7 November 2024 | National Cyber Security Centre NCSC

Phone fraud in the cyber domain

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
National Cyber Security Centre NCSC

Contents

1 Introduction

Phone users are increasingly subject to fraudulent calls. However, the phenomenon of phone fraud is not new. Criminals have always tried to manipulate people through phone calls to try to obtain money. This report explains how the scam works, how common it is in the context of technological developments and how to identify such a fraud attempt. It also examines the measures taken by telecommunications service providers and lawmakers to address the situation.

1.1 Scam or fraud?

In everyday speak people often refer to ‘phone scams’, but the correct legal term for this offence is ‘fraud’.

> Art. 146 Swiss Criminal Code (Fraud)
>
> Any person who with a view to securing an unlawful gain for themselves or another wilfully induces an erroneous belief in another person by false pretences or concealment of the truth, or wilfully reinforces an erroneous belief, and thus causes that person to act to the prejudice of their or another's financial interests, shall be liable to a custodial sentence not exceeding five years or to a monetary penalty.

1.2 Phone fraud in the cyber domain

Phone fraud (in the cyber domain) is widespread internationally, as trust can be built up during the call allowing the victim to be manipulated in a targeted manner. This allows the fraudsters to react immediately and appropriately to potential doubts on the part of the victim. Their aim is to swindle money, personal details or other sensitive data by pretending to call on behalf of a trustworthy organisation - e.g. a bank, a government agency or another company. They also use guises likely to be known to the callee - such as a customer, a helpdesk employee or even a work colleague such as a manager or someone from the IT department - as a pretext for their fraud attempts. The ‘grandchild trick’ is a classic example that plays on the private life of the callee: a fraudster calls an elderly person and pretends to be their granddaughter or grandson in need of money.

Technological advances enable criminals to combine the agility of direct oral conversations with cyber technologies. The latter allow them to refine their techniques and use the data obtained to their advantage. New technologies can be used before, during and/or after a fraud attempt.

Phone scams harnessing the use of new technologies have spread out in the early 2000s when cybercriminals began to use Voice over IP (*VoIP*) technology, voicemail applications and automated calling systems for phone phishing. VoIP technology can be used to create fake phone numbers and disguise a caller’s identity. This makes the calls look like they are coming from legitimate companies or institutions. Voice over IP also allows the perpetrators to make hundreds of automated fraudulent calls over the internet, making it difficult to trace the numbers used.

But now there are many ways in which criminals can combine phone calls and cyber methods. For example, they may dial a random number. Or on the contrary, they may first seek to collect personal data from publicly available sources, social networks or previous data leaks to person-

alise their attacks and gain the trust of victims. Phone fraud in the digital space is often supplemented with other forms of social engineering[1], such as sending phishing mails or creating fake websites to increase the credibility of the attack. For example, some criminals trick their victims into calling them by first sending them an email.

As soon as a victim has handed over their data, the criminals can use it to enrich themselves through fraud, by committing further criminal offences or by selling the data on to other criminals. In the latter case, the criminals are said to act as initial access brokers. Such threat actors specialise in compromising computer systems and networks in order to then sell the unauthorised access to other threat actors.

2 Techniques used

Phone fraud in the digital space is based on two aspects - technological progress in the field of phone communication and pure psychological manipulation.

2.1 Technological developments

The technological parameters include, for example

- Automated calls (robocalls):
  Such calls are made *en masse* and are usually made in English. By giving the impression that they come from well-known organisations, the aim is to create proximity and trust. Thanks to this technique, criminals can reach a large number of potential victims and keep human resources low. They can therefore concentrate on people who decide to stay on the line after listening to the automated call.
- Falsification of phone numbers (phone spoofing):[2]
  The cybercriminals falsify the caller ID so that the callee sees a trustworthy number. This is intended to entice callees to answer the call. The National Cyber Security Centre (NCSC) has observed cases of phone spoofing in which not only the phone numbers of banks but also police authorities have been faked.
- Inducement to call back:
  The criminals send a recorded audio message to several employees of a company simultaneously. The caller ID is probably digitally modified so that it resembles that of a person within the organisation. The recording contains a message purporting to be urgent. The person whose voice is heard often pretends to be someone trustworthy and requests a call back to a specific number for more detailed information. The call back number then corresponds to a number that the criminals have chosen in advance specifically for the scam.

2.2 Deception and manipulation

Cybercriminals are skilful in manipulating their victims. The use of psychological techniques such as manipulation with the aim of obtaining confidential information or money is known as social

[1] See section 2.2. for definition

[2] Spoofing generally involves disguising a communication from an unknown source as a communication from a known and trusted source (similar to identity theft).

engineering. Such an approach makes use of basic human characteristics and behaviour to deceive victims. For example, cybercriminals use public sources to find out about their targets in advance and use this personal information to appear legitimate, gain the victim's trust and obtain additional information. A key element of social engineering is the use of emergency scenarios. The perpetrator plays on crisis situations such as the imminent closure of an account or an accident to get the victim to disclose sensitive information quickly. Someone who is under stress has no time to think logically and rationally about what they have been told. Other emotions can also be manipulated for criminal purposes, such as curiosity, guilt, empathy, fear or respect for authority. These emotional manipulations lure the victim into acting rashly.

3 Criminals and technological progress

Since the emergence of phone fraud in the 2000s, the cyber phenomenon has continued to evolve and this is set to continue. Due to technological progress, criminals have ever more powerful tools at their disposal. In the early stages, calls mainly came from international or internet numbers. Today, criminals can spoof local phone numbers, masking their identity from the callee by displaying a local phone number.

3.1 Examples of SIM box, malware and eSIM misuse

One technological development that has made phone fraud easier for criminals is the SIM box.[3] This is a device that uses multiple prepaid SIM cards, often purchased with fake identities, to route international phone calls to a desired network as a local call. This type of fraud exploits the difference between local and international rates so that perpetrators only have to pay the local rate. Today, more and more criminals are resorting to this method as it has become much cheaper.

Another technological advance consists in using malware[4] to perfect a scam. Some malwares can manipulate devices, implant pre-recorded voice messages and redirect calls to fraudulent call centres. Once such malware has been downloaded and installed, it demands the victim's consent to access their contacts, microphone, camera, location service and more. A Trojan, for example, can trick victims into believing that they are communicating with customer services when they dial their bank's phone number.

More recently, the emergence of the eSIM has enabled criminals to develop another variant of phone fraud in the cyber domain. Using eSIM technology, the digital SIM card is embedded in the device, which offers users flexibility and convenience, but also harbours new fraud risks. In the case of eSIM fraud, criminals use techniques such as SIM swapping or social engineering to obtain the victim's mobile phone number. Using these methods, they can access various services such as online banking and social networks that are authenticated via that number. As many online services use SMS-based two-factor authentication (2FA), criminals can intercept security codes by taking over a mobile phone number and log into accounts without authorisation. This can lead to both financial losses and breaches of privacy. To protect themselves, users should use strong passwords and alternative authentication methods such as authentication apps or security tokens. Furthermore, mobile network providers can provide additional security by applying a stricter verification process when changing eSIM profiles.

[3] https://www.infosysbpm.com/blogs/bpm-analytics/what-is-sim-box-fraud.html

[4] e.g. voice phishing (vishing) application, Trojan horse

3.2 Emergence of artificial intelligence (AI)

Since the emergence of artificial intelligence (AI) methods such as machine learning, these new technologies are increasingly being used to automate calls and evade detection systems. One obstacle for criminals is language. While reliable translation tools are now used for emails and text messages, this is still rarely the case for phone calls. Calls are therefore usually made in English, the most widely spoken language worldwide. But this is where AI could be of use to criminals in the future. Today, it is common to share spoken content over the internet. Thanks to the emergence of commercially available software applications for generative artificial intelligence (GenAI), a few clicks are enough to deliver relatively credible results and lay the ground for a fraud attempt. This development has a significant impact on how criminals operate and therefore on what needs to be done to defend against voice-based threats. All criminals need to impersonate a voice is an audio sample such as a recorded phone call or a video published on social media.

The more information is shared via the internet or on social networks, the higher the risk of identity fraud and other cybercriminal activities. It is important to be proactive by limiting the amount of personal data published on the internet, or at least being aware of the potential consequences of making such information public.

In Switzerland, the main AI-based fraud schemes include phone fraud, investment fraud (fake celebrity endorsement) and fake sextortion with AI-generated images. Due to the relatively low number of reports in this area, the NCSC assumes that these are probably the first attempts by cybercriminals to find out how AI can be used profitably for cyberattacks in the future. In many cases, it is difficult to determine the extent to which artificial intelligence has been used. For example, it can only be surmised whether a translation tool was used or not. The use of AI is only obvious in a small number of cases.

4 Cyber phone fraud in Switzerland

Cyber phone fraud is an established phenomenon in Switzerland. Such cases have been reported since the creation of the Reporting and Analysis Centre for Information Assurance (MELANI) in 2004, which later became the National Cyber Security Centre (NCSC).

4.1 Fake support and fake support pop-up

The most recurrent cases of cyber phone fraud registered in Switzerland involve victims being informed by scammers purporting to be from Microsoft support that their computer had been hacked and that they needed to react immediately. Victims were tricked into installing remote access software such as AnyDesk onto their computers. The criminals then tried to log into the victim's online banking system and make money transfers.

For some time now, the NCSC has also been observing a similar variant in which pop-up windows appear when advertising websites are displayed. In this case, the pop-up is designed in such a way that the user believes the content of the pop-up. This states that the computer is infected with a virus and that a certain phone number should be called to help with troubleshooting. The scam then continues as described above.

4.2 Fraudulent calls from alleged bank employees

The NCSC also regularly receives reports concerning calls from alleged bank employees enquiring whether the person called has made a certain payment.[5] In many cases, the caller claims, for example, that a debit has been made for a flat screen in an electronics shop and recommends calling the fraud department of the cantonal police immediately. A phone number supposedly for the police is given to the victim. The victim is then encouraged to carry out various actions and check their online banking activities. They are asked to confirm certain details so that the payment can be cancelled. The NCSC assumes that in these cases the victim is to be tricked into accessing a website created by the criminals from which they can cancel the fictitious, allegedly fraudulent payments. Access data and one-time passwords are requested for this purpose. In the background, the criminals log into the victim's online banking account using the data they have obtained to initiate payments to their benefit. Meanwhile, the victim is made to believe that the payment has been successfully cancelled. Here too, there are variants in which the cybercriminals attempt to gain access to the victim's computer using remote access software to then carry out fraudulent actions.

4.3 Robocalls - Automated calls from alleged authorities

Since July 2023, Switzerland has been experiencing waves of phone fraud on a large scale. Criminals make automated calls to thousands of Swiss people every day, allegedly in the name of the police, and accuse the potential victims of a criminal offence. In these cases, numerous calls are made simultaneously. If a person answers the call, they hear a recorded message claiming that the call concerns a police investigation. To obtain further information, the person should press ‘1’. If they do so, they are connected to a call centre employee. The callee is informed that they are suspected of being involved in a case of money laundering or another criminal offence, and that their bank account is being frozen. In this scam, the criminals also use AnyDesk or similar remote access software to access the victim's bank account.

The criminals use call centres and usually speak English with a foreign accent. However, the NCSC has noticed that there is a growing tendency for callers to speak good German or French.

They falsify their caller ID, which is known as spoofing. They often choose random mobile phone numbers, which are displayed to the callee. The callee may then try to call back but would then reach the actual owner of the phone line, who are unaware that their number has been misused by the scammers.

Thanks to the recorded message trick, criminals can carry out more calls at the same time and are therefore able to better target their victims by only processing calls that are answered and where callees stay on the line and follow instructions of the tape recording, for example.

The NCSC found that some people who had expressed doubts about the authenticity of the call during the conversation were subsequently called back by what appeared to be a public Interpol number. They were then asked to verify the number online enabling the criminals to gain credibility.

Although there are some differences, there are many similarities between the classic fake support calls and the automated threatening calls:

---

[5] See ‘In focus‘: https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2023/wochenrueckblick_44.html

- The perpetrators operate from call centres.
- They use hijacked phone numbers, often with the same area code as the target numbers.
- The victims are tricked into installing a remote access software and authorising access to online banking systems.

4.3.1 Differences between fake support calls and robocalls

Figures 1 and 2 illustrate the impact of automated threatening calls allegedly made by the police on the number of reports received by the NCSC over the last twelve months. The phenomena of 'fake support' and 'threatening calls allegedly made by the police' are compared below and the most relevant differences are highlighted.

In both cases, the aim is to convince potential victims to download a remote access software, which grants the criminals access to the computer. With fake support, this is done in one-to-one calls, as described above. The criminals contact each potential victim individually. As a result, reports to the NCSC have now been at a consistently low level for a year and a half. On average, the NCSC receives around 60 reports per month. The offenders' approach appears to be resource-intensive and not very productive for them.

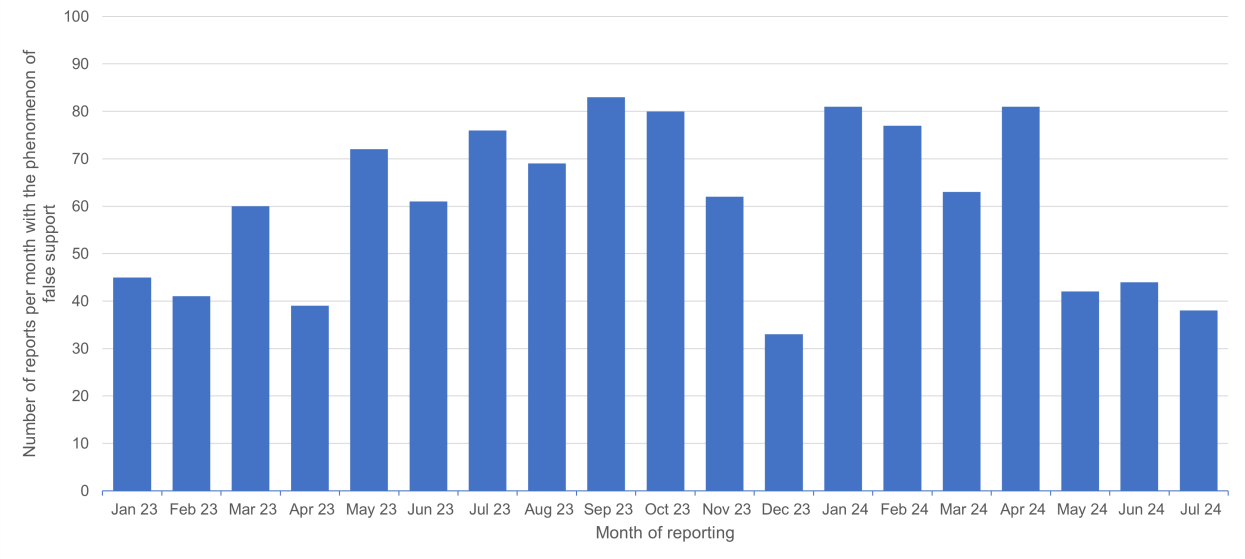

***Figure 1**. Reports of fake support calls per month. The number of reports is distributed regularly throughout the year and is at a low level.*

Therefore, criminals have looked for ways to make this type of scam more effective. The criminals do not personally make these calls, supposedly made by the authorities, but instead select many different numbers automatically at random within a short period of time. Only those who stay on the line and press the button mentioned in the automated announcement are forwarded to a scammer. This allows criminals to only process calls they deem promising. As a result, the situation in terms of incoming messages is very different. Until June 2023, this scam was hardly known in Switzerland. From July 2023, the number of reports rose steadily and finally reached the 1,000 mark per month in the following month. This was probably the criminals' first test run. In October of the same year, the number of reported cases rose significantly. At times, the NCSC received around 1,000 reports a week related to this scam alone. After a short break at the beginning of 2024, the number of reports again rose sharply in February, once again reaching record levels of over 1,500 per week. From the 31st of July on, the NCSC was only receiving around one hundred reports per week regarding this particular scam.

The number of fraudulent calls and in turn the number of reports to the NCSC hence depend less on the criminals' human resources than on the technical capabilities and efficiency of the bots that make the automated calls.

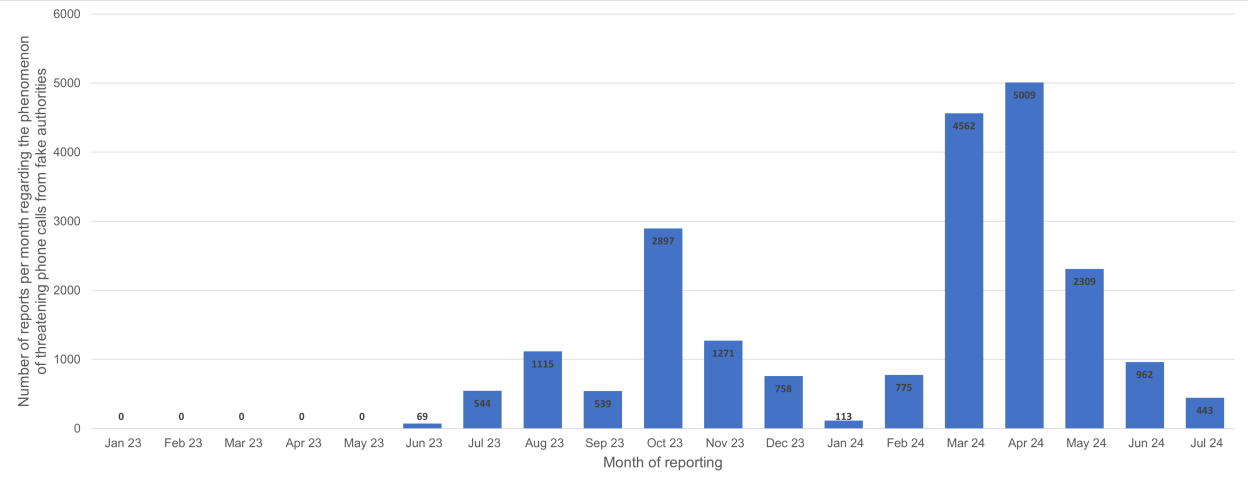

***Figure 2**. Reports of threatening calls allegedly made in the name of the authorities. The large number of reports in March and April 2024 is striking. The number of reports fell again in the summer months.*

4.3.2 Working hours of criminals

Figure 3 shows the average distribution of reports received over the course of the day, related to reports of fraudulent calls from alleged authorities only. The NCSC assumes that most cases of cyber-related phone fraud are reported immediately after receiving such a call. Consequently, the time at which the fraudulent call was made overlaps the time at which the report was made. As such, the working hours of the criminals are estimated based on the times at which the reports are received.

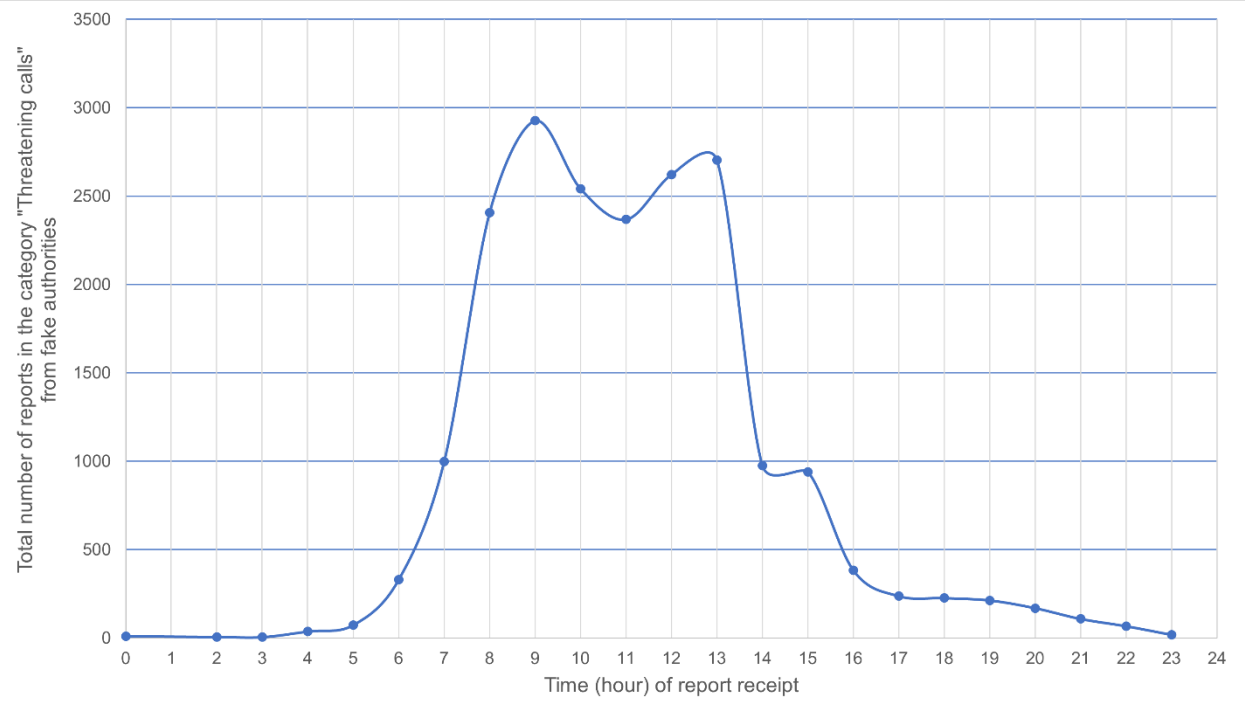

***Figure 3**. Average time distribution of calls allegedly made by the authorities. The reports start at 5am and reach a first peak at 9am. A second peak occurs at 1pm and from 4pm onwards, the number of messages decreases again.*

The distribution is reminiscent of a 'normal working day', which starts at 6am and lasts until 4pm. Based on the drop off in the number of reports received at 11am, it can be concluded that the criminals take a lunch break - although it is not yet lunchtime in Switzerland. This might suggest that the criminals are in a country in a time zone further East.

5 View of a telecommunication provider

After considering the nature of reports submitted to the NCSC, the following section sets out the view of a Swiss telecommunication provider.

5.1 Cat-and-mouse game

Criminals are constantly developing new methods to defraud phone customers. They seek to maximise their chances of success by combining a variety of techniques. One of these techniques consists in identity fraud. By concealing the identity of the person making the call, the perpetrators know that a call is more likely to be answered as the caller appears trustworthy. The method seems to be successful, as the number of calls made under false identities has increased by 50 per cent in the last two years. That trend is likely to continue.

The use of artificial intelligence (AI) in phone fraud is also very popular with criminals. Although the methods used to make automated calls are currently still relatively simple, it is only a matter of time before criminals develop more complex techniques to optimise their fraud attempts. Regardless of whether the callers use a fake identity, it is currently neither permitted nor technically possible for telecommunications providers (*voice service* providers) to identify robocalls that use AI methods based on content, language or voice. This is a significant disadvantage considering that cybercriminals are using AI for malicious purposes. Telecommunication providers could use the same AI-powered technical capabilities not only to monitor call patterns, but also to identify robocalls based on an analysis of call content. With the help of automated and privacy-respecting alerts, they could react accordingly and take appropriate countermeasures. The current disadvantage needs to be addressed so that telecommunication providers do not remain one step behind criminals.

5.2 Measures on the part of telecommunication providers

Telecommunication providers have used a range of technical and legal measures to fight against criminals. They can use technical measures to block such phone attacks and limit the number of attempts:

- Call filtering can be used to analyse incoming calls and block suspicious numbers associated with phone fraud.
- Voice recognition can be used to identify callers, especially in the case of risky transactions or sensitive interactions.
- Algorithms allow providers to detect unusual call patterns or behaviours that indicate attempted attacks, such as a high volume of calls to certain numbers within a short period of time.

In Switzerland, providers rely on analysing call patterns to detect anomalies. Efforts are also being made to curb the spoofing of Swiss numbers from abroad. Another challenge is that the perpetrators are constantly adapting their techniques. It is therefore essential to alert the public to their new methods. Certain telecommunication providers, for example, regularly inform their customers

about this topic via various channels and recommend to exercise caution. Under no circumstances should personal data such as passwords and PINs be disclosed to callers. The providers also recommend that their customers activate the call filter available for both landlines and mobile phones. This also shields customers from unwanted advertising calls.

5.3 Supporting role of the Federal Office of Communications (OFCOM)

According to telecommunication providers, the necessary legislation already exists. A joint initiative of the providers and the Federal Office of Communications (OFCOM) is currently aiming to find an industry-wide solution to the problem. As soon as the Swiss telecommunication industry has found a suitable solution, OFCOM can provide support with implementation, regulation and, if necessary, supervision.

Overall, the fight against phone fraud is and remains a complex challenge. It requires close cooperation between providers, regulatory authorities and the public. This is the only way to develop legally compliant, effective technical solutions that protect customers' privacy. While a completely effective protection against phone fraud is not possible, the risk can however be reduced with the right countermeasures.

6 Protecting the individual is a legally complex task

In addition to Art. 146 of the Swiss Criminal Code, several other acts (and institution) are also relevant:

- The Federal Act against Unfair Competition (UCA) prohibits unfair business practices, including fraudulent practices such as phone scams.
- The Federal Act on Data Protection (FADP) regulates the processing of personal data and can be invoked in cases where phone fraud involves the unauthorised collection or misuse of personal data.
- The Telecommunications Act (TCA) regulates telecommunications services and networks. It can be invoked in cases where phone fraud involves misuse of the telecommunications infrastructure.
- The Swiss Financial Market Supervisory Authority (FINMA) supervises financial institutions and insurance companies. It can therefore impose sanctions on entities involved in phone fraud targeting the financial sector.

6.1 Legal aspects from OFCOM's perspective

Telecommunications law mandates telecommunication providers to protect their customers against unfair advertising calls (Art. 3 para. 1 let. u, v and w UCA). Customers must be provided with a means of shielding themselves from such calls. This is achieved by offering a call filter for instance (see section 5.2). This solution must confer protection in line with the state of the art (Art. *45a* TCA). Thus, providers must react to new technologies and procedures and adapt the functionality of the filters accordingly. As unfair advertising calls are usually accompanied by spoofing of the displayed number, the filters provided by the providers should also be suitable for combating identity theft (Art. 179^{decies} SCC) in the context of phone fraud. These elements can help to protect users against phone fraud attempts.

From the point of view of telecommunications law, a victim of fraud can invoke Art. 146 of the Swiss Criminal Code and exercise their right to information (Art. 45 TCA). This aims to ensure

that the origin, i.e. the connection from which the abusive calls originate, is traced by the providers used to make the call. Calls with spoofed numbers can be considered abusive, especially if they are made as part of a suspected fraudulent act. It remains to a criminal court to decide whether these conditions are met. However, in such case, the standard of proof of prima facie evidence is sufficient. The heart of the issue, though, is that such calls usually originate from abroad. The foreign provider, if it can be traced at all, is not subject to Swiss telecommunications law.

6.2 International legal boundaries

Another issue resides in the fact that call filtering must not lead to the blocking of legitimate calls, as this would contravene the obligation of interoperability, according to which providers must always forward calls to the recipients. It should also be noted that providers are not permitted to know the content of calls due to telecommunications secrecy. The filters must therefore be set using various indicators and function dynamically, as criminals are always changing the numbers used for fraud. If the callers use mobile phone numbers, for example, it is even more difficult for the providers to assess whether the call is legitimate, as it could well originate from a person with a Swiss phone number abroad and not from a fraudster.

In May 2024, authorities from the United States uncovered a criminal group they named 'Royal Tiger'. Their aim is to facilitate fraudulent calls via international networks. According to a press release[6], the group attempts to impersonate government authorities, banks and public service organisations. The calls are aimed at deceiving consumers worldwide by offering them supposedly reduced interest rates on their credit cards or by asking them to authorise purchase requests for orders they have never made. Currently, Royal Tiger operates out of India, the United Kingdom, the United Arab Emirates and the United States. US lawmakers have decided to create a new classification for these types of robocalls, namely Consumer Communications Information Services Threat *(*C-CIST*)*.[7]

In Austria, an amendment to a relevant ordinance came into force on 21 December 2023 (with an implementation deadline of 1 September 2024)[8], according to which Austrian telecommunication operators must verify the phone number of incoming calls from abroad made using Austrian numbers. If verification is not possible, the number may not be displayed. However, this does not prevent fraudulent calls with numbers from other, particularly German-speaking, countries, such as spoofing calls with German numbers.

6.3 Artificial intelligence and the future

In addition to the sheer technical complexity involved, there is also a problem of human manipulation using AI. On 12 December 2023, the NCSC published an article[9] on the use of artificial intelligence for fraud attempts. A combination of spoofing and voice alteration using AI offers criminals great opportunities. The better the technology becomes, the more difficult it will be to identify fraud attempts.

One way to curb spoofing would be to introduce a verification process (similar to the one used for emails) to check the origin and authenticity of the phone number. Corresponding solutions are

[6] https://www.documentcloud.org/documents/24661582-doc-402506a1

[7] https://www.documentcloud.org/documents/24661584-da-24-388a1

[8] https://www.rtr.at/9_novelle_kem-v

[9] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_49.html

currently being discussed in international bodies such as the European Conference of Postal and Telecommunications Administrations (CEPT), the Electronic Communications Committee (ECC) and the International Telecommunications Union (ITU). OFCOM is regularly involved in these discussions. The legal basis for the introduction of such processes has existed in telecommunication law since the last revision. However, for these to lead to an improvement in the situation, they would have to be introduced in as many countries as possible.

7 Precautionary measures recommended by the NCSC

One can protect themself against phone fraud by applying the following measures:

1. Do not trust all callers: End implausible calls immediately
2. Do not allow yourself to be intimidated or put under pressure
3. Never disclose passwords or PIN codes over the phone
4. Do not disclose any business information to strangers
5. Never grant strangers access to your computer, even if they appear trustworthy

8 Conclusion

In many cases the weakest point in phone fraud attempts in the digital space is the callee. If they are put under pressure, either privately or professionally, they may act rashly and carelessly, especially when presented with an alleged emergency. In these cases, it is often the victims themselves who open the door to opportunistic criminals. Today, security cannot and must not depend solely on whether users can correctly identify the threat and take appropriate measures. Criminals operate worldwide and in internationally connected networks. Conventional identification methods such as the famous 'calling line identification' are outdated due to technological advances. In contrast to emails, where DMARC authentication[10] enables spoofing techniques to be identified and restricted, there are no new authentication methods in telephony yet. According to OFCOM, trials with STIR/SHAKEN protocols[11] in North America yielded poor results. Numerous industry organisations have abandoned this standard[12], which underlines the difficulty of introducing new authentication methods on a global scale.

[10] Domain-based DMARC (Message Authentication Reporting and Conformance) is an email security protocol. DMARC checks email senders based on the Domain Name System (DNS), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) protocols.

[11] Series of protocols for authenticating callers and their data when making calls via the VoIP network (https://www.fcc.gov/call-authentication).

[12] https://commsrisk.com/global-stir-shaken-is-dead-what-comes-next/