CCUK best practice guide:
"Sharing information to prevent, detect and report fraud"

December 2024

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312

A. Introduction

1. This guidance is created for Comms Council UK (CCUK) members to support the implementation of a new information sharing initiative, supported by National Trading Standards (NTS).

2. The key aims of the initiative are to:
   a. Work collectively to help prevent, detect and report fraud effectively;
   b. Share information with a professional organisation who will help us create a feedback loop and improve the quality of information shared going forward; and
   c. Simplify information sharing and enable CCUK members to work together to stamp out scam calls and criminals within our sector.

3. This guidance outlines how, as CCUK members, we can all practically get involved with this new initiative, ensuring we all share and act on information in an appropriate way.

B. Why this guidance and initiative is necessary

1. Scams, fraud and nuisance calls are all serious problems that are at the top of the political and regulatory agenda. Criminals are becoming increasingly sophisticated and inventive in finding ways to scam or defraud individuals and businesses via calls, messaging and texts.

2. There are several initiatives taking place to tackle these issues with Government, regulators, law enforcement bodies, specific sectors (e.g. banking) and the telecoms industry. They are all well-intentioned but lack a joined-up approach, without any reporting or analysis, to be truly effective countermeasures.

3. There is no single solution to resolve the problem, however there are a number of tactics available to help minimise it. These tactics range from proactive measures, such as call blocking and caller verification, to reactive measures including reporting incidents of fraud to the relevant authority and retrospectively blocking service.

4. Comms Council UK (CCUK) believes that, collectively, our members are well-positioned to get involved more pro-actively in this space. So, we have joined forces with the National Trading Standards (NTS) Scams Team to launch an initiative which enables members to share information appropriately both within the CCUK membership and with relevant industry stakeholders to prevent, detect and report fraud.

5. By doing what we can to prevent fraud, we can not only save victims from substantial financial losses, but we can also help rebuild trust in telephone calls, which in turn benefits our members by rebuilding the confidence to use voice as a primary means of communication.

6. The NTS Scams Team/CCUK understand that it is difficult to know what information can be shared and who best to share it with and in what format. The NTS Scams Team has considerable experience in managing similar scenarios for other industries, including banking and mail services, and so are ideally placed to help us make this a success.

C. Anonymised information sharing with National Trading Standards

1. In the past, members have shared concerns with CCUK that they are nervous to share information about potential criminals publicly. These concerns arise from uncertainty about what can and cannot be shared without breaching privacy rules, but also the level of evidence that members feel they need to provide to justify sharing negative feedback is sometimes difficult to reach.

2. This reluctance leads to those facilitating scam calls often moving freely between providers and the authorities taking a 'whack-a-mole' approach to closing them down.

3. This is why CCUK has joined forces with the NTS Scams Team to address these concerns. Their considerable experience will help ensure this is a safe place to share information, they will take reports of proven or potential criminals and feed it back to CCUK members anonymously. They are also able to use their existing intelligence to build patterns and profiles that further strengthen the information they are given, and this can again be anonymised and shared with members to help prevent further support for the perpetrators of fraud.

To report proven or potential criminal behaviour to the NTS Scams Team, please email scamsteamadmin@surreycc.gov.uk, including:

- **Company or individual name**
- **Directors and shareholders details, where applicable**
- **Addresses and phone numbers**
- **Nature of the business and services requested**
- **Summary of issues, complaints or concerns**

D. Key actions requested of all members

1. Ensure you are following best practice guidance to prevent misuse of sub-allocated and assigned numbers (please refer to our guidance released April 2024).

2. Update your internal process for responding to reports of potential misuse to include notifying the NTS Scams Team, as described in the following guidance.

3. Provide CCUK with your nominated 'single point of contact' to ensure you receive data shared by other members in an appropriate way. These SPOCs are to be shared with the NTS Scams Team.

E. Information sharing guidance

1. There are two factors to consider when sharing information. The first is 'personal data' which is clearly defined and protected by the Data Protection Act 2018. The second is more general information about a business or individual which may be commercially sensitive or has the potential to be defamatory.

When should you share information

2. Our aim is to more promptly stop criminal behaviour. By sharing information about these individuals or businesses with other service providers we hope to be able to reduce their ability to simply hop between providers as they so often do today.

3. If you have reason to suspect that one of your customers is perpetrating fraud or facilitating others to do so, or even has been rejected by you based on your 'know your customer' checks, this should trigger you to share information under this new scheme. Whilst individual reports may not alone be enough to trigger enforcement activity, multiple reports can build a picture that can ultimately help prevent the criminals receiving service from our sector and in some cases support enforcement action.

Sharing commercially sensitive or potentially defamatory information

4. There is, of course, an expectation that members will act in the best interests of the wider industry to support the aims of this initiative through:
    a. Ensuring reports are made expressing genuine concerns about potential criminal behaviour as opposed to passing on vexatious complaints.
    b. Overcoming concerns of being judged for exposing any potential vulnerability within a business.

5. Within the initiative, we support members in two ways:
    a. We would encourage members to report genuine concerns promptly, as the sooner information is shared the sooner interventions can be used to limit their ability to perpetuate fraud. *If at a later date the concern proves unfounded, then this too can be reported into the system and shared within the CCUK members' community.*
    b. By anonymising data and feedback, we can mitigate the risk of being named directly as a business involved.

6. It has become very apparent that any provider can be susceptible to some very sophisticated criminals and criminal networks and only by working together and being as open as possible can we hope to block their progress.

7. NTS Scams Team will endeavour to process reports from you within two or three working days, and as demand fluctuates they will endeavour to resource appropriately to ensure information is acted on promptly.

8. The type of information needed by the NTS Scams Team will vary in each case but will usually include:
    - Company or individual name
    - Directors and shareholders details where applicable
    - Addresses and phone numbers
    - Nature of the business and services requested
    - Summary of issues, complaints or concerns

9. When preparing your data to be shared, please check what could be considered 'personal data'.

Personal data

10. Data protection law is clear about what personal data can be shared and in what circumstances and the ICO has published a Code of Practice[1] to assist organisations with compliance. What follows are key highlights relevant to this specific guidance only and assumes you are already familiar with and compliant with your general obligations under the Data Protection Act 2018.

11. The key principles to be followed when sharing any personal data are:
    - You must be able to demonstrate compliance with the regulations.
    - You must share personal data fairly and transparently.
    - You must identify at least one lawful basis for sharing data before you start any sharing:

[1] The Data Sharing Code of Practice is a statutory code made under section 121 of the Data Protection Act 2018. It is a practical guide for organisations about how to share personal data in compliance with data protection law. To see full details visit here.

- **Legal Obligation**: If there is a legal requirement for telecommunications providers to share information about suspected criminal activity (e.g., compliance with the Investigatory Powers Act 2016 or other statutory requirements), then the **legal obligation** basis applies. Under GDPR, organisations can process (and share) personal data when necessary to comply with a legal obligation.
- **Legitimate Interests**: If no specific legal requirement exists, service providers could rely on **legitimate interests** as a lawful basis for sharing data. Under this basis, data-sharing must be necessary to prevent or detect crime, and it must balance the provider's interests with the privacy rights of the data subjects. Service providers need to conduct a legitimate interests assessment (LIA) to demonstrate that their interest in preventing fraud or other criminal activities outweighs any potential risk to the individual's privacy.

- You must process personal data securely with appropriate measures in place.

12. Personal data only includes information relating to a natural person who:
    a. Can be identified or who are identifiable, directly from the information in question; or
    b. Who can be indirectly identified from the information in combination with other information.

13. The most common personal data in the context of this guidance is likely to be a name, address or IP address.

14. Remember, if you are sharing publicly-available business information, this is not classified as personal data. However individuals acting as sole traders, company directors etc – and data related to them as an individual – is likely to constitute personal data.

15. You can share personal data where it is necessary and proportionate to do so. The Data Protection Act (DPA) 2018 provides us with a framework to allow the sharing of personal data with law enforcement authorities that need to process personal data for the law enforcement purposes, such as the prevention, investigation and detection of crime. The NTS Scams Team DOPA are classed as a 'competent authority' which means they are treated the same as law enforcement in this context.

16. The DPA framework does not force you to disclose personal data, but it allows you to disclose personal data on a voluntary basis, provided that it is necessary and proportionate to do so.

17. When sharing personal data, you need to consider the following points and make a note of the decisions made so you can explain your reasoning if challenged:
    - Consider the impact: Keep a note explaining what you are sharing and why and what the potential outcome of your action could be.
    - Consider why you are sharing: In this context you will be sharing data to prevent or report criminal activity.
    - Consider how you are sharing: It is important to contain exposing personal data to the intended recipient, in this case by sending an email to the nominated address and avoiding cc/bcc addresses.
    - Keep records: Make a note of what data you have shared, who to and your reason for doing so.

18. The ICO has recently released further guidance on the topic, this can be found here.

19. If you have any queries about this guidance or our information sharing initiative, please contact team@commscouncil.uk

ENDS