Europe Economics analysis of various sources.

8.4 Harms to public bodies

Estimating country-wide harms to public bodies was not possible in this study as public bodies are unique with many unique harms, and thus extrapolating estimates from our fieldwork was not feasible (in the same way that we were able to do for consumers and businesses). In addition, there is limited data available on harms to public bodies, such that our estimates are illustrations only of selected harms, and our aggregated figures should be considered only partial estimates of harm These estimates are our own, informed by our discussions with the organisations listed rather than provided by them.

8.4.1 An Post

As set out in Chapter 3, a key cost to An Post and other delivery companies would be the operational costs of dealing with missed deliveries as a result of customers not responding to reminder SMS if they suspect these of being spam. This could include drivers having to re-deliver parcels, or An Post setting up and maintaining parcel redelivery or collection IT systems and hubs. Whilst it is likely that this is a key cost implication of scam texts, it is not possible to quantify given a lack of data on the proportion of missed deliveries that is driven by customers being suspicious of a scam culture, and the costs of resolving these missed deliveries.

One-off cost to direct mail campaign to Irish households

Public bodies may feel the need to respond to scam calls and texts by alerting consumers to the dangers of the scams and encouraging them to remain vigilant. Such campaigns may take the form of media adverts and mail campaigns. As an illustrative example, an awareness campaign by An Post via a direct mail to every household in Ireland (1.6 million suggested by An Post) would cost approximately €1.3m. This assumed a mailing unit cost of €0.84 based on the price for commercial customers of sending more than 500,000 50g

letters through An Post's 'PostAim' service.[152] We note that the actual cost for An Post sending this mail itself is likely to be lower. On the other hand, this estimate does not account for the costs of designing, reviewing and printing the mailings.

8.4.2 An Garda Síochána

Additional costs of personnel

Our interview with An Garda Síochána raised the concern that increased scam activity seen of late has resulted in an increased demand for personnel within the specific fraud team we spoke to, the Garda National Economic Crime Bureau (GNECB). We conduct an illustrative estimation of the resource implication of this, acknowledging that this may not represent an actual increase in costs e.g. if these resources were displaced from another part of the Gardai.

The GNECB suggested that an additional dedicated sergeant and five fraud analysts would be required to deal with the additional workload in the department. Assuming an hourly rate for all personnel,[153] this would amount to around €400,000 a year. This could cover all types of fraud and so would not be exclusive to scam calls and texts but provides an illustrative example of the magnitude of the potential costs.

8.4.3 The Health Service Executive (HSE)

HSE Case Study 1: Harm from Did Not Attends (DNAs)

Our interview with the HSE added to the evidence from the literature that health care providers can incur costs from excessive numbers of missed appointments ('did-not-attends', or DNAs). We estimate this cost on the evidence-based assumption that text reminders sent to outpatients can reduce the number of DNAs. The approach assumes that the erosion of trust in texts caused by scam communications translates directly into outpatients ignoring their text reminders and not attending their appointments. Our estimates are based on data from the literature and our consumer survey, rather than information directly provided by the HSE.

The crucial component is the reduction in non-attendance due to text reminders. The literature provides multiple candidate options for this. Chen et al (2008) used a randomised controlled trial (RCT) in China and found that attendance rates among participants at health promotion centres who received text reminders improved by 7 percentage points (p.p.) relative to control group.[154] Similarly, Youssef (2014) conducted a RCT in Saudi hospitals and found text reminders reduced non-attendance rates by 10.3 p.p. overall.[155] A review from 2011 cited by the Department of Health (2019) found that 28 of 29 international studies found positive results and reduced DNAs by 34% on average.[156] We use Yousef's result as a central estimate as it benefits from being more recent than Chen et al. and the 2011 review. This is important as it is more likely to capture contemporary levels of reliance on mobile devices. The reporting of percentage-point change also aligns with our approach.

An estimate of the cost per DNA in Ireland is taken from HSE/BIU: €21 (in 2021 prices).[157] Using the number of appointments made in the year of the HSE/BIU source (2017), 3.79m, and Youssef's estimate of the

[152] An Post, PostAim [online] [accessed November 2022].
[153] €32 per hour - CSO Earnings and Labour Costs Quarterly (2021), table 8b (public sector): average hourly wages for An Garda, (q4 2021)
[154] Chen et al. (2008) 'Comparison of an SMS text messaging and phone reminder to improve attendance at a health promotion center: a randomized controlled trial' [online]
[155] Youssef, A. (2014) 'Effectiveness of text message reminders on nonattendance of outpatient clinic appointments in three different specialties: A randomized controlled trial in a Saudi Hospital' [online]
[156] Department of Health (2019) 'Using SMS Reminders to Reduce Non-attendance at Hospital Appointments: an Umbrella Review of Key Issues' [online].
[157] HSE/BIU/Plunkett, O. (2018), letter in response to PQ 15609/18 [online]: cost per DNA of €20.

reduction in non-attendance due to text reminders, we estimate the total cost savings that may be attributed to text reminders in a year: €8m.

We then assessed the impact of scam texts on these cost savings realised by text reminders, by assuming that scam texts erode the trust placed in these reminders. The consumer survey is used to inform the erosion in trust: we identify the share of adults who reported using text services for health reminders *and* who have stopped responding to text messages from public bodies. This value is then multiplied by the reduction in the non-attendance due to SMS reminders. This results in an estimated harm from increased DNAs at €3.8m in one year. Table 8.26 summarises the inputs and calculation steps.

Table 8.26: Key assumptions for harm: increased operating costs due to Did Not Attends (HSE)

	Variable description	Estimate	Source of estimate
A	Cost per DNA	€21	Plunkett/HSE/BIU (2018, 2018 prices): cost of missed new and review hospital appointments, €20
B	Number of appointments made in a year	3,787,972	Plunkett/HSE/BIU (2018): Number of appointments made in 2017: 3,787,972
C	Reduction in non-attendance rate due to SMS reminders	-0.103	Youseff (2014): Percentage point reduction in overall hospital outpatient nonattendance rate due to receiving SMS reminders: 10.3 p.p.
D	Cost savings from text reminders = A * B * C	-€8m	Calc
E	The share of people who use SMS for health reminders and have stopped responding to text messages from public bodies.	47%	Consumer survey: the share of people who use SMS for health reminders (Q40) and have stopped responding to texts from public bodies (Q38).
F	C * E = Share of people who use SMS for health reminders and could have attended their appointment, but have stopped responding to texts from public bodies due to awareness of scam texts.	5%	Calc
	Harm = A * B * F	€3.8m	

HSE Case Study 2: Harm from increased operating costs due to HSE's cybersecurity measures

Our fieldwork highlighted that the HSE faces increased operating costs due its cybersecurity measures, which include tackling scam calls and texts. This total harm has two base components: the annual cost of fraudulent website monitoring and takedown,[158] and the cost of hiring staff. The first component uses an annual cost of monitoring fraudulent websites, the number of fraudulent websites identified per day, an assumed share of identified websites that are taken down (100%) and the cost per website takedown. Given the above, we estimated the cost of fraudulent website monitoring and takedown of €1.7m for a year. This illustrative estimate is likely to be the upper bound for any organisation, given the HSE's size and complexity and propensity to be impersonated by scammers.

We assumed one FTE is tasked with managing and liaising with internet service providers to track whether the identified fraudulent website domains have been taken down. We assume that this occupies a third of an employee's time during working hours. Thus the second component consists of multiplying this FTE by a CSO estimate of the average hourly wages in health, an additional cost of €25,500.

[158] This entails following up on suspected fraudulent websites which are used as links in scam texts to collect information from victims.

Table 8.27 : Key assumptions for harm: increased operating costs due to HSE's cybersecurity measures

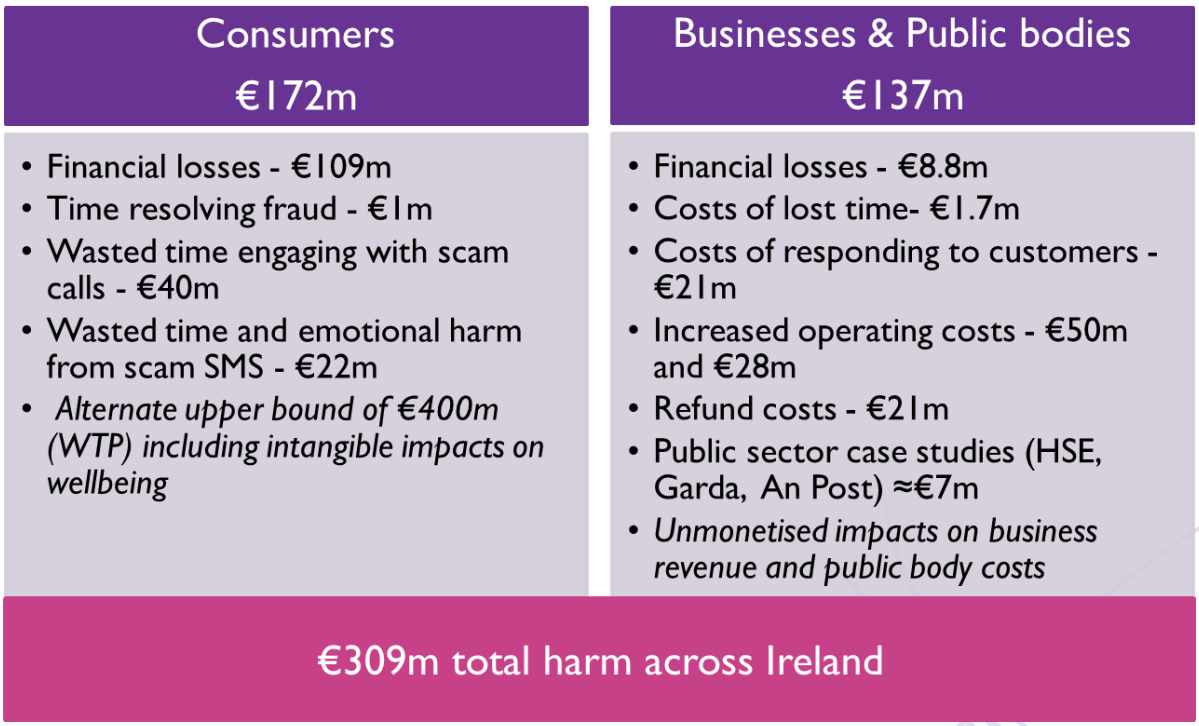
Variable description	Estimate	Description of estimate
Annual cost of monitoring fraudulent websites.	€ 250,000	The cost of monitoring to identify the scam HSE websites that are shared via spoofed texts.
Number of fraudulent websites identified per day	5	4-5 sites found per day.
Share of websites taken down	100%	Assumption: 100 percent of the websites Identified are taken down
Cost per website takedown	€ 800	Cost of website take-down
FTE time employed to ensure websites are taken down every day in hours	2.6	Assumption: one FTE is tasked with managing and Liaising with internet service providers to track whether the identified fraudulent website domains have been taken down. We assume a third of an employee's time is occupied by this.
Cost of FTE (hourly)	€ 37.17	CSO Earnings and Labour Costs Quarterly (2021), table 2 (NACE sectors): avg hourly wages for information and communication, (q4 2021)

Source: Europe Economics analysis of various sources.

8.5 Summary of harms

The figure below summarises the quantified harms across Irish stakeholders.

Figure 8.7: Summary of harm from scam communications in one year

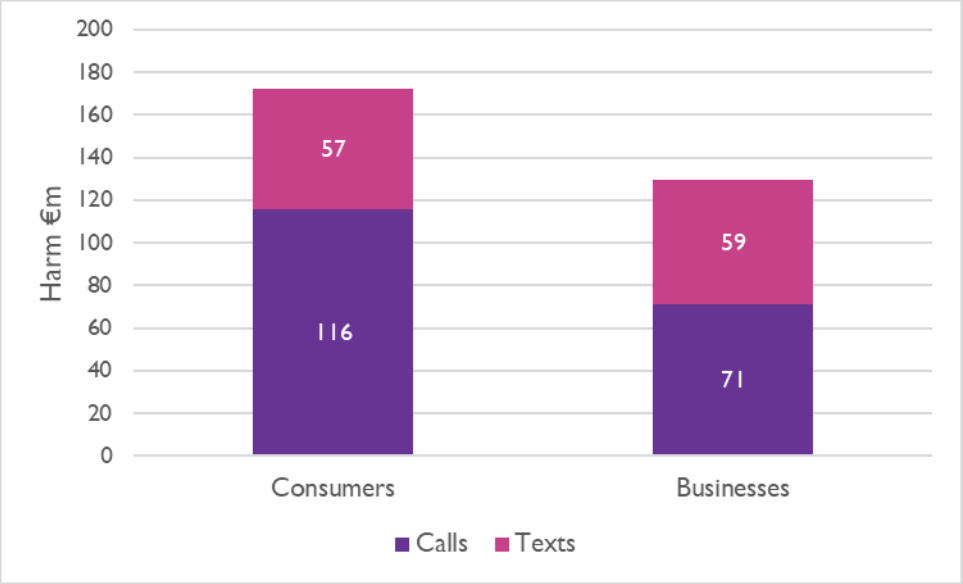


Source: Europe Economics analysis. Values may not add due to rounding

8.5.1 Split of harm between calls and texts

The consumer and business harm is split between calls and texts as shown in the figure below.

Figure 8.8: Split of consumer and business harm between calls and SMS in a year (€m)



Source: Europe Economics analysis

9 Appendix 2: Cost and Benefits of Interventions

9.1 Modelling methodology

Our approach to modelling the costs and the benefits of the interventions can be divided into four steps:

- We produced estimates of the costs of the interventions. This was informed by discussions with ComReg, the operators interviewed in the fieldwork phase of this project and information provided by vendors and other national regulatory authorities (NRAs). For some interventions, ComReg shared nonbinding quotes received from vendors which were used in our calculations. The costs are split between one-off costs (incurred in the year of implementation) and ongoing costs (incurred every year thereafter). We estimate the costs across a range of industry stakeholders.

- We modelled the ongoing level of harm from scam calls and texts that could be experienced in the absence of the technical interventions – the counterfactual. The benefits from the interventions are therefore estimated in relation to this counterfactual harm.

- Our framework for estimating the benefits of the interventions was to estimate the extent to which each intervention would reduce the harms to consumers and businesses presented in Chapter 3. The effectiveness of the interventions was informed by information provided by mobile network operators (MNOs), vendors and other NRAs and our understanding of scammers' behaviour as explored in Chapter 2.

- In the final step we compared the costs and benefits of each intervention over time and made recommendations on the interventions to implement in order to reduce the harm from scam calls and texts in a proportionate manner.

9.1.1 The intervention period

We have modelled the costs and benefits of the interventions over seven years, representing the time period over which the interventions are likely to be effective before existing infrastructure and technology become obsolete.

The two firewall-based interventions, namely the Voice Firewall and SMS Scam filter, are less exposed to the risk that future developments render them obsolete, given their ability to dynamically adapt to new threats. For this reason, the benefits of the firewalls may continue for a longer period than the seven years analysed here.

All costs and benefits over the intervention period have been discounted to present values using the standard social discount rate in Ireland of four per cent.[159]

[159] Department of Public Expenditure and Reform (2019). 'Public Spending Code: Central Technical References and Economic Appraisal Parameters'. p.11 – [online]

9.2 The counterfactual harm

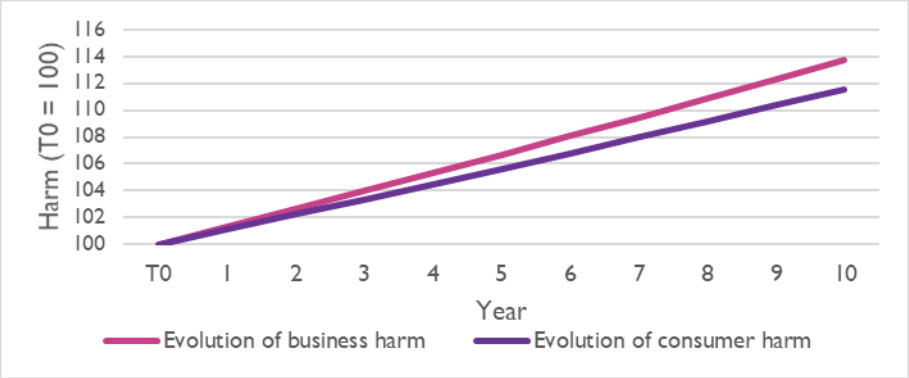
The starting point for constructing the counterfactual was to identify the range of factors that could influence the level of harm from scam calls and texts experienced in the coming years. This includes population growth, mobile and fixed line usage, internet use, and scammers' abilities. We considered it most practical (and transparent) to focus on variables that capture one or more of these factors, to avoid the complexity that comes with a counterfactual that needs to integrate multiple competing variables.

For this purpose, we chose variables that capture consumer and firm population growth. These both account for the number of consumers and firms that can be targeted by scammers and are a proxy the evolution in overall telecom device usage. For consumers, we use the compound average growth rate of persons over 15 in Ireland between 2021 and projected in 2031,[160] 1.1%. For firms, we use the compound average historical growth rate of enterprises in Ireland over 2010-2020,[161] 1.3%. These growth rates are assumed to reflect the annual growth over the implementation period.

This baseline counterfactual implicitly assumes that (absent any ComReg interventions) developments in either the ability of consumers/businesses to avoid scams, or the ability of scammers to outwit consumers, balance each other out such that the prevalence and impact of scams grow linearly with population growth.

The growth in harms for consumers and businesses is shown in Figure 4.30. The chart is indexed such that the year for which the harms were calculated in Chapter 3 is equal to 100 (in 'T0' in the chart).

Figure 9.1: The evolution of harms to consumers and businesses in the baseline counterfactual (T0 = 100)

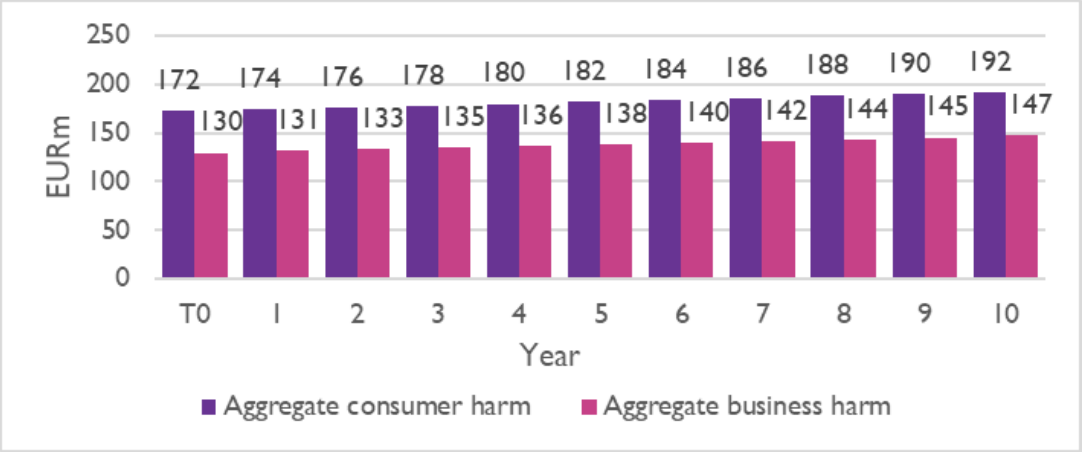


Note: T0 refers to the year for which the harms are calculated in Chapter 3.

Figure 9.2 illustrates the total annualised harm for consumers and businesses over a 10-year horizon.

[160] CSO, cited in Pensions Committee (2021) [online]
[161] CSO 'Business Demography 2020' [online]

Figure 9.2 : Total annualised harm for consumers and businesses over a 10-year horizon



Source: Europe Economics analysis. Note: T0 refers to the year for which the harms are calculated in Chapter 4.

9.2.1 Alternative counterfactual scenarios

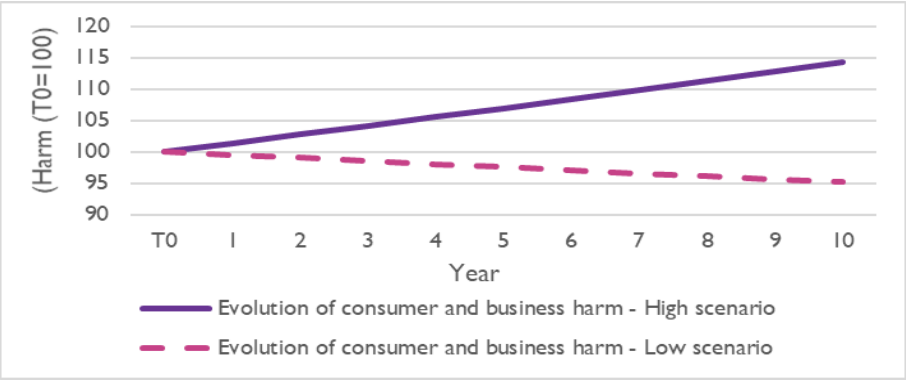
We also estimated illustrative alternative scenarios for harm under the counterfactual for businesses and consumers. These reflect the possibility that the implicit assumption in the baseline counterfactual does not hold, and instead consumers and firms become more capable of avoiding scams and/or scammers move their attention away from Ireland, for example. We note that the construction of the counterfactual scenarios makes use of proxy variables and the results should be considered as indicative estimates in the absence of sufficient data on the evolution of the impact of scams.

The alternative counterfactual scenarios are as follows:

- High harm scenario – For the high scenario, we used the growth rate in smartphone usage (1.3 per cent compound annual growth rate between 2018 and 2024) which outstrips population growth. This is based on the assumption that as consumers and businesses use mobile communications more, scammers develop new, more successful scams.
- Low harm scenario. For the low scenario, to proxy consumers and businesses becoming more savvy to scams we used an indicative negative growth rate growth rate of -0.5 per cent.

The growth in harm under the high and low scenario for consumers and businesses is shown in Figure 9.3.

Figure 9.3 : The evolution of harms to consumers and businesses in the high and low scenario (T0 = 100)



Source: Europe Economics analysis. Note: T0 refers to the year for which the harms are calculated in Chapter 4.

For the rest of our analysis we use the central counterfactual.

9.3 The costs of the interventions

Chapter 5 sets out a description of the costs entailed for each intervention. We estimated the one-off and ongoing costs of implementing the proposed interventions over the seven-year intervention period. The general approach assumed that the one-off costs of each intervention would be incurred in the first year of implementation, which is "year 1" for most of the interventions. The exceptions are where certain setup costs are split between years 1 and 2 for: V2 (VoLTE) setup costs in the Mobile CLI blocking intervention; setup costs for the Full SMS Sender ID Registry; and regulator setup costs and aggregator sender ID connection costs in the Phased-in Full SMS Sender ID Registry. The ongoing costs of each intervention are incurred in the subsequent years and do not vary from year to year. For simplicity, we have also assumed that costs are incurred at the beginning of the year.

Given the nature of the interventions (largely fixed investment costs[162]) we assume that the costs to each stakeholder within a stakeholder group are the same regardless of their size. For example, the cost of an intervention to an operator would be the same for all operators. Table 9.1 sets out the number of operators and aggregators assumed for each relevant intervention, as informed by ComReg.

Table 9.1 : Number of operators and aggregators per intervention (large grouping)

Intervention	Number
DNO/PN	30 operators
Fixed CLI call blocking	10 International Gateway Operators
Mobile CLI call blocking	4 largest operators
Voice firewall	5 largest operators
SMS registries	3 enabling operators 30 aggregators
SMS scam filter	4 largest operators

Our sensitivity analysis includes a smaller grouping of operators for the Voice firewall and SMS scam filter interventions – three MNOs each.

For the SMS registry interventions, which would require Sender ID owners to register, we assumed 500 Sender ID owners for the Full sender ID registry and 50 for the Partial sender ID registry.

For estimated project costs we constructed costs based on FTEs and project time. Hourly rates are sourced from the CSO and ComReg: €30 per hour for a business analyst, €70 per hour for an IT specialist/engineer.[163]

9.3.1 DNO/PN

We understand that these two interventions are typically implemented simultaneously by operators as they make use of the same technical solution. Based on ComReg and stakeholder estimates we use a one-off cost per operator of around €30,000 to cover the time needed to specify, implement and test the interventions, with a small ongoing cost to manage changes to the two lists of around €3,000 a year per operator.

ComReg would incur costs of staffing from the setup of the DNO and PN databases and from the establishment of associated processes and procedures. These are assumed to be part of BAU costs.

[162] We note that some firewalls offered by vendors are subscription-based services with no fixed upfront investment costs. Our cost models assume an element of up-front software and project costs.

[163] CSO, 2021 Q1 - [online]

9.3.2 Fixed CLI blocking

One-off project development costs would by incurred by operators and include around 80 FTE days for a team to implement and test a fixed international CLI blocking solution, with minimal identified ongoing costs. This reflects the reliance of this intervention on existing network switch capabilities.

9.3.3 Mobile CLI blocking

Whilst this intervention would also mainly rely on existing network switch capabilities, we assume some material one-off costs covering both software and project costs for some operators to implement a solution to verify the validity of mobile CLIs. A key element here is developing operators' ability to check the roaming status of both their and other operators' customers' mobile numbers. This would entail changes to operators' core networks. However we assume that only large operators will incur this cost, with smaller operators achieving this through re-routing their traffic via the big operators. We estimate a one-off cost of around €300,000 per large operator for the relevant software, and around €60,000 in internal development and project costs.

A further element of cost would be incurred by the same large operators over years 1 and 2 as delivery of mobile services via VoLTE increases. This is in anticipation of needing a new reconfiguration to check roamer status in a VoLTE landscape, and is estimated at around €500,000 per large operator. This would include around €250,000 for a shared solution and €250,000 for a VoLTE roaming product, both largely software costs.

Ongoing costs would largely become business as usual (BAU) in time but would include additional vendor operational expenditure, which we estimate at around 20 per cent of one-off software costs.

Our estimates for fixed and mobile CLI blocking are based on the assumption that these changes are made to existing platforms – costs may vary if operators choose to build new capabilities for both interventions together.

9.3.4 Voice firewall

Given the novelty of Voice firewalls, we use broad cost estimates based on vendor quotes. We assume that one-off costs for the software would be around €580,000 and €310,000 for optional vendor items (software licenses, extra signalling and 50tps license) per operator, plus further project costs for operators to develop new platforms of around 30 per cent of the software cost. Ongoing costs are estimated at 20 per cent of software costs, reflecting new staff/services to manage the technology and ongoing vendor service payments.

9.3.5 SMS Sender ID registry

The specifications of a sender ID registry that we analyse are as follows:

- Partial sender ID registry: requiring specific organisations to register their sender IDs with ComReg;
- Full sender ID registry: requiring all sender ID owners to register their sender IDs with ComReg; and
- To account for a Full sender ID registry implemented in stages, a Phased-in Full sender ID registry.

The first two specifications are described in Chapter 4. The partial registry is implemented and becomes effective in year 1. The setup costs of the full registry are incurred in years 1 and 2, and the benefits are experienced in year 3. The phased-in full variation considers the scenario in which the partial registry is implemented first and is active in years 1 and 2, during which time costs are also borne for the introduction of a full registry which becomes active in year 2.

Operators and aggregators

There would be one-off costs of €150,000 for each operator and €100,000 for each aggregator to develop the required infrastructure (internal project and development costs). On top of any charge the operator may impose on the aggregator, we anticipate that aggregators will incur a costs to set up each connection with sender ID owners:

- In the partial registry, the per-connection cost is €4,000 in respect of 50 large sender ID owners.
- In the full registry, the per-connection cost is €4,000 in respect of 100 large sender ID owners and €750 in respect of the remaining 400 sender IDs. The rationale is that smaller ID owners would pay less for cheaper SMS services than 100 main large organisations.
- In the phased-in full registry, 50 sender IDs are connected at a cost of €4,000 in year 1, and the remaining 50 at the same rate, plus 400 sender IDs at €750 each in year 2.

We assume that businesses with sender IDs are connected to one aggregator each.

Operators would incur ongoing costs of adjusting the firewalls once new CLIs enter the registry – equal to a few days' FTE time per month. We have not assumed any material ongoing costs for aggregators.

Senders and the regulator

ComReg would incur costs as part of implementing the SMS registry. Part of this cost would stem from an upfront cost to update IT equipment and the development of a portal. This is assumed to amount to €150,000. Further one-off costs would be incurred equivalent to 1 FTE for project costs. ComReg estimates that it would need 4.5 FTEs on an ongoing basis to oversee and manage the registry, based on equivalent resources needed in the Singapore model. These costs are assumed to be equal in the partial and full registries, except that they are split between years 1 and 2 in the two full registry specifications.

Sender ID owners may incur costs from this intervention including a one-off registration fee and ongoing Sender ID renewal fee to ComReg, and service charges to aggregators and potentially operators. These are assumed to be transfer costs from ComReg and aggregators.

Using the above costs, we estimate a series of one-off and ongoing costs to operators, aggregators, the regulator. Table 9.3 to Table 9.5 summarise the total costs incurred by each stakeholder. Table 9.6 presents the total cost across all stakeholders.

9.3.6 SMS scam filter

For the SMS scam filter, we estimate a one-off software cost of €426,000 plus €270,000 of optional vendor items (software licenses of 5tps, 50tps and 200tps plus deployment costs). This estimate was informed by a quote provided by a vendor. An ongoing cost of 20 per cent of the one-off vendor costs (excluding professional fees, testing, training) is assumed to account for the additional complexity of the intervention and ongoing vendor fees.

We assume that the SMS scam filter is implemented without any delay due to the need for supporting legislation. Any delay in the passing of this legislation could result in continued consumer harm and undermine the effectiveness of this intervention. This is necessary to simplify our analysis, given the uncertainty inherent in predicting the passing of legislation. However, we note that any such delay results in large harm to Irish consumers and businesses, with a 1-year delay resulting in a reduction in net benefit of €93m over seven years.

9.3.7 Summary of costs by stakeholder

The tables below summarise the costs for each intervention and the affected industry stakeholders.

Table 9.2: Description of intervention costs

Intervention	One-off costs	Ongoing costs	Affected stakeholders
DNO / PN blocking	Internal costs to implement the blocks – business case design, testing, configuration.	Updating the lists and change requests.	Around 30 operators
Fixed CLI blocking	Internal project costs to implement and test the solutions.	No material ongoing costs identified.	Around 10 International Gateway Operators (IGOs)
Mobile CLI blocking	V1 – internal costs to design and test on-net roamer checks, plus software costs to extend roamer checks to other operators' customers. V2 – costs of shared solution between main operators (including proxy servers) and solutions for VoLTE roaming. Internal project and infrastructure costs plus software costs.	Ongoing software costs (20%)	Three main MNOs plus one large IGO. Other operators assumed to be able to route traffic over the proxy server solution.
Voice firewalls	Vendor costs and internal project costs to implement the solutions.	Ongoing vendor costs (20%)	Three main MNOs plus two large fixed operators for the Large Grouping scenario.
Full and partial sender ID registry	Operators – internal development costs to update filtering (design, configuration, testing); costs of new connecting aggregators.	Updating connections to new aggregators and new IDs.	3 enabling operators
	Aggregators – internal development costs to make new connections to operators; business costs of onboarding ID senders.	Updating connections to new aggregators and new IDs.	10 large and 20 smaller aggregator
	ComReg – IT development to set up registry and portal	Assume all connections made up-front so minimal ongoing costs. Updating registry	ComReg
	Sender ID owners – costs of connecting to aggregators and registry fees to ComReg. Note that sender ID costs would represent transfers from aggregators and ComReg, so not modelled explicitly.		500 in total. 100 classified as 'large' senders.
SMS scam filter	Vendor costs and internal development costs.	Ongoing vendor costs (20%)	3 main MNOs plus 1 large fixed operator for the Large Grouping scenario.

The tables below present the one-off and ongoing costs for each intervention across the various stakeholders. We present the total costs for each population, as well as the cost per individual stakeholder.

Table 9.3 : Operators: total one-off and ongoing cost over the 7-year intervention period (€)

Intervention	Total one-off cost	Total ongoing cost	One-off cost per stakeholder	Ongoing cost per stakeholder
DNO/PN	981,000	100,800	32,700	3,360
Fixed CLI blocking	462,000	0	46,200	0
Mobile CLI blocking with VoLTE after 2 years	1,424,000 (3,424,000 with VoLTE)	240,000 (640,000 with VoLTE)	356,000 (856,000 with VoLTE)	60,000 (160,000 with VoLTE)
Voice firewall	5,918,500	890,000	1,183,700	222,500
Partial sender ID registry	450,000	60,480	150,000	20,160
Full sender ID registry	450,000	60,480	150,000	20,160
Full (phased-in) sender ID registry	450,000	60,480	150,000	20,160
SMS scam filter	4,384,000	392,000	1,096,000	98,000

Note: The number of stakeholders for each cost category maps onto Table 9.2 above. Only key stakeholders who would bear the material costs of the interventions are considered.
Source: Europe Economics analysis.

Table 9.4 : Aggregators: total one-off and ongoing cost over the 7-year intervention period (€)

Intervention	Total one-off cost	Total ongoing cost	One-off cost per stakeholder	Ongoing cost per stakeholder
DNO/PN	0	0	0	0
Fixed CLI blocking	0	0	0	0
Mobile CLI blocking	0	0	0	0
Voice firewall	0	0	0	0
Partial sender ID registry	3,200,000	0	106,667	0
Full sender ID registry	3,700,000	0	123,333	0
Full (phased-in) sender ID registry	3,700,000	0	123,333	0
SMS scam filter	0	0	0	0

Source: Europe Economics analysis.

Table 9.5 : Regulator: total one-off and ongoing cost over the 7-year intervention period (€)

Intervention	Total one-off cost	Total ongoing cost
DNO/PN	0	0
Fixed CLI blocking	0	0
Mobile CLI blocking	0	0
Voice firewall	0	0
Partial sender ID registry	210,940	360,000
Full sender ID registry	210,940	360,000
Full (phased-in) sender ID registry	370,940	360,000
SMS scam filter	0	0

Source: Europe Economics analysis.

Table 9.6 : Total one-off and ongoing cost over the 7-year intervention period LARGE GROUPING (€000s)

Intervention	Total one-off cost	Total ongoing cost
DNO/PN	981	605
Fixed CLI blocking	462	nil
Mobile CLI blocking with VoLTE after 2 years	3,424	3,440
Voice firewall	5,919	5,340
Sender ID Registry (Partial)	3,861	2,523
Sender ID Registry (Full)	4,361	2,102
Sender ID Registry (Full phased-in)	4,521	2,523
SMS scam filter	4,384	2,352

Source: Europe Economics analysis. Values not discounted.

Table 9.7 : Total one-off and ongoing cost over the 7-year intervention period SMALL GROUPING (€000s)

Intervention	Total one-off cost	Total ongoing cost
DNO/PN	981	605
Fixed CLI blocking	462	nil
Mobile CLI blocking with VoLTE after 2 years	3,424	3,440
Voice firewall	3,551	3,204
Sender ID Registry (Partial)	3,861	2,523
Sender ID Registry (Full)	4,361	2,102
Sender ID Registry (Full phased-in)	4,521	2,523
SMS scam filter	3,288	1,764

Note: Small Grouping changes the number of affected operators from five and four in the Voice firewall and SMS scam filter interventions to three in each.
Source: Europe Economics analysis. Values not discounted.

9.4 The benefits of the interventions

9.4.1 The approach

We are not aware of any other study that has estimated the benefits of interventions to counter scam calls and texts.[164] There is particular uncertainty due to factors such as the unknown number of scams, the novelty of interventions and the general lack of data in this area. We were able to make use of the large consumer and business surveys, plus insights from ComReg and the industry, enabling this report to be based on a robust empirical estimation of the harms from scam communications along with informed estimates and logical modelling of the effectiveness of each intervention.

We estimated the benefits of implementing the interventions over periods of seven years. For DNO/PN and Fixed CLI blocking, the benefits (i.e. the amount by which they reduce the harm from scam calls and texts) begin to be felt the year the intervention is implemented (year 1). The benefits of the remaining interventions are experienced with a one-year lag – to account for the time taken to implement the infrastructure – with the exception of the Full SMS Sender ID Registry which brings benefits in year 3.

For simplicity, similar to the intervention costs, we have assumed that the benefit of each intervention will come into effect at the beginning of the year.

[164] We note the study done by the ACMA in Australia, which considered the impacts of a small set of interventions on costs caused by scam calls. ACMA (2020) 'Reducing the impact of scam calls: Regulation Impact Statement' [online]

In order to estimate the impact of each intervention over time, we determined the percentage reduction in scam calls and texts each intervention that would have over the intervention period. We consider two stages of impact to capture the possibility that the immediate effects wane over the implementation period.

- Initial impact – This refers to the immediate percentage reduction in scam calls and texts each intervention would have the year it is implemented.
- Impact with decay – This refers to the percentage reduction in scam calls and texts each intervention would have after two years. This captures the possibility that the intervention may be less effective compared to when first implemented (initial impact) due to scammers using work-arounds and new approaches. We have assumed that the Voice firewall and Scam filter interventions do not experience a reduction in effectiveness as these are based on machine learning and designed to adapt to scams.

Table 9.8 reports the percentage reduction in scam calls and texts for each intervention. For simplicity and based on expert opinion we have assumed that 50 per cent of all scam calls are fixed CLI spoofing, with 50 per cent from mobile CLI spoofing. This means that the reduction in fixed CLI scams that is experienced as a result of the DNO/PN[165] and Fixed CLI blocking interventions applies to 50 per cent of all calls. The same rationale is applied to Mobile CLI blocking.

The business harms have been estimated in aggregate (the amount lost due to scam calls and texts). To assess the effectiveness of the interventions, we have attributed roughly an equal weight to the proportion of harm caused by scam calls and texts. This decision has been informed using the proportion of businesses that indicated they had received a scam call or text in the business survey.[166]

Our understanding of the effectiveness of interventions is informed by discussions with MNOs as well as information provided to it by vendors and other NRAs and our understanding of scammers' behaviour as explored in Chapter 3. We note that this requires assumptions given the inherent uncertainty in the effectiveness of interventions, many of which are new and only just subject to testing or early implementation in other countries. Nevertheless, we have attempted to find and draw upon publicly available information is available on interventions effectiveness, where possible. The table below summarises the evidence on effectiveness presented in Chapter 5 and how this has been used to assess the effectiveness of each intervention for the modelling.

[165] An operator shared confidential data on the blocking activity during first months of the DNO and PN list operation in Ireland. This supports the assumption that the calls captured by the DNO and PN interventions constitute a subset of scam calls presenting with fixed CLIs.

[166] Business survey Q.3 Has your business received scam calls or sms (texts) in the past year? 68 per cent of respondent said that they received scam calls with 56 per cent scam texts. This implies a share of 55 per cent and 45 percent respectively.

Table 9.8 : Intervention effectiveness evidence and assumptions

Intervention	Country	Source	Evidence	Our assumptions	Initial impact (%)	Decay impact (%) (after 2 years)
DNO/PN	UK	Talk Talk	TalkTalk has seen a 65 per cent reduction in complaints about scam calls since it introduced the measures. Ofcom estimated that about 700,000 people received spoof calls in the three months to August 2022. [online]	We assume 5 per cent of fixed CLI scam calls. Effectiveness would decay over time as scammers shifted away from spoofing DNO/PN numbers towards other fixed CLIs.	-5	-3
	Ireland	Large IGO	Irish operator data shows that DNO number spoofs are low in Ireland (1-2% of calls), but that list is currently very small. May increase as list expands			
Fixed CLI blocking	Australia	Regulator	The Australian Competition and Consumer Commission's Scamwatch says that between 1 January and 13 November this year, reports about phone scams decreased by 61% from 135,400 in 2021 to 57,400 this year. The reduction is being credited to the scam calls code the industry brought in to identify, block and trace incoming calls from scammers in 2020. More than 549m calls have been blocked by telcos since the scam code was introduced.[online]	Intervention would initially address 90% of fixed CLI scam calls. Decay in effectiveness due to scammers shifting towards non-spoofed international numbers or spoofed UK CLIs which Irish consumers may still trust.	-90	-80
	Norway and Other Scandinavian countries	Telia	Millions of calls being blocked by Telia in Norway and other Scandinavian countries due to Fixed CLI blocking [online]; [online]; [online]			
	Ireland	Large IGO	Majority of scam calls coming from international fixed and mobile CLIs			
Mobile CLI blocking	Finland		Little experience with this intervention in other jurisdictions. Finnish regulator expects intervention to be largely effective against spoofed mobile CLIs from international sources.	Intervention would address 90% of spoofed mobile CLI calls. Decay would arise if scammers used legitimate Irish SIM cards	-90	-80

				to make scam calls. Assume equivalent decay to fixed intervention.		
Voice firewall	International	Vendor	- International vendors tell ComReg they expect firewall to be highly effective at blocking voice scam calls ("in the 90s")	The firewall would address 90% of remaining scam calls, after the preceding interventions. No decay in effectiveness assumed given dynamic solution.	-90	-90
	UK	Operator	Everything EveryWhere (EE) in the UK is blocking as many as two hundred million scam calls in a year, following the introduction of an artificial intelligence based "anti-spam filter" in 20211.			
SMS registry (full)	Singapore		The IMDA's registry appears fairly successful to date. There has been a 64% reduction in scams through SMS from Q4 2021 to Q2 2022. Scam cases perpetrated via SMS make up around 8% of scam reports in Q2 2022, down from 10% in 2021.	Intervention would apply to all scam texts spoofing sender IDs (assumed to represent the bulk of scam texts causing harm). Some decay as scammers shift to non-sender ID scams.	-65	-60
SMS registry (partial				Same as above, with adjusted effectiveness to represent partial registry consisting of the most commonly spoofed organizations' IDs.	-55	-50
Scam filter	UK	EE	- Scam filter technology has blocked over 11 million scam texts since its inception in July 2022.[online]	The firewall would address 85% of remaining scam texts, after the preceding interventions. No decay in effectiveness assumed given dynamic solution based on machine learning and ability to adapt to scammers' workarounds.	-85	-85
		VF	- International experience shows firewalls blocking millions of scam texts per month, with Vodafone reporting a 76% reduction in scam texts.			

	Australia	Telstra	In April 2022, technology had blocked over 185 million scam text messages in the three months to July and 225 million to December.			
		Optus	Between 1 December 2020 and 31 March 2022, Optus blocked more than 232 million scam calls and now block an average of ten million texts every month.			

9.4.2 The scenarios

We have reported the benefits of the interventions in two scenarios:

- Scenario 1: Cumulative benefits. The interventions are applied one after the other. The tables show the incremental results of each intervention, along with the cumulative impacts. In this scenario the two firewall interventions (Voice firewall and scam filter) target the *remaining harm* from the scam calls or texts not picked up by the preceding interventions. Therefore as the effectiveness of the preceding interventions decays, the benefits of these interventions grow.
- Scenario 2: Interventions in isolation. This scenario informs a raw cost-vs-benefit of each intervention as though they were each implemented alone in separate worlds.

In the following section we present the benefits of the interventions along with the net benefits after subtracting the costs of each intervention from its benefits.

9.5 The net present benefit of the interventions

The benefits of the interventions – the amounts by which they reduce harm – are then netted by their costs in each year. This produces a series of the future net benefits.

We discount the future net benefits to produce net present value benefit estimates using a social discount rate of 4 per cent.[167]

We set out our rationale for each and the implications this has when interpreting the figures. We report two figures in the estimate tables:

- Reduction in harm – this is the discounted difference between the counterfactual harm and the total harm in the counterfactual.
- Net present benefit – this is the discounted difference between the reduction in harm each intervention results in and its cost.

Scenario 1: Interventions implemented cumulatively

The results show that the incremental reduction in harm caused by the Voice firewall and Scam filter interventions is lower if the interventions implemented before them are still working well and scammers have not yet found new means of reaching Irish consumers (i.e. without CLI spoofing). Consequently, in this scenario the incremental Voice firewall net present benefit is just €142m after seven years – much lower than the two CLI blocks. Despite these highly conservative assumptions, the Voice firewall is still great value, with over €15 in benefits for every €1 cost. In contrast, the value of the Fixed CLI block is reduced marginally from €486m when implemented in isolation, to €469m.

The incremental benefits of the Scam filter are predictably lower if implemented following the Full SMS registry, assuming that it is working well and that scammers have not yet found new means of reaching Irish consumers (i.e. without SMS ID spoofing). This is despite the Full SMS registry only beginning to reduce harm in year 3 as a Partial registry would be functioning in year 2, thus reducing the incremental benefit of the Scam filter intervention in this year in particular. Despite these highly conservative assumptions, the SMS scam filter is still great value, with over €33 in benefits for every €1 cost.

[167] Department of Public Expenditure and Reform (2019). 'Public Spending Code: 'Central Technical References and Economic Appraisal Parameters'. p.11 – [online]

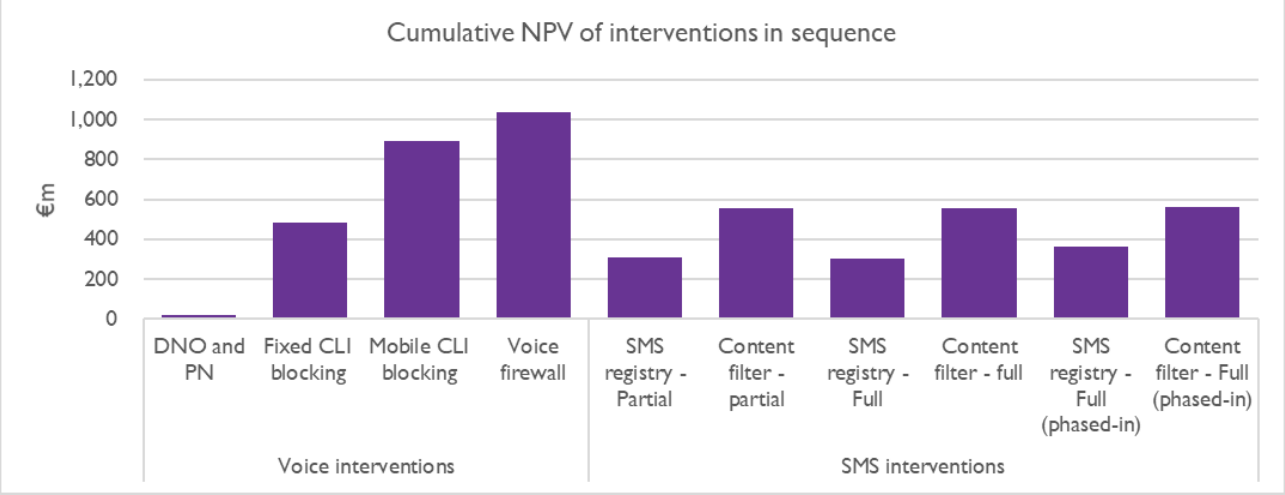
Table 9.9: Scenario 1: Estimated cumulative reduction in harm and net present benefit across the interventions (€m); cumulative NPV shown

Intervention	Present-value incremental reduction in harm (€m)	Incremental NPV (€m)	Cumulative NPV (€m)
VOICE INTERVENTIONS			
DNO and PN	21	20	20
Fixed CLI blocking	469	469	488
Mobile CLI blocking	414	408	896
Voice firewall	152	142	1,038
SMS INTERVENTIONS 1			
SMS registry - partial	317	311	311
SMS scam filter after Partial	251	245	555
SMS INTERVENTIONS 2			
SMS registry - full	312	306	306
SMS scam filter after Full	255	248	555
SMS INTERVENTIONS 3			
SMS registry - full (phased-in)	372	366	366
SMS scam filter after Full (phased-in)	204	197	564

Source: Europe Economics analysis. Note: The difference between the Cumulative NPV may not exactly equal the Incremental NPV due to rounding.

Figure 9.4 illustrates the net present benefits in scenario 1.

Figure 9.4 : Scenario 1: cumulative net present value benefit across the interventions (€m)



Source: Source: Europe Economics analysis.

Scenario 2: Interventions implemented in isolation

Table 6.7 presents the results of this scenario both in terms of benefits (reduction in harm) and net present benefits (benefits less costs over time). The Voice firewall would have the most significant impact of all the voice interventions, with a net present benefit of €881m over the period. This is driven predominantly by the fact that the Voice firewall is assumed to cause a non-decaying 90 per cent reduction in all scam calls.

Despite the Fixed CLI and Mobile CLI blocking interventions targeting equal shares of scam calls, the net present benefit of the Mobile CLI block is slightly less than that of the Fixed CLI block. This is driven by the fact that it is considerably costlier, and its effects on reducing harms are experienced a year after implementation commencement.

For the sender ID options, the phased-in variant of the full SMS registry scores the highest, with a net present benefit of €366m. This is because it begins to stem the harm from scam texts in year 2 in line with the effectiveness of the Partial registry, before realising the effects of the Full registry in year 3. In turn, the registry begins to decay in year 5, giving it the longest period of 'original' (or full strength) impacts.

The Scam filter intervention would be the most effective intervention for SMS scams, with a net present benefit of €514m over the seven years. We assume that the SMS scam filter is implemented without any delay due to the need for supporting legislation. This is necessary to simplify our analysis, given the uncertainty inherent in predicting the passing of legislation. However, we note that any such delay results in continued harm to Irish consumers and businesses, with a 1-year delay resulting in a €93m cost of uncaptured harm over the seven years.

The Voice Firewall has a much greater NPV than the SMS scam filter primarily because harm from voice scams across consumers and businesses is much greater than harm from SMS scams. It is also expected to be more effective (addressing 90% of calls as opposed to 85% of texts).

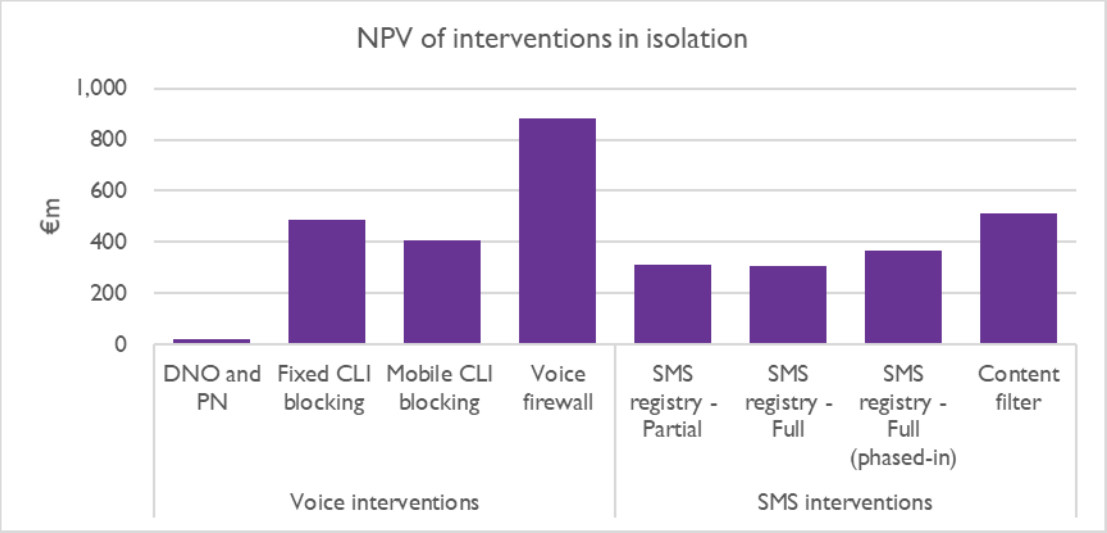
Table 9.10: Scenario 2: Estimated present-value reduction in harm and net present benefit per intervention in isolation (€m)

Intervention	Present-value reduction in harm (€m)	Net present benefit (€m)
DNO and PN	21	20
Fixed CLI blocking	487	486
Mobile CLI blocking	414	408
Voice firewall	892	881
SMS registry - partial	317	311
SMS registry - full	312	306
SMS registry - Full (phased-in)	372	366
SMS scam filter	520	514

Source: Europe Economics analysis.

Figure 9.5 illustrates the net present benefits in scenario 2.

Figure 9.5: Scenario 2: net present value benefit, per intervention (€m)



Source: Source: Europe Economics analysis.

Scenarios 1 and 2: Discussion

As noted in the "static" view of harm, Scenario 1 would vastly understate the benefits of the dynamic measures on their own (the Voice Firewall and SMS scam filter), as it assumes that scammers blocked by

static measures such as CLI Blocking will not find new routes to customers or develop scams that sidestep the static interventions altogether.[168] While we do not know the degree to which scammers will circumvent such interventions, we do know they will try and there is emerging evidence of such practices both in Ireland and abroad.

To account for this, Scenario 2 can be interpreted as the impact of the dynamic interventions on reducing dynamic harm, assuming that the same level of harm prevails in spite of the static interventions (e.g. if scammers were to fully circumvent these interventions such that their benefits were zero). This is equivalent to assessing the impact of the dynamic interventions in isolation (e.g., on overall harm). Therefore, these figures can be considered upper bounds for the potential benefits of the Voice Firewall and SMS spam filter. This approach enables us to capture the potential benefits of the dynamic interventions,[169] in light of scammers' adaptability.

We find that the voice firewall and SMS scam filters are important and provide benefits of €142m and €197m even where scammers do not adapt to the static interventions, because they offer additional protection (e.g., against scams originating in Ireland). However, they become increasingly more important the more scammers adapt to the static interventions, rising to €881m and €514m respectively when considered in isolation (i.e. akin to a scenario where scammers fully adapt). Again, the exact benefits of each intervention depends on the reaction of scammers to the static interventions, including at what point they adapt. We consider this approach appropriate for estimating the range of potential benefits because assuming a specific level of adaptation (and related timing) by scammers over such a long period would require information that is simply not available.

The table below presents our central scenario where scammers adapt to some extent to the static interventions (such that their effectiveness decays over time) and an extreme scenario where scammers adapt fully to the static interventions, such that their benefits are zero. Whilst this is an unlikely scenario, it nevertheless provides an absolute lower bound to the benefits of the intervention packages.

[168] While our models do build in a "decay rate" in interventions effectiveness, the real issue is whether scammers will be able to circumvent the static interventions altogether.

[169] The static harm assumes that the value and profile of harm from scams in 2022 (e.g., % from Fixed CLI spoofing, Mobile CLI spoofing) is forecast into the future, whereas dynamic harm assumes that the same level of prevails but completely circumvents the static measures.

Figure 9.6: Comparison of costs and benefits assuming different levels of scammers' adaption

Intervention	Cost (€m)	Net Benefit	
		Scammers adapt minimally to static interventions	Scammers adapt fully to static interventions
Voice interventions			
Static interventions (DNO,PN, Fixed & Mobile CLI Blocking)	€8m	€896m	-8m
Voice firewall	€10.2m	€142m	€881m
SMS Interventions			
Static: SMS registry – Full (phased-in)	€6.4m	€366m	-6.4m
SMS scam filter	€6.2m	€197m	€514m
Combined			
Total	**€31m**	**€1.6bn**	**€1.4bn**

Source: Europe Economics analysis. Values may not add due to rounding. Note that the reported costs in the table are present value figures over the 7-year implementation horizon.

The tables below present an annualised reduction in harm and net benefit for each intervention. This provides a broad point of comparison with the annual harm of around €300 million (although the figures in the tables are discounted over the seven-year intervention period).

Table 9.11: Annualised figures across 7 years for Scenario 1 (€m)

CUMULATIVE INTERVENTIONS	Annual reduction in harm (7 years discounted)	Annual net benefit (7 years discounted)*
DNO and PN	3	3
Fixed CLI blocking	70	70
Mobile CLI blocking	129	128
Voice firewall	151	148
SMS registry – full (phased-in)	53	52
SMS scam filter – full (phased-in)	82	81

*These figures are the annualised NPV of the 7-year totals presented in the last column of Table 9.9.

Note: the sum of the reduction in harm from the cumulative voice interventions (€151m) and SMS interventions (€82m) equates to the harm reduced per year. This can be broadly compared to the annual total harm figure for 2022 (€310m), bearing in mind it also includes discounting over time and an assumed growth-rate of harm.

Table 9.12: Annualised figures across 7 years for Scenario 2 (€m)

INTERVENTIONS IN ISOLATION	Annual reduction in harm (7 years discounted)	Annual net benefit (7 years discounted)
DNO and PN	3	3
Fixed CLI blocking	70	69
Mobile CLI blocking	59	58
Voice firewall	127	126
SMS registry - partial	45	44
SMS registry - full	45	44
SMS registry – full (phased-in)	53	52
SMS scam filter	74	73

9.6 Sensitivity analysis

We present our key findings with the following sensitivity analysis. Our overall finding is that the cost-benefit ratio of all the interventions remains positive in all scenarios.

9.6.1 High harm counterfactual

Assuming that the harm from scam communications grows at our higher assumed rate, the benefits of the interventions will be greater as they will prevent a greater amount of harm. The table below presents the results for the cumulative package of interventions for this high harm scenario. The total net present benefits across the voice and SMS interventions (assuming a phased-in full ID registry) are €1.61bn.

Table 9.13: Scenario 1: Estimated cumulative reduction in harm and net present benefit across the interventions (€m); HIGH HARM SCENARIO

Intervention	Present-value incremental reduction in harm (€m)	Incremental NPV (€m)	Cumulative NPV (€m)
VOICE INTERVENTIONS			
DNO and PN	21	20	20
Fixed CLI blocking	472	472	492
Mobile CLI blocking	417	411	902
Voice firewall	153	143	1,046
SMS INTERVENTIONS 1			
SMS registry - partial	319	313	313
SMS scam filter after Partial	253	246	559
SMS INTERVENTIONS 2			
SMS registry - full	314	309	309
SMS scam filter after Full	256	250	559
SMS INTERVENTIONS 3			
SMS registry - full (phased-in)	375	368	368
SMS scam filter after Full (phased-in)	205	199	568

Source: Europe Economics analysis. Note: The difference between the Cumulative NPV may not exactly equal the Incremental NPV due to rounding.

9.6.2 Low harm counterfactual

The table below shows the results for the cumulative net benefits of the package of interventions in the low harm counterfactual, in which harm reduces over time even in the absence of the interventions. The total net present benefits across the voice and SMS interventions (assuming a phased-in full ID registry) are €1.49bn.

Table 9.14: Scenario 1: Estimated cumulative reduction in harm and net present benefit across the interventions (€m); LOW HARM SCENARIO

Intervention	Present-value incremental reduction in harm (€m)	Incremental NPV (€m)	Cumulative NPV (€m)
VOICE INTERVENTIONS			
DNO and PN	20	19	19
Fixed CLI blocking	440	440	459
Mobile CLI blocking	385	379	837
Voice firewall	141	130	968
SMS INTERVENTIONS 1			
SMS registry - partial	294	289	289
SMS scam filter after Partial	233	226	515
SMS INTERVENTIONS 2			
SMS registry - full	287	282	282
SMS scam filter after Full	239	232	514
SMS INTERVENTIONS 3			
SMS registry - full (phased-in)	345	339	339
SMS scam filter after Full (phased-in)	189	183	523

Source: Europe Economics analysis. Note: The difference between the Cumulative NPV may not exactly equal the Incremental NPV due to rounding.

9.6.3 Small / large operator groupings

To account for some uncertainty in the number of operators to which the Voice firewall and SMS scam filter interventions might apply, we estimated the net benefits of the interventions with a smaller grouping – instead of four and five operators for the Voice and SMS dynamic interventions respectively, we modelled a scenario with only three MNOs in each. The results show that the net benefits increase marginally to a total of €1.605bn.

Table 9.15: Scenario 1: Estimated cumulative reduction in harm and net present benefit across the interventions (€m); SMALL GROUPINGS

Intervention	Present-value incremental reduction in harm (€m)	Incremental NPV (€m)	Cumulative NPV (€m)
VOICE INTERVENTIONS			
DNO and PN	21	20	20
Fixed CLI blocking	469	469	488
Mobile CLI blocking	414	408	896
Voice firewall	152	146	1,042
SMS INTERVENTIONS 1			
SMS registry - partial	317	311	311
SMS scam filter after Partial	251	246	557
SMS INTERVENTIONS 2			
SMS registry - full	312	306	306
SMS scam filter after Full	255	250	556
SMS INTERVENTIONS 3			
SMS registry - full (phased-in)	372	366	366
SMS scam filter after Full (phased-in)	204	199	565

Source: Europe Economics analysis. Note: The difference between the Cumulative NPV may not exactly equal the Incremental NPV due to rounding.