UK Finance:
Tech and telco warnings research

Strand report

Thinks
Insight & Strategy

Contents

01. Executive summary

Thinks
Insight & Strategy

Context and objectives

- Following a **comprehensive review of counter-fraud** campaigns and interventions for the National Crime Agency (NCA), in 2022, we conducted a gap analysis and strategic review for the Lending Standards Board (LSB) to better understand how to address authorised push payment (APP) scams through effective warnings.

- A number of gaps emerged from this review, including **exploring the opportunities and challenges for the tech and telco sectors in playing a role in actively combatting scams.**

- In order to address these gaps, we have conducted a **multi-strand research programme exploring effective warnings from a consumer perspective.**

- We then conducted research into different consumer 'personas' to create guidance to **tailor warnings for particular segments of consumers**.

- In this strand, we have built upon the consumer research from the financial sector, incorporating what **this means for the technology and telecommunications sectors** which play a major role in the fraud chain.

Consumer Research → Personas Research → **Tech & Telco Research**

4

Thinks

We took an iterative approach to understanding the role for tech and telco sectors in protecting consumers from fraud

① ② ③

We are here!

Methodology

Evidence review - of the role the tech and telco sectors can play in protecting consumers from fraud

Topline findings call

User journey mapping – to identify opportunities in current tech and telco user journeys

Revisiting the 'personas' effective warnings toolkit – to adapt the guidance to the tech and telco sectors

Final report and debrief

Review of >30 sources and evidence grid

>10 user journey maps

Updated guidance for warnings

Objectives

1 **To explore the current landscape of the tech and telco sectors response to fraud** (especially when occurring in the payment journey) to provide a rounded evidence base.

2 **To explore opportunities and challenges for the tech and telco sectors to work to prevent fraud** and in the design and implementation of effective warnings.

3 **To identify actionable next steps for the sectors** in protecting consumers from fraud and creating effective customer warning journeys.

5

Thinks
Insight & Strategy

Key findings for tech and telco sector warning development

The scale of fraud in the tech and telco sectors is significant	However, the sector is felt to have been slow to take action on the issue. While telco has a greater history of engagement, incentives to act are low and there is a lack of coordination within each sector.
Pressure for the sector to take responsibility for consumer safety from fraud is mounting	An increase in legislation, such as the Telco Fraud Sector Charter and Online Fraud Charter, have signaled movement towards taking greater responsibility and points to opportunities for action.
Understanding these opportunities will support greater action	This is a need to really understand when and how consumers can be better protected along tech and telco journeys. We have mapped out user journeys across the sectors to show where opportunities for effective warnings are and what challenges the sectors may face in implementing this.
The guidance for the financial sector should be adapted to apply to the T&T sectors	This guidance is backed by evidence, but needs to be adapted to take into account sector sensitivities and starting point. The guidance points to universal steps, including introducing positive friction through a clear CTA, provision of tailored advice and stating why a risk has been identified.
Some aspects of the guidance will be more challenging to implement, even if they apply	Sector sensitivities means that T&T will be especially reluctant to implement warnings that appear accusatory, identify individual consequences or implement pauses in the journey. Instead, focusing on getting the basics right will lead to a more productive start.

Thinks
Insight & Strategy

Adapted guidelines to support the tech & telco sectors to deliver effective fraud warnings

Status	Guideline	Summary
Retain guideline	**Provide a clear CTA**	There are opportunities for the sectors to advise consumers on practical steps to take to ensure the legitimacy of their journey (e.g. safer ways to pay, suspicious requests to look out for).
	Tailor the warning	Tailoring the warning shared with consumers will increase relevance and grab attention regardless of which sector or transaction is generating the warning.
	Explain why a risk is being identified	Providing contextual information when warnings are triggered helps consumers to understand the presence of positive friction in their journeys and grab attention.
Retain guideline with considerations	**Visually grab attention**	Breaking from the brand's usual look, feel and tone makes warnings stand out. This is enough to grab attention, without using alarmist visuals, that the sectors are likely to be wary of using at this stage.
	Be firm and clear	Clarity and use of simple English is recommended. Firmness of tone will indicate that the sectors are taking protecting consumers seriously and this should be positioned as positive reputationally. However, they are also likely to be sensitive to being firm in borderline cases.
	Humanise the experience	Sharing personal experiences of scams shows they can happen to anyone. However, space limitations will be a challenge for both sectors, with this guidance likely to be more appropriate for warnings included in broader communications and consumer education.
	Refresh warnings regularly	Refreshing warnings regularly prevents them from becoming 'wallpaper'. However, the focus for these sectors should be on getting the basics right first.
To consider in the future	**Create a pause**	A low-friction user experience is key to value propositions, particularly for the tech sector. As such, the sectors are likely to resist implementing a pause. Focusing on providing a clear CTA and encouraging consumers to think and pause of their own volition is likely to be more effective.
	Demonstrate individual consequence	As the tech and telco sectors are not typically involved in reimbursement, there is less incentive to emphasise individual consequence than in the finance sector. However, focusing on loss aversion (rather than personal loss) may be a route in.

Looking to the future

There are examples of best practice in effective warnings throughout the tech and telco sectors, as shown in the user journeys.

However, implementation of warnings is inconsistent and levels of engagement among the sector are mixed.

The evidence has shown that principles that work for the finance sector can be adapted and applied to the tech and telco sectors.

The guidelines provided in this deck give UK Finance an evidence base in which to ground future conversations with the tech and telco sectors. These conversations can help to understand the sectors' plans and any opportunities for future collaboration.

UK Finance will have a strong role to play in continuing conversations and collaboration between the finance and tech and telco sectors to ensure learnings are shared.

Thinks
Insight & Strategy

02. Tech and telco's position in the fraud landscape

Thinks
Insight & Strategy

The scale of fraud in the UK cannot be understated

Fraud is the most common type of crime experienced in the UK.

An estimated 3 million UK consumers lost a combined estimated £1.9bn to financial fraud in 2022[1].

Yet scams are widely underreported.

Fewer than a third report the crime to the authorities, and this figure is estimated to be lower still for some types of scams[2].

Almost 3/4 of adults in the UK have been targeted by scams.

And, over a third have lost money to them[3].

Fraud cases grew by 25% between March 2020 & 2022[4]

Some types of fraud have returned to pre-pandemic levels, but others remain high and are predicted to grow further still…

We are seeing increasing levels of investment aimed at tackling this fraud, notably by the banking and financial services sector. **But where do the tech and telco sectors fit into this effort?**

[1] Home Office Fraud Strategy, 2023
[2] National Trading Standards, 2023
[3] Office for National Statistics, 2022
[4] House of Lords Digital Fraud Committee, 2022

Thinks

A large and growing proportion of fraud cases involve the tech and telco sectors

Tech

The continued growth in the sector has brought new and more global opportunities for fraudsters.

By 2022, around three quarters of online fraud cases had their beginnings on social media platforms[1]. Cases almost doubled on Facebook Marketplace in just one year.

This pattern is forecast to continue with new technologies emerging[2].

87% of users have encountered content online which they believe to be a scam or fraud[3].

Telco

The fraud threat involving telco is ever-evolving.

Voice phishing, or *vishing*, is not new, but VoIP-enabled number spoofing* is on the rise - and adds an extra layer of complexity faced by consumers[4].

Cases of SMS-based 'smishing' attacks have risen steadily in recent years[5].

18% of fraud cases start via telco, and these account for 44% of all losses[1].

[1] UK Finance, 2022
[2] Consumers International, 2019, Smailli, 2022
[3] Yonder Consulting, 2023
[4] Ofcom, 2022
[5] Which? Press Office, 2021

*Number spoofing is the process of changing the Caller ID to any number other than the actual calling number. Voice over Internet Protocol is a technology that allows voice calls to be made using a broadband Internet connection instead of a standard phone line. Criminals can customise the caller ID display name when setting up an account, allowing them them to easily impersonate someone else.

Thinks
Insight & Strategy

Sectors have historically been slow to assume responsibility, to varying degrees

Level of responsibility assumed

Telco

Tech

Tech platforms have been positioned as passive actors, not responsible for user activity[1] - and have been regulated as such.

Anti-fraud resourcing has not been a priority; platforms feel their responsibility is to shareholders[1]. This has left users largely responsible for scam detection.

Efforts to encourage 'polluter pays'-based contributions* to victim reimbursement have been resisted[2].

The telco sector has a greater history of engagement on fraud.

Vodafone and others were working on early fraud detection back in the 1990s, during a time when the UK uptake of mobile phones was accelerating[3].

However, there has since been a general lack of incentive and obligation to take the lead in an increasingly complex fraud landscape. Measures have often been reported as uncoordinated or piecemeal[4].

[1] Napoli and Caplan, 2017
[2] Barrett, C., 2023
[3] P Burge, 1997
[4] Ofcom, 2022
[5] House of Lords Digital Fraud Committee, 2022

A polluter pays based contribution system would see companies paying into a communal fund to support the financial sector to reimburse scam victims.

Thinks
Insight & Strategy

As expectation on sectors grows, steps have been taken in a positive direction

Tech	Recent examples*

- **TikTok** banning content with links to external, potentially fraudulent, websites[1].

- **Meta** implementing 'warning screens' over content that might be misleading[2].

- **eBay** has brought advanced marketplace compliance technology in-house, purchasing AI fraud detection company 3PM Shield[3].

Telco	Recent examples*

- **EE** implementing a 'Spam Shield' SMS blocking system, which has reportedly reduced the number of reported spam and scam messages on the network by over 90%[1].

- Members of the **Communications Crime Strategy Group**** contributing to the formation of the sector charter on fraud in 2022. This tackles key issues, such as scam calls, subscription fraud and SIM swap fraud[4].

Both	

- Members of **techUK** working with the Home Office's Joint Fraud Taskforce[5] and backing the 2023 'Take Five - to Stop Fraud' national campaign.

- Provision of educational resources and signposting to victim support services.

[1] House of Lords Digital Fraud Committee, 2022
[2] Meta, 2023
[3] eBay, 2023
[4] Ofcom, 2022
[5] techUK, 2023

See the 'User journeys' section of this report for further detail of measures in place.
***Members include BT, EE, Sky Mobile, Tesco Mobile, Three, Virgin Media, O2 and Vodafone*

13

Thinks
Insight & Strategy

Both sectors have faced deterrents and challenges in stepping up their efforts

Reputational

- **A fear of blocking legitimate businesses** and risking false positives.

- There is a hesitancy to be seen as heavy-handed with users.

- A 'network effect'* can prevent platforms being held to account[1].

Structural

- A lack of standardised data sharing between platforms and sectors.

- **A lack of information obtained at sign-up** to help identify criminals - often just an email address is required.

- Authorised fraud is more complex to detect[2].

Financial

- A fear of deterring transactions resulting in a loss of revenue.

- The expense of top-down implementation of anti-fraud technologies.

- **Bottom-up human moderation is expensive** so outsourcing this to users makes economic sense.

Legal

- A lack of regulatory leadership to facilitate collaboration and assuage user data privacy concerns[3].

- **The fraudulent act often happens off the platform or service**[4].

- The international nature of fraud makes this challenging to regulate.

[1] Hermann, 2021; Riefa, 2019
[2] Sneade, P., 2022
[3] Ofcom ACE, 2023
[4] House of Lords Digital Fraud Committee, 2022

14

*A 'network effect' is the idea that when more people use a product or service, its value increases. Among social media organisations in particular, users want to use the platforms their peers use. As a result, these organisations are not subject to the usual market forces that apply regarding levels of customer service.

Thinks
Insight & Strategy

Recent regulatory change signals an opportunity for cross-sector collaboration

Growing consumer and financial sector demand for action[1]

Intensifying media spotlight on fraud

Increase in scams and disruptions to services

Increased top-down legislative leadership

Telco Fraud Sector Charter *(2021)[2]*	**Sets out agreed courses of actions on key issues** such as scam calls, smishing, subscription fraud and SIM swap fraud. Encourages greater data sharing with industry, law enforcement and finance sector.
Online Safety Act *(2023)[2]*	**Places a duty of care on tech sector to ensure users are safe online.** Increases Ofcom power to take enforcement action, such as in issuing fines to services that fail to comply with agreed-upon duties.
Online Fraud Charter *(2023)[2]*	**Voluntary agreement between the Government and the tech sector to reduce fraud on their platforms and services.** Agrees several key measures incl. developing appropriate warnings in response to unknown users.

Heightened engagement by sectors

Thinks
Insight & Strategy

03. Guidelines for developing warnings

Thinks
Insight & Strategy

From consumer research, we have identified nine guidelines for effective warnings that apply to the finance industry

VISUALLY GRAB ATTENTION
When designing an online warning, make this visually attention-grabbing, using colours and symbols consumers are used to associating with a warning.

BE FIRM AND CLEAR
Use Plain English and short sentences e.g. "Payment flagged as high risk - it is likely this is a scam. You could lose your money".

CREATE A PAUSE
Asking very specific questions can introduce positive friction. Forcing a pause may also be appropriate in some cases, for example, putting a payment on hold.

DEMONSTRATE INDIVIDUAL CONSEQUENCE
Tell consumers they may lose their money if they ignore the warning.

TAILOR THE WARNINGS
Tailor to the scam or purchase type and anything known about the consumer to engage consumers and make them listen.

HUMANISE THE EXPERIENCE
Share comparable examples. Empathy is critical in warnings, so that warnings resonate and allow consumers to admit if there is an issue.

REFRESH WARNINGS REGULARLY
Warnings need to be refreshed regularly to avoid becoming 'wallpaper' - use these guidelines to support the iteration of warnings.

EXPLAIN WHY A RISK HAS BEEN IDENTIFIED
For consumers with less trust, digital or financial confidence, as well as those with lower comprehension, explaining why a scam is thought to be occurring can provide an important pause.

PROVIDE AN ACTIONABLE CTA
Consumers move through routine payment journeys quickly. Providing a specific action they can take to confirm the legitimacy of the payment can help.

Thinks
Insight & Strategy

This guidance can be adapted for the tech & telco sectors, reflecting the different opportunities and challenges

The finance sector is further along in their journey of developing warnings than the tech and telco sectors.

Direct comparisons between the sectors are unlikely to improve stakeholder relations. Rather, recommendations must be made sensitively to maximise buy-in.

The opportunities and challenges for these sectors are different.

These need to be reflected in any guidance developed on designing and implementing warnings for the tech and telco sectors.

As a result, we have re-visited the guidance on developing warnings in the finance sector and **adapted it to be appropriate for the tech and telco sectors**, **recognising the unique challenges and opportunities** that emerged from our desk research.

Thinks
Insight & Strategy

To reflect this context, we have adapted the guidelines for the tech & telco sectors

Status	Guideline	Summary
Retain guideline	**Provide a clear CTA**	There are opportunities for the sectors to advise consumers on practical steps to take to ensure the legitimacy of their journey (e.g. safer ways to pay, suspicious requests to look out for).
	Tailor the warning	Tailoring the warning shared with consumers will increase relevance and grab attention regardless of which sector or transaction is generating the warning.
	Explain why a risk is being identified	Providing contextual information when warnings are triggered helps consumers to understand the presence of positive friction in their journeys and grab attention.
Retain guideline with considerations	**Visually grab attention**	Breaking from the brand's usual look, feel and tone makes warnings stand out. This is enough to grab attention, without using alarmist visuals, that the sectors are likely to be wary of using at this stage.
	Be firm and clear	Clarity and use of simple English is recommended. Firmness of tone will indicate that the sectors are taking protecting consumers seriously and this should be positioned as positive reputationally. However, they are also likely to be sensitive to being firm in borderline cases.
	Humanise the experience	Sharing personal experiences of scams shows they can happen to anyone. However, space limitations will be a challenge for both sectors, with this guidance likely to be more appropriate for warnings included in broader communications and consumer education.
	Refresh warnings regularly	Refreshing warnings regularly prevents them from becoming 'wallpaper'. However, the focus for these sectors should be on getting the basics right first.
To consider in the future	**Create a pause**	A low-friction user experience is key to value propositions, particularly for the tech sector. As such, the sectors are likely to resist implementing a pause. Focusing on providing a clear CTA and encouraging consumers to think and pause of their own volition is likely to be more effective.
	Demonstrate individual consequence	As the tech and telco sectors are not typically involved in reimbursement, there is less incentive to emphasise individual consequence than in the finance sector. However, focusing on loss aversion (rather than personal loss) may be a route in.

The following guidance provides a good starting point for the tech and telco sectors

Retain guideline	Provide a clear CTA	Tailor the warning	Explain why a risk is being identified
Why is this guidance important?	Informing consumers of actionable steps to ensure legitimacy of their journey supports the **building of protective habits**.	Targeting particular fraud types that are relevant to the user journey **helps warnings to stand out and feel memorable**.	As consumers may not be used to seeing warnings across these journeys, **explaining why a risk is identified is important for engagement**.
What are the challenges to implement this?	Organisations may initially **resist anything that is felt to disrupt the user journey**.	**Organisations may be cautious of making consumers nervous** by highlighting potential fraud in their journey.	Organisations will likely feel cautious of identifying a potential risk, in the **event that it is a legitimate service user.**
What is our recommendation?	**Retain guideline.** This introduces positive friction and relies on the user to 'pause' their journey rather than disrupting it from a service end.	**Retain guideline.** Where warnings are present, they should be tailored to the user journey to increase consumer relevance.	**Retain guideline.** This complements the provision of a clear CTA in introducing positive friction and providing a rationale to consumers as to why the warning is present.

Thinks
Insight & Strategy

Factoring in sector sensitivities on brand and tone supports the following adapted guidance

Retain with considerations	Visually grab attention	Be firm and clear
Why is this guidance important?	**Breaking away from brand look and feel makes warnings stand out**, avoiding becoming 'wallpaper'.	**Clarity and simple English remains essential** for effective anti-fraud warnings, regardless of the sector.
What are the challenges to implement this?	Organisations may **resist using visual cues for 'danger'** or that we may typically associate with a warning.	The sectors are **cautious about overly firm warnings** and appearing accusatory in borderline cases.
What is our recommendation?	**Retain with considerations.** Breaking from brand look and feel, rather than using visual 'danger' cues, is a good starting point.	**Retain with considerations.** Clarity is important and firmness in tone will indicate that consumer protection is being taken seriously. However, this should be balanced with sensitivity to avoid sounding accusatory.

Thinks
Insight & Strategy

Getting the basics right will be important before pursuing the following guidance

Retain with considerations	Humanise the experience	Refresh warnings regularly
Why is this guidance important?	Sharing relatable personal accounts **helps warnings sink in and dispels 'victim' stereotypes**.	Over time, consumers will get used to the language, tone, look and feel of warnings. **Regular updates can stop warnings from becoming 'wallpaper'.**
What are the challenges to implement this?	Limited space and **worries around 'scare stories' frightening users** may prohibit their use along journeys.	Before regularly refreshing warnings, **getting the basics down first is the priority.**
What is our recommendation?	**Retain with considerations.** This guideline is more suitable for sector communications and warnings outside of user journeys (e.g. help pages and emails).	**Retain with considerations.** Identifying opportunities for warnings along user journeys and implementing these is an important first step. Refreshes of warnings can be considered once this is in place.

Thinks
Insight & Strategy

This guidance is unlikely to be applicable at present, but may be relevant in the future

To consider in the future	Create a pause	Demonstrate individual consequence
Why is this guidance important?	Forcing a pause **gives consumers a moment to 'cool off' and reflect on any warnings** or new information.	Warnings that indicate you may lose your money if you ignore the advice are **attention grabbing and make consumers stop and think.**
What are the challenges to implement this?	**Minimising friction** is an important part of user proposition across the T&T sectors. The telco sector are also likely to face **technical challenges** in implementing a pause in how consumers communicate using their services.	The T&T sectors are **not typically involved in reimbursement of consumers**. The sectors will be **wary of language that appears to blame users** for actions taken using their services.
What is our recommendation?	**To consider in the future.** While this is unlikely to be appropriate guidance at present, there may be a role for this in the future (for example, implementing a pause when following a dodgy link).	**To consider in the future.** This guidance can be revisited should legislation on reimbursement change in the future. In the meantime, focusing on loss aversion (rather than personal loss) may be a route in.

Thinks
Insight & Strategy

04. User journeys

We have created a range of user journeys exploring warnings in tech and telco

We created user journey maps through:

Simulating a range of user journeys and actions on platforms (seeking out riskier content types)

Supplementary desk research on where warnings have and haven't been reported

These journey maps cover four categories:

E-commerce
Top risks: Purchase scams, payment in advance scams

Social media
Top risks: Varied (inc. investment fraud, romance scams, phishing)

Dating apps
Top risks: Romance scams

Telco
Top risks: Impersonation fraud, payment in advance fraud

While evidenced by numerous simulated journeys (including seeking out suspicious actors and content), the user journey mapping process cannot replicate every situation, and as services do not publish their processes for triggering warnings and guidance, certain contextual triggers may not be shown.

Thinks
Insight & Strategy

The user journeys shed light on existing best practice and gaps and how this can be built on

Understanding users' experiences of using the tech & telco sectors' services shows us:

1. Where, if at all, warnings are present in current user journeys.

2. Where opportunities are to implement warnings across user journeys.

We have mapped out a wide range of user journeys across both the tech and telco sectors. Across this, there are examples of sector best practice. However, these are often applied inconsistently.

Where relevant, we have also highlighted **where existing warnings can be improved or new warnings would be valuable** based on the literature and the consumer research.

Thinks
Insight & Strategy

In order to disrupt purchase scams, warnings present in e-commerce should visually draw attention to actionable steps to safer usage

Challenge	Key guideline		Considerations
In e-commerce, **fast, convenient user journeys are a core to the value proposition** – contributing to a positive user experience and boosting sales.	**VISUALLY GRAB ATTENTION**	Quick, uninterrupted user journeys are non-negotiable – this makes **attention-grabbing visuals even more important to help draw attention** when friction can't be introduced.	**Breaking from brand look and feel** will help draw attention, without necessarily using visuals and colours that cue 'danger'.
Platforms will be **resistant to warnings that will scare customers**, which may drive them away or lead transactions to be abandoned.	**PROVIDE A CLEAR CTA**	Providing clear CTAs, such as safe ways to pay or how to check legitimacy of a seller, allows platforms to **reinforce desired behaviours without scaring customers**.	A clear CTA will introduce positive friction, **causing a consumer to stop and think**, without disrupting their journey.

Thinks
Insight & Strategy

Gumtree displays warnings with CTAs on how to 'stay safe' from purchase scams
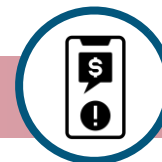
Stage of Journey	Searching for products	Deciding on the product	Reporting a scam	Optional educational resources

Image				
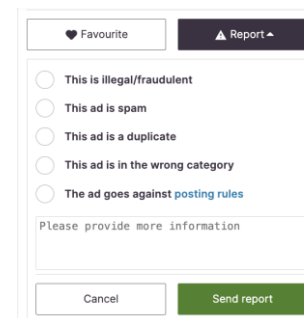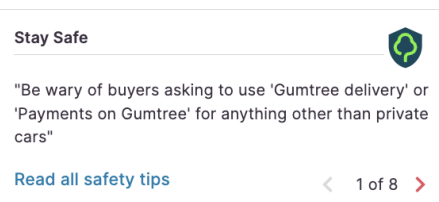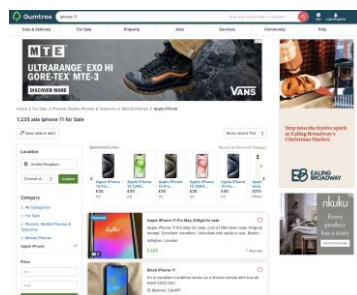
Warning	There are no warnings or guidance at this stage.	On the page for the specific item there is a 'stay safe' box, with 8 tips around common scams.	There is an option to report an ad you believe to be a scam.	There is information around spotting scams in the 'Safety' section of the website.

Gumtree

Thinks
Insight & Strategy

This is an example of good practice – but, these could be made more visually striking

Stage of Journey

Searching for products

Deciding on the product

Reporting a scam

Optional educational resources

Image

Stay Safe

"Be wary of buyers asking to use 'Gumtree delivery' or 'Payments on Gumtree' for anything other than private cars"

Read all safety tips   1 of 8

♥ Favourite   ⚠ Report

This is illegal/fraudulent
This ad is spam
This ad is a duplicate
This ad is in the wrong category
The ad goes against posting rules

Please provide more information

Cancel   Send report
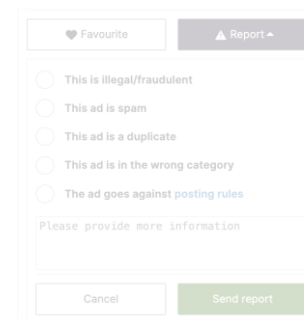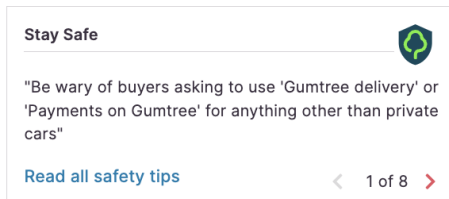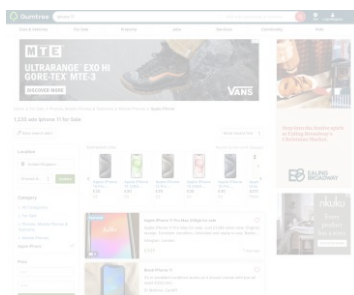
GUIDANCE:

VISUALLY GRAB ATTENTION

This is an example of good practice: Gumtree's warning boxes already provide clear CTAs on how to use the platform safely. In some areas, warnings are even tailored to product (e.g. pets, cars).

However, these can be improved as they visually **blend in with the platform, and could be made more visually distinct to grab attention.**

Gumtree

Thinks
Insight & Strategy

eBay's user journey is light on warnings, relying on users to interpret sellers' reputational data

Stage of Journey

Searching for products	Deciding on product	Messaging seller	Checkout	Optional educational resources

Image
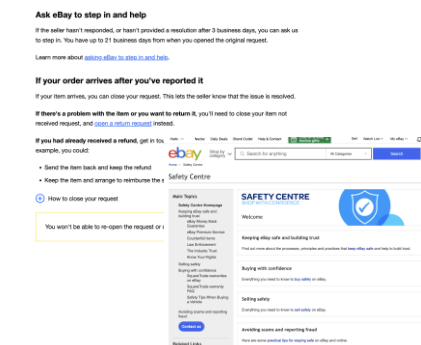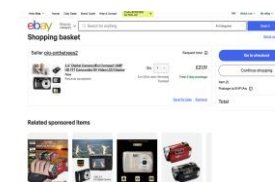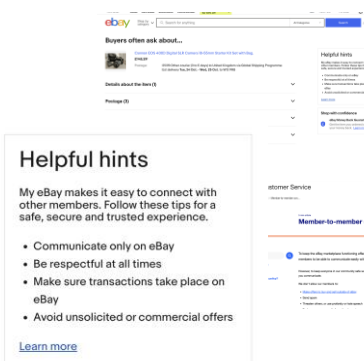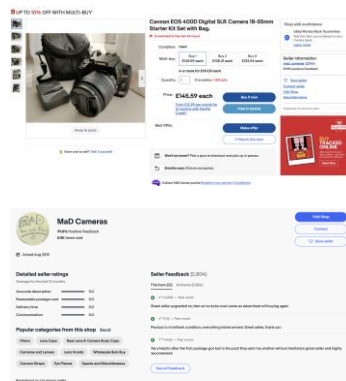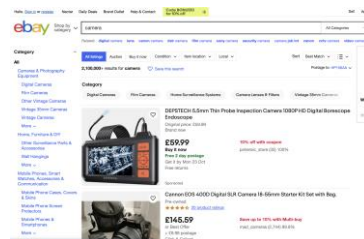
Warning

| No warnings are shown at this point of the journey. | There are **no warnings on individual products**, but reputational data on the the seller is shown. | 'Helpful hints' are shown with relevant advice. But, the **tone and visuals are too reassuring** and not explicit about scams. | **No warnings are shown** at the point of checkout. | If one has suspicions after checkout, there is high **quality information** – but for some, this will be **too late**.* |

Most consumers are only likely to read the educational resources after experiencing fraud. In some cases, flagging a fraudulent transaction may lead to refunds.

ebay

Thinks
Insight & Strategy

At the point of checkout, a warning could break from brand visuals and provide a clear CTA

Stage of Journey

| Searching for products | Deciding on product | Messaging seller | Checkout | Optional educational resources |

Image
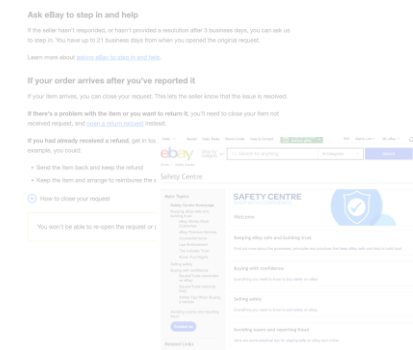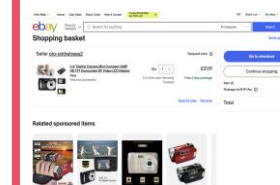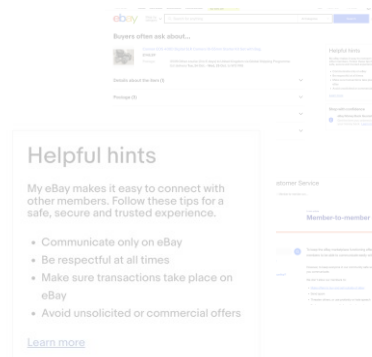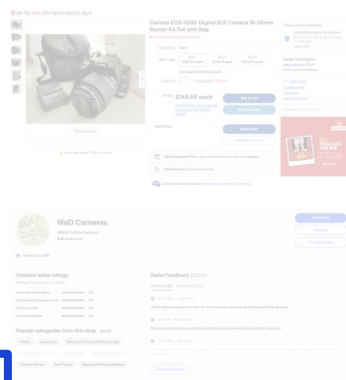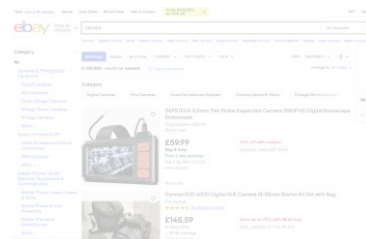
GUIDANCE:

VISUALLY GRAB ATTENTION

PROVIDE A CLEAR CTA

Ahead of making the transaction, eBay could provide a clear CTA, such as suspicious activities and safer ways to pay.

This guidance should visually stand out from brand look and feel to grab attention, but it doesn't need to look alarming!

ebay

Thinks
Insight & Strategy

Facebook Marketplace has few in-journey warnings, relying on users to seek out optional guidance

Stage of Journey	Searching for products	Deciding on product	Messaging seller	Optional educational resources

Image

Current warnings	There are no warnings or guidance at this stage.	There is no warnings or guidance at this stage.	There is no warnings or guidance at this stage, including for accounts with characteristics that might be seen as suspicious*.	Guidance on scams and fraud protection available elsewhere on website. This has to be proactively accessed by users.

*These characteristics include accounts registered within the past year, accounts with no profile picture or personal information (i.e. a name, photos, interactions with other users etc.).

Facebook Marketplace

Thinks
Insight & Strategy

At the point of messaging a seller, a visually distinct warning with practical advice would be effective

Stage of Journey

Searching for products

Deciding on product

Messaging seller

Optional educational resources

Image

At the point of messaging a seller, the platform could **provide guidance on how to check legitimacy of the seller and advice for a safe transaction**. For example, advice on meeting to exchange a product and safe ways to pay.

This should **visually stand out to grab users' attention** when they are communicating with a seller.

GUIDANCE:

PROVIDE A CLEAR CTA

VISUALLY GRAB ATTENTION

Facebook Marketplace

Thinks
Insight & Strategy

Social media warnings should be tailored to help users identify the wide range of potential fraud types they may be faced with

Challenge	Key guideline		Considerations
With a huge variety of content and potential fraud types, **generalised warnings can be lost in the noise of social media.**	**TAILOR THE WARNING**	When warnings are triggered in response to suspicious content, the **warning should be relevant to the suspected fraud type** (e.g. investment) where possible.	**Fraudsters are notoriously fast to adapt**, so keeping up with their changing approaches remains important.
Social media platforms **may be concerned that warnings will make their platforms feel unsafe.**	**PROVIDE A CLEAR CTA**	Frequent reinforcement of clear steps to avoid harm **can help teach users what to look out for**.	With users' concerns about safety growing, being on the front foot may be a reputational advantage. However, **cutting through noise remains difficult.**

Thinks
Insight & Strategy

When following links in content/adverts, Instagram users are taken directly to content

Stage of Journey	Coming across advert	Clicking on advert	Reporting a scam	Optional educational resources

Image
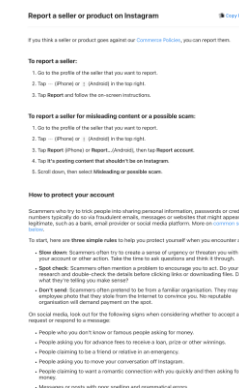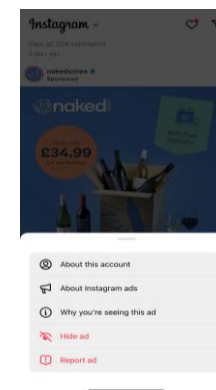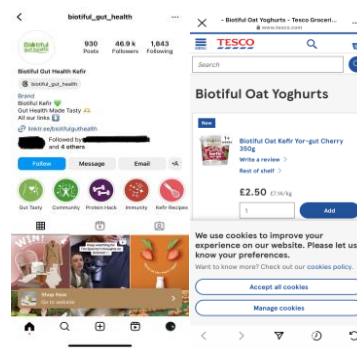
Warning	Instagram flags that this is an advert by showing a 'sponsored' label under the username.	When you click on the advert there are no warning pages – you are taken directly to the linked website.	You can report any advert that you feel is suspicious.	Elsewhere on the website, useful guidance on avoiding scams and reporting potential fraudsters.

35

Instagram

Thinks
Insight & Strategy

When following an external link, Instagram users should be warned with key watch-outs

Stage of Journey

Coming across advert	Clicking on advert	Reporting a scam	Optional educational resources

Image
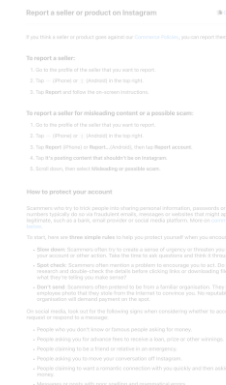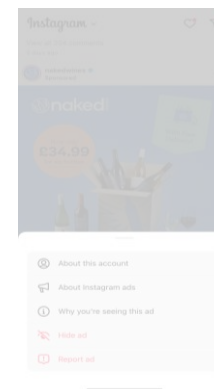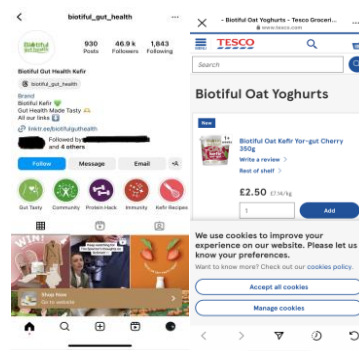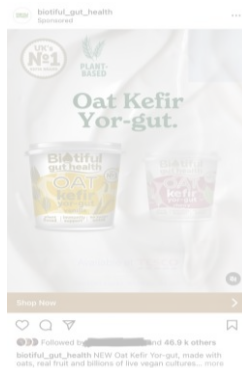
When following external links which have not been verified as legitimate, **consumers should be advised about what to look out for before leaving the platform**.

GUIDANCE:

PROVIDE A CLEAR CTA

Instagram

Thinks
Insight & Strategy

Even in risky areas (such as investments), Instagram does not display a warning

Stage of Journey	Coming across a likely investment scam	Engaging with investment scam	Reporting an investment scam	Optional educational resources
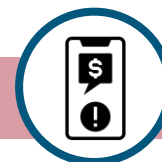
Image
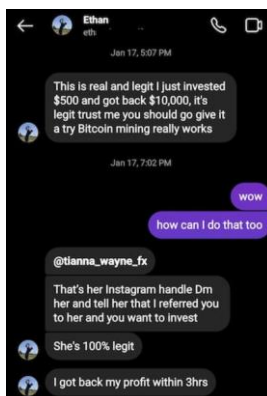
Warning

Receiving a message or coming across a post promoting a likely investment scam. There is nothing here to flag this.	When clicking on a link, you are brought directly to a website, without any warnings before you leave the platform.	Users can report posts or accounts that they feel are promoting investment scams.	Instagram's website have an "Avoid Scams on Instagram" section for users to educate themselves on warning signs.
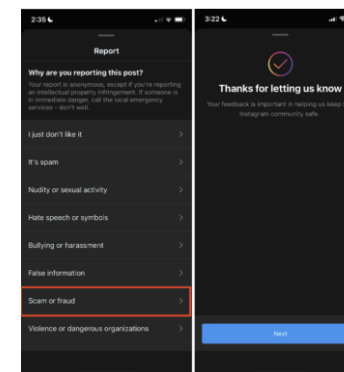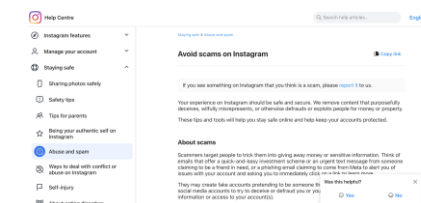
In high-risk areas like these, tailored warnings making risks clear should be added

Stage of Journey

Coming across a likely investment scam

Engaging with investment scam

Reporting an investment scam

Optional educational resources

Image
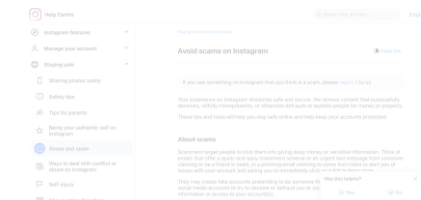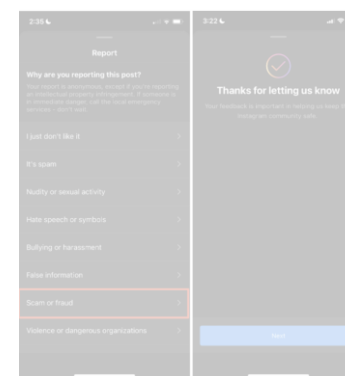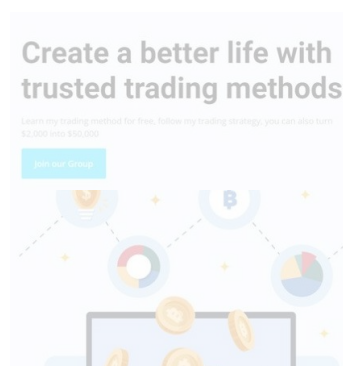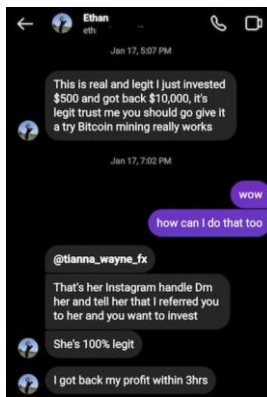
Content referring to risky areas such as investments should trigger tailored advice on the specific risk.

Users in 'hot states' may be likely to ignore warnings, so making it clear exactly *why* caution is required will be important too.

GUIDANCE:

TAILOR THE WARNING

EXPLAIN WHY A RISK IS BEING IDENTIFIED

Instagram

Thinks
Insight & Strategy

Warnings in dating services should be clear and sensitive when identifying risks, and help users identify suspicious contact and requests

Challenge	Key guideline		Considerations
Romance scams are complex and emotional. **This means that superficial 'warnings' may be ineffective.**	**PROVIDE A CLEAR CTA**	Platforms should work to **make looking out for the early warning signs as habitual as possible** before people are 'in too deep'.	Services are **likely to be cautious to warn beside individual users**. Instead watch-outs could be inserted between users in apps with 'swiping' systems.
Dating is a sensitive and personal topic, **so overbearing warnings about individual users may be deemed undesirable**.	**EXPLAIN WHY A RISK IS BEING IDENTIFIED**	While 'verification' does not guarantee that one isn't a romance fraudster, **flagging that unverified users may be higher risk may still be desirable.**	This is likely to **impact users who decide not to self-verify, which may concern platforms**. However, encouraging more verification is a positive step.

Thinks
Insight & Strategy

While Hinge has a verification system, it does not warn users about unverified profiles

Stage of Journey

Viewing a profile

Messaging another user

Reporting a fraudulent profile

Optional educational resources

Image
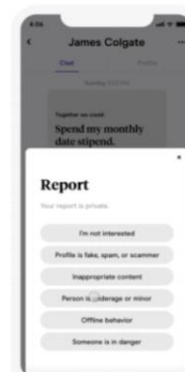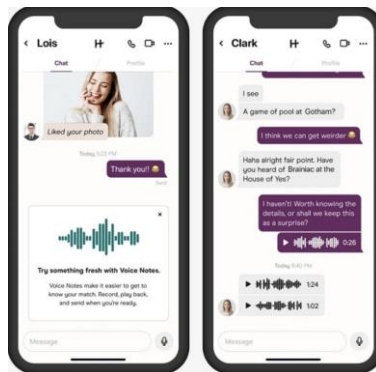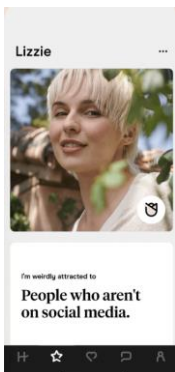
Warning

No warnings are displayed when viewing profiles. Users can 'verify' their identity, but unverified users show no additional warnings.

There are no warnings when interacting with users, even if the profiles are unverified.

Users can report fraudulent profiles in the app.

The Hinge website contains "Safe Dating Advice".

Hinge

Thinks
Insight & Strategy

Occasional warnings between users can allow dating apps to share key romance fraud watch-outs

Stage of Journey

Viewing a profile

Messaging another user

Reporting a fraudulent profile

Optional educational resources

Image

Lizzie

I'm weirdly attracted to
People who aren't on social media.

Safe Dating Advice
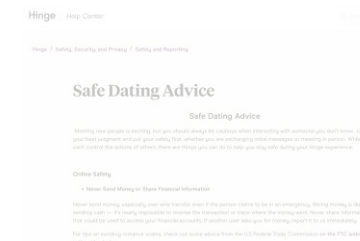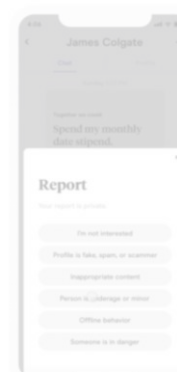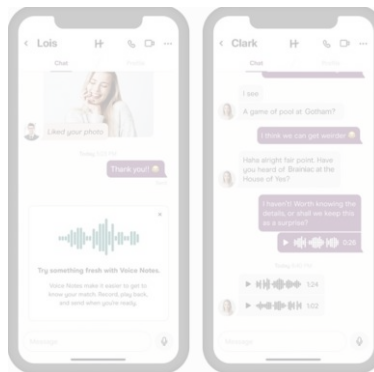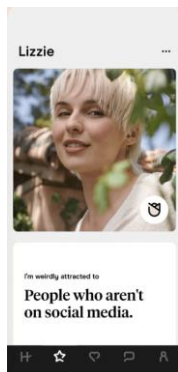
Occasional warnings can be applied 'between' users providing key watch-outs. Additional warnings for non-verified users would also be benficial.

These warnings can use sensitive language and give advice to users on how to stay safe. While verification is not a guarantee against romance fraud, encouraging its uptake is still beneficial.

GUIDANCE:

EXPLAIN WHY A RISK IS BEING IDENTIFIED

PROVIDE A CLEAR CTA

Hinge

Thinks
Insight & Strategy

Telco's existing flagging systems could be bolstered with better contextual information and attention-grabbing visuals

Challenge	Key guideline		Considerations
Current warnings identify some fraudulent approaches, but not **why** they are suspicious.	**EXPLAIN WHY A RISK IS BEING IDENTIFIED**	Fraud detection systems are partially effective, but many fall through the net. **By explaining contextual flags that do occur, users can learn what to look out for themselves.**	Telco do not have direct control of all aspects of how warnings are displayed. To some extent, this **depends on collaboration with handset providers**.
Current warnings are generally effective – but in some cases are easy to miss as they blend in with the UI.	**VISUALLY GRAB ATTENTION**	**Breaking with look and feel of operator and handset provider branding** will help to make warnings more noticeable.	Telco does not have direct control over many aspects of how warnings are displayed – so this will **require collaboration**.

Thinks
Insight & Strategy

Telco firms' caller ID flagging systems identify suspected fraudulent callers – but not all are caught

Stage of Journey	Pre-screening	Displaying caller ID	Blocking or reporting	Optional educational resources

Image	*Vodafone UK proactively blocks phone numbers used by known scammers to send high volumes of calls and texts to its customers. The company currently blocks around 675,000 calls every day, all while ensuring that legitimate numbers are not blocked.*			

| **Current warnings** | Networks pre-screen incoming calls, although many still do get through – with different networks' detection systems varying in accuracy. | When this system is triggered, the risk is clearly flagged to the user through caller ID. However, many fraudulent or spoofed calls do get through this system. | For fraudulent numbers which are not flagged, a clear reporting system exists in which users can block the number in question. | Networks provide information online about how to identify and respond to suspicious calls, often with clear CTAs. This must be accessed proactively. |

Phone

Thinks
Insight & Strategy

Building on this, telco could look into building more information on suspicious features and how to react

Stage of Journey

Pre-screening	Displaying caller ID	Blocking or reporting	Optional educational resources

Image

Vodafone UK proactively blocks phone numbers used by known scammers to send high volumes of calls and texts to its customers. The company currently blocks around 675,000 calls every day, all while ensuring that legitimate numbers are not blocked.

Scam Likely

Incoming call

Scam Likely
234-555-6789

Remind Me   Message

Decline   Accept

REJECT CALL WITH MESSAGE

020 3582 8990
London • 12:02

Add contact   Report spam

Report and block
+442035828990?

You will no longer receive calls or texts from this number.

Cancel   Report spam
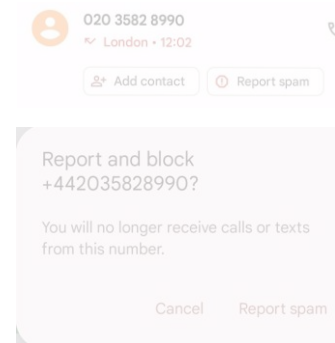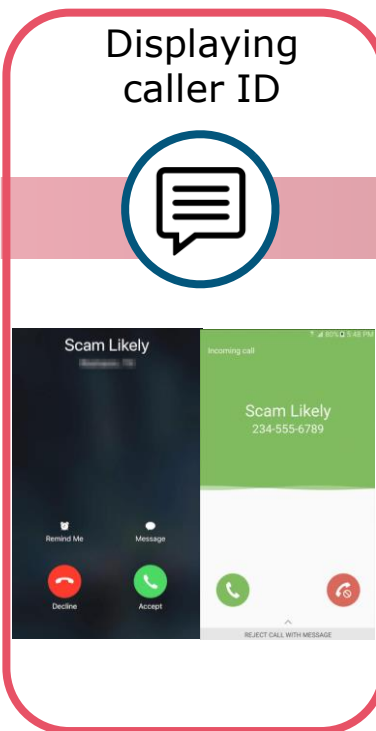
1) **Don't respond to any unexpected call, email or text, without checking first.** If it's out of the blue, check it's for you

- If it's a call, hang up, find a number you can trust, and call back on that
- If it's your bank, you can call back using the number on the back of your card
- Or, if concerned, dial 159 to be connected securely to most UK banks

Building on these powerful interventions, telco may be able to **work with operating system providers to provide contextual information about why an approach is suspicious in borderline cases.**

Explaining what users should do next (i.e. block and report the number) will help build protective behaviours and return important information to the telco sector.

GUIDANCE:

EXPLAIN WHY A RISK IS BEING IDENTIFIED

PROVIDE A CLEAR CTA

Phone

Thinks
Insight & Strategy

SMS messages from unknown numbers are flagged in iOS – but blend in with the visuals

Stage of Journey	Pre-screening	Incoming text	Blocking or reporting	Optional educational resources

Image				

Current warnings	Some networks screen incoming messages and flag or block suspicious activity*. Pre-screening systems vary by network.	On iOS, unknown numbers are flagged. iOS systems refer to the text as possible 'junk' in a format and colours consistent with branding.	When clicking this flag, users are prompted to delete the message and report it as 'junk'.	Networks provide information online about how to identify and respond to suspicious messages. Information must be accessed proactively.

45

*While networks' systems vary, key determinants appear to be reports by other users, content similar to other common fraudulent approaches, and high frequencies of outgoing texts/calls.

 SMS

Thinks
Insight & Strategy

Telco should look into working with OS providers to make warnings more noticeable and informative

Stage of Journey

Pre-screening

Incoming text

Blocking or reporting

Optional educational resources

Image

SPAM

EE - We were unable to process your bill.
In order to access then please confirm details via the link
http://weas...nk
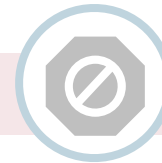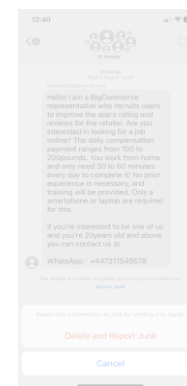
Most common types of fraud

Spam SMS

Spam messages are usually marketing messages that are sent to you without you requesting them. The people who send these messages may be trying to access your personal information (smishing), sell you a premium rate service or encourage you to contact them so that you can be referred to another company that will try to sell you something.

Legitimate marketing messages will usually be received from a shortcode or company that you recognise because in the past you've asked to receive their messages or used a service from them. Find out more about shortcodes.

Report the message to us by:

1. Forwarding the unwanted message free of charge to 7726

2. Forwarding the number of the person who sent you the message free of charge to 7726

3. If you're worried about the spam messages you've received, you can also report your message to the Information Commissioner's Office (ICO) who will be able to help you

4. It may not be possible for the ICO to follow up individual complaints if you haven't got any details about the company.

While flagging non-contacts is valuable, this could be more attention-grabbing, by breaking from usual colour schemes.
Where possible, **providing further information on why the message has been flagged as suspiciou**s will be helpful (for example, the inclusion of a link).

GUIDANCE:

VISUALLY GRAB ATTENTION

EXPLAIN WHY A RISK IS BEING IDENTIFIED

SMS

Thinks
Insight & Strategy

05. Recap of implications

Adapted guidelines to support the tech & telco sectors to deliver effective fraud warnings

Status	Guideline	Summary
Retain guideline	**Provide a clear CTA**	There are opportunities for the sectors to advise consumers on practical steps to take to ensure the legitimacy of their journey (e.g. safer ways to pay, suspicious requests to look out for).
	Tailor the warning	Tailoring the warning shared with consumers will increase relevance and grab attention regardless of which sector or transaction is generating the warning.
	Explain why a risk is being identified	Providing contextual information when warnings are triggered helps consumers to understand the presence of positive friction in their journeys and grab attention.
Retain guideline with considerations	**Visually grab attention**	Breaking from the brand's usual look, feel and tone makes warnings stand out. This is enough to grab attention, without using alarmist visuals, that the sectors are likely to be wary of using at this stage.
	Be firm and clear	Clarity and use of simple English is recommended. Firmness of tone will indicate that the sectors are taking protecting consumers seriously and this should be positioned as positive reputationally. However, they are also likely to be sensitive to being firm in borderline cases.
	Humanise the experience	Sharing personal experiences of scams shows they can happen to anyone. However, space limitations will be a challenge for both sectors, with this guidance likely to be more appropriate for warnings included in broader communications and consumer education.
	Refresh warnings regularly	Refreshing warnings regularly prevents them from becoming 'wallpaper'. However, the focus for these sectors should be on getting the basics right first.
To consider in the future	**Create a pause**	A low-friction user experience is key to value propositions, particularly for the tech sector. As such, the sectors are likely to resist implementing a pause. Focusing on providing a clear CTA and encouraging consumers to think and pause of their own volition is likely to be more effective.
	Demonstrate individual consequence	As the tech and telco sectors are not typically involved in reimbursement, there is less incentive to emphasise individual consequence than in the finance sector. However, focusing on loss aversion (rather than personal loss) may be a route in.

Looking to the future

There are examples of best practice in effective warnings throughout the tech and telco sectors, as shown in the user journeys.

However, implementation of warnings is inconsistent and levels of engagement among the sector are mixed.

The evidence has shown that principles that work for the finance sector can be adapted and applied to the tech and telco sectors.

The guidelines provided in this deck give UK Finance an evidence base in which to ground future conversations with the tech and telco sectors. These conversations can help to understand the sectors' plans and any opportunities for future collaboration.

UK Finance will have a strong role to play in continuing conversations and collaboration between the finance and tech and telco sectors to ensure learnings are shared.

Thinks
Insight & Strategy

06. Appendix

i.   Additional journey maps
ii. Bibliography

Thinks
Insight & Strategy

Facebook Marketplace *high chance of scam scenario*

Stage of Journey	Searching for products	Deciding on pet	Messaging seller	Optional educational resources

Image				

Current warnings	There are no warnings at this stage, despite selling pets being a common area for fraudsters.	There are no warnings at this stage.	There are no warnings or guidance on what might be suspicious in a seller account*.	Elsewhere on the website, there is optional advice on scams and fraud. However, this relies on the user seeking out this information.

*For example, being registered this year and having a non-human profile picture.

Facebook Marketplace

Thinks
Insight & Strategy

Facebook Marketplace *high chance of scam scenario*

Stage of Journey

Searching for products	Deciding on pet	Messaging seller	Optional educational resources

Image

There are products that are known to be at higher risk of scam on e-commerce sites, such as the sale of pets. There is an **opportunity to provide a more tailored warning** when consumers search for these products and **explain why they are high risk**.

Follow-up advice is also likely to be welcomed to help consumers navigate a high risk space safely.

GUIDANCE:

TAILOR THE WARNING

EXPLAIN WHY A RISK IS BEING IDENTIFIED

The account in question was registered this year and has no images of themselves.

Facebook Marketplace

Thinks
Insight & Strategy

Tinder

	Viewing a profile	Messaging another user	Reporting a fraudulent profile	Optional educational resources
Stage of Journey				

| **Image** | | | | |

| **Warning** | Users have the option to "Photo Verify" their profiles, and to choose to only allow Photo Verified users to message them. | Before messaging another user, the "Request Photo Verification" feature allows users to request the other user completes Photo verification. | Users can report 'spam' in the app. | The Tinder website contains "Dating Safety Tips". |

Dating apps

Tinder

Stage of Journey	Viewing a profile	Messaging another user	Reporting a fraudulent profile	Optional educational resources

Image

> **Explaining why an unverified profile is a risk will act as an incentive for more users to verify themselves.**
>
> As with Hinge, platforms may wish to use sensitive language so as not to discourage users. Therefore, it is even more important that the warning is tailored to make it clear how the user can stay safe.

GUIDANCE:

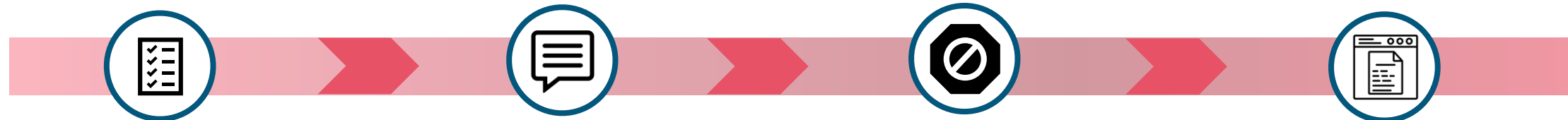**EXPLAIN WHY A RISK IS BEING IDENTIFIED**

TAILOR THE WARNING

tinder

Thinks
Insight & Strategy

Telco

SMS (Android)

Stage of Journey	Pre-screening	Incoming text	Blocking or reporting	Optional educational resources

Image

Current warnings	Some networks screen incoming messages and flag or block suspicious activity*. Pre-screening systems vary by network.	On Android, unknown contacts are not always flagged. However, some frequently flagged numbers display a fairly eye-catching warning.	Suspicious numbers can be flagged as 'spam', sharing their details with both their network & Android fraud detection systems.	Networks provide information online about how to identify and respond to suspicious messages. Information has to be accessed proactively.

*While networks' systems vary, key determinants appear to be reports by other users, content similar to other common fraudulent approaches, and high frequencies of outgoing texts/calls.

SMS

Thinks
Insight & Strategy

Telco

SMS (Android)

Stage of Journey

Pre-screening

Incoming text

Blocking or reporting

Optional educational resources

Image

While the visual style of warnings are more eye-catching on Android than iOS, the lack of a warning for all unknown numbers appears to be an oversight.

Explaining why a risk has been identified and what the user should do next will help to elevate this warning even further.

GUIDANCE:

EXPLAIN WHY A RISK IS BEING IDENTIFIED

PROVIDE A CLEAR CTA

SMS

Thinks
Insight & Strategy

Sources cited in this report

- Barrett, C., 2023, 'It's Time Social Media Platforms Unfriended Fraudsters', Financial Times. https://www.ft.com/content/884cd0c4-c8bc-438c-b9c2-ae74448e33ae

- Burge, P., 1997, 'Fraud detection and management in mobile telecommunications networks', European Conference on Security and Detection, https://ieeexplore.ieee.org/document/605807

- Consumers International, 2019, 'Social Media Scams: Understanding the Consumer Experience to Create a Safer Digital World', https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf

- eBay, 2023, Press release https://www.ebayinc.com/stories/news/ebay-acquires-3pm-shield-to-bring-advanced-marketplace-compliance-technology-in-house/

- Hermann, J., 2021, 'How Did We Get So Stuck on Here?', New York Times https://www.nytimes.com/2021/05/11/style/social-media-stuck.html

- Home Office, 2022, 'Fraud Sector Charter: Telecommunications'.

- Home Office, 2023, 'Fraud Strategy: Stopping Scams and Protecting the Public'.

- Home Office, 2023, 'Online Safety Bill / Act 2023'**

- House of Lords Digital Fraud Committee, 2022, 'Fighting Fraud: Breaking the Chain'.

- Meta, 2023, 'Fraud and Deception Policy'. https://transparency.fb.com/en-gb/policies/community-standards/fraud-deception/#policy-details

- Napoli, P., and Caplan, R., 2017, 'Why Media Companies Insist They're Not Media Companies, Why They're Wrong, and Why It Matters'. First Monday. https://firstmonday.org/ojs/index.php/fm/article/view/7051/6124

- National Trading Standards, 2023, https://www.nationaltradingstandards.uk/news/19-million-lose-money-to-scams-but-fewer-than-a-third-report. Survey Report.

Sources are listed alphabetically by author/organisation. All links accessible on 19.01.24
* The Online Safety Bill passed into law in October 2023, during the period of research for this report

Thinks
Insight & Strategy

Sources cited in this report

- Ofcom, 2022, '*Good Practice Guide to Help Prevent Misuse of Sub-Allocated and Assigned Numbers'*.

- Ofcom Advisory Committee for England (ACE), 2023, '*User-Generated Content-Enabled Fraud and Scams'*.

- Office for National Statistics (ONS), 2022, '*Crime Survey for England and Wales (CSEW)'*.

- 2023 Riefa, C., 2019, '*Consumer Protection on Social Media Platforms: Tackling the Challenges of Social Commerce',* EU Internet Law in the Digital Era; Regulation and enforcement. *https://link.springer.com/chapter/10.1007/978-3-030-25579-4_15*

- Smaili, N. and Rancourt-Raymond, 2022, '*Metaverse: Welcome to the New Fraud Marketplace'.* Journal of Financial Crime 31, no. 1, https://www.emerald.com/insight/content/doi/10.1108/JFC-06-2022-0124/full/html

- Sneade, P., 2022, '*Tackling Fraud and Scams: An Ecosystem-Wide Approach',* Frontier Economics Ltd. https://home.barclays/content/dam/home-barclays/documents/news/PressReleases/Tackling-Fraud-and-Scams-An-Ecosystem-Wide-Approach.pdf

- techUK, 2023, '*How UK Tech Companies Are Playing Their Part to Tackle the Rise of Online Fraud',* https://www.techuk.org/resource/how-uk-tech-companies-are-playing-their-part-to-tackle-the-rise-in-online-fraud

- UK Finance, 2022, *Annual Fraud Report.*

- Which?, 2023, '*Make Tech Giants Take Responsibility',* https://www.which.co.uk/campaigns/tech-giants-responsibility

- Which? Press Office, 2021 https://press.which.co.uk/whichpressreleases/smishing-attacks-in-the-uk-grew-by-nearly-700-in-the-first-six-months-of-2021-which-reveals

- Yonder Consulting for Ofcom, 2023, '*Executive Summary Report: Online Scams & Fraud Research',* https://www.ofcom.org.uk/__data/assets/pdf_file/0025/255409/online-scams-and-fraud-summary-report.pdf

Sources are listed alphabetically by author/organisation.. All links accessible on 19.01.24.

Thinks
Insight & Strategy

Additional sources included in the evidence review

- Bailey. J, Giambrone Law, 2023, 'How the Online Safety Bill Could Impact on Online Financial Scams and Fraud'. https://www.giambronelaw.com/site/news-articles-press/library/articles/financial-scams-frauds-online-safety-bill

- Button, M., Hock, B., Shepherd. D., Gilmour. P.,2023, 'Understanding the Rise of Fraud in England and Wales through Field Theory: Blip or Flip?'. Journal of Economic Criminology 1 https://doi.org/10.1016/j.jeconc.2023.100012.

- Dachis, A., 2019 'How Google Legally Profits From Massive Fraud on Its Platform (and What You Can Do About It)'. https://www.extremetech.com/internet/294213-how-google-legally-profits-from-massive-fraud-on-its-platform

- Venkataramakrishnan, S., 2022, 'Banking, Tech and Telecoms Groups Combine to Gather Intelligence on Scammers', Financial Times https://www.ft.com/content/68a13465-3d4e-4ae9-a2ef-7bf23f88761c

- Barrett, C., 2022, 'Instagram Must Stop the Scammers Targeting Gen Z'. Financial Times. https://www.ft.com/content/b2702828-a094-4edd-a440-154c4dbbd6c4

- Fraud Advisory Panel, 2021, 'Joint Position Statement: Preventing Fraud on Social Media, https://www.nebrcentre.co.uk/wp-content/uploads/2022/08/Social-Media-and-Fraud-Apr21.pdf

- Prenzler, T., 2020, 'What Works in Fraud Prevention: A Review of Real-World Intervention Projects'. Journal of Criminological Research, Policy and Practice 6, no. 1, https://doi.org/10.1108/JCRPP-04-2019-0026.

- Holkar, M. and Lees, C., 2020, 'Caught in the Web; Online Scams and Mental Health'. Money and Mental Health Policy Institute. https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf

- National Audit Office, 2023, 'Preparedness for online safety regulation' https://www.nao.org.uk/wp-content/uploads/2023/07/preparedness-for-online-safety-regulation-summary.pdf

- Poster, W., 2022, 'Introduction to Special Issue on Scams, Fakes, and Frauds'. New Media & Society volume 24, no. 7. https://doi.org/10.1177/14614448221099232.

- Hyde, R. and Wilson, P. 2023, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud in the UK'. Social Market Foundation interim report, https://www.smf.co.uk/wp-content/uploads/2023/07/Fraudemic-July-2023-2.pdf

- Cross, C. 2022, 'Meeting the Challenges of Fraud in a Digital World', The Handbook of Security.. https://doi.org/10.1007/978-3-030-91735-7_11.

Sources are listed alphabetically by author/organisation,. All links accessible on 19.01.24.

Thinks
Insight & Strategy

Thank you!

Carol McNaughton Nicholls | cmcnaughtonnicholls@thinksinsight.com
Talia Coroniti | tcoroniti@thinksinsight.com
Michael Keating | mkeating@thinksinsight.com
Orla O'Dwyer | oodwyer@thinksinsight.com
Tim Postle | tpostle@thinksinsight.com

hello@thinksinsight.com
T: +44 (0)20 7845 5880
www.thinksinsight.com

Thinks
Insight & Strategy