Systemic Spotlight:

# Reducing fraudsters' theft of mobile numbers

**The Telecommunications Industry Ombudsman receives complaints from consumers whose mobile numbers have been stolen by a fraudulent third party. This new Systemic Spotlight explores the issue and how the Telecommunications Industry Ombudsman has worked with service providers to improve security and protect consumers.**

## How do fraudsters steal numbers?

Fraudsters can steal a consumer's mobile number by getting their mobile service provider to switch the number to a new SIM card in the fraudster's hands (known as "SIM swaps"). Alternatively, fraudsters try to transfer the mobile number to another mobile service.

Before attempting a SIM swap, fraudsters collect personal information about the consumer. This may be through deceptive emails (phishing), scam calls, or by taking information from websites and social media.

Fraudsters use this information to trick providers into believing they are the owner of the mobile number. They do this by exploiting the way providers verify the identity of the consumer.

## Potential consequences for consumers

Increasingly, consumers say they have suffered serious consequences after falling victim to this type of scam. The wide use of mobile numbers as an additional security check for consumers' most sensitive accounts (such as banking and email) means taking possession of a mobile number is a powerful instrument for fraud.

For instance, consumers report having thousands of dollars drained from their bank account because the bank uses consumers' mobile numbers to conduct a text-based "two-factor authentication" check. Other consumers report having their email inbox accessed because their mobile number is used for authentication or password recovery.

## Strengthening providers' identity verification procedures

In handling complaints, we look at the steps the mobile service provider took to verify the customer's identity before completing the SIM swap. While consumers expect their providers to keep their number and account secure, we recognise this is increasingly difficult in a connected world where many people have basic personal details publicly accessible online.

Over the past year, our systemics team identified a trend of complaints about providers who had a low bar for identity verification. For instance, we found instances where providers only required the consumer's full name, date of birth and the mobile number as proof of identity. We were particularly concerned to see some identity verifications were conducted solely through online chat.

The following summaries of recent systemic investigations illustrate our work with two providers in strengthening their identity verification procedures as a way of reducing fraudulent SIM swaps.

# Systemic investigation – GreenTel*

In May 2018, our systemics team told GreenTel we were interested in its account security procedures and how effective they were at preventing increasingly common types of fraud such as SIM swaps.

In the preceding six months, we identified complaints where a fraudster was allowed to take control of a GreenTel customer's mobile number after providing limited personal details. We told GreenTel that requiring only a person's full name, date of birth and service number may not be reasonable given the availability of this information in the public domain. While GreenTel cannot control how banks choose to use mobile numbers as a security measure, we thought this risk should be considered by GreenTel if it is to take reasonable steps to protect customers' personal information and account integrity.

During the systemic investigation, GreenTel acknowledged both GreenTel and the broader telecommunications industry must adapt as criminal activity adapts. GreenTel told us it had progressively been rolling out process changes, including prohibiting SIM swap requests over online chat and over the phone during evenings. Based on our feedback, GreenTel also implemented refresher training to its staff around privacy and deceptive behaviour.

Our systemics team worked with GreenTel, identifying further complaints where its new processes may have failed or where its staff had given customers incorrect information on the use of PIN numbers. GreenTel told us it had taken disciplinary action against staff members whose actions were not compliant.

Most importantly, GreenTel told us it will rollout and embed its own two-factor authentication process by the end of January 2019. This means customers wanting to perform a SIM swap (or other related transactions such as updating contact details) will be sent an SMS to their handset with a link directing them to a secure webpage where the transactions can be approved. If a customer is unable to receive an SMS on their phone, they would be directed to visit a GreenTel store to complete the transaction. In our initial systemic notification to GreenTel, we'd referred to a form of two-factor authentication as an example of good industry practice.

Our systemics team will continue to monitor complaints after rollout of GreenTel's two factor authentication procedure and hope to see a reduction in complaints about fraudulent SIM swaps.

The Telecommunications Industry Ombudsman also welcomes other initiatives GreenTel has been involved in to combat telecommunications fraud, such as the trial of biometric identification verification solutions and assisting the police in investigating fraud offences.

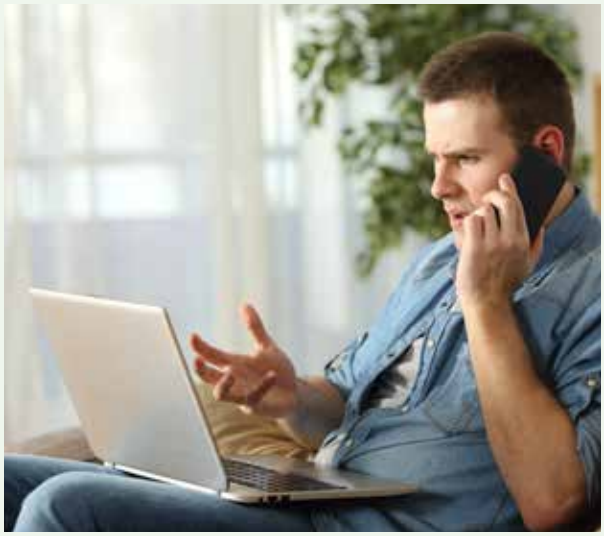
**Case study 1**

**Mr Smith's* phone and bank accounts are hacked**

In January 2018, Mr Smith lodged a complaint saying a fraudster had contacted GreenTel* on online chat and successfully had his mobile number transferred to another SIM card. He said the fraudster only had to state his name and date of birth to GreenTel. The fraudster was also able to change all of Mr Smith's contact details on his GreenTel account.

Mr Smith told us this had allowed the fraudster to hack his banking profile and drain his bank accounts of tens of thousands of dollars. He said the fraudster also ordered additional GreenTel devices on his account and he was left without a mobile service for days.

*Name of individuals, organisations and companies have been changed



## Systemic investigation – Blue Phones*

In October 2017, our systemics team began working with Blue Phones about its account security procedures.

We'd identified a number of complaints from consumers who said Blue Phones had allowed their account to be accessed by an unauthorised third party. We wanted to better understand how Blue Phones verified its customers' identities for various transactions over different platforms such as online, by telephone and in store.

Blue Phones told us it required customers to take enhanced authentication steps before they could make a transaction Blue Phones deemed to be "high risk". After our systemics team sought clarification about SIM swaps specifically, Blue Phones confirmed it deems SIM swaps to be high risk transactions. This meant a customer would need to provide an additional form of ID, usually a driver's licence. Blue Phones also introduced a further two-factor authentication step by sending customers one time PIN numbers by SMS for all high risk transactions.

While the Telecommunications Industry Ombudsman does occasionally receive complaints from consumers who find additional verification steps onerous, we think this inconvenience is outweighed by the benefit of reducing fraudsters' ability to impersonate consumers.

Blue Phones also told us it was continually seeking to strengthen its privacy and fraud-related controls. For instance, in March 2018, Blue Phones piloted new ID verification technology that would allow it to check the legitimacy of ID being used (for instance, the passport or driver's licence).

**Case study 2**

**Ms Chan* has $9000 taken out of her bank account**

In July 2017, Ms Chan complained to our office saying a fraudster had called Blue Phones* using her name and tried to take her mobile number. She said her mobile service was disconnected and $9,000 was taken out of her bank account.

*Name of individuals, organisations and companies have been changed

**Case study 3**

**Mrs Fuke* is asked for additional ID verification**

In July 2018, Mrs Fuke complained to our office and told us she contacted Blue Phones* to discuss upgrading her service to take up a bonus data promotion. While discussing the upgrade, the sales representative told her she would need a new SIM card for the upgrade to be complete.

During the discussions to process the upgrade, Mrs Fuke was required elsewhere, so she arranged a call back time to complete the transaction. She told us when the agent contacted her to continue the transaction, they asked her to supply a passport or licence number.

Because she refused to supply the additional personal details, Mrs Fuke told us Blue Phones would not complete the order. In response to her complaint, Blue Phones told Mrs Fuke it was asking for ID to make sure the product will be delivered to the right person and to avoid any fraudulent activity.

*Name of individuals, organisations and companies have been changed

## What consumers should do if their mobile number is stolen

If you find your service is suddenly disconnected or receive notification about a SIM swap you didn't authorise, you may be a victim of mobile number theft. We suggest you:

- Contact your bank or financial services provider immediately and explain that your mobile number has been taken. Ask them to check for any withdrawals or unusual transactions on your account.
- Contact your mobile service provider and ask them to get your number back.
- Contact IDCARE, Australia and New Zealand's national identity and cyber support service at www.idcare.org or call 1300 432 273.
- If theft has occurred, contact the police.

For unresolved complaints about financial institutions, contact the Australian Financial Complaints Authority at www.afca.org.au or via phone 1800 931 678.

If you have a complaint about how your mobile service provider dealt with a SIM swap, contact the Telecommunications Industry Ombudsman at www.tio.com.au or via phone on 1800 062 058.

## How consumers can protect against the theft of their mobile numbers

The more publicly available your personal information is, the more susceptible you are to mobile number theft. To protect yourself, we suggest you:

- Don't respond to emails asking for your bank account details, phone number and personal details.
- Don't respond to any caller who asks for access to your computer. Don't give them any passwords or other information. Hang up.
- Don't click on links in emails or text messages saying you have won a prize or have a message, particularly if you don't know the sender.
- Reduce disclosure of personal details such as full name, mobile number and full date of birth on social media, online dating websites or blogs. If you must enter these details, ensure they are hidden from public view.
- Lock your letterbox. Fraudsters can gain personal information about you by physically stealing your mail.

## Ways providers can strengthen identity verification procedures

Providers can reduce the theft of its customers' mobile numbers by strengthening their identity verification procedures. For instance, these measures have been adopted widely by providers:

- Allowing customers to set up PINs on their telco accounts.
- Enhancing the customer authentication steps before customers can make a transaction by requiring customers to provide an additional form of ID as well as full name, date of birth and mobile number.
- Introducing two-factor authentication by sending customers one time PIN numbers through SMS or email for all high risk transactions such as SIM swaps.

We welcome the industry's continued work towards consistently robust identity verification procedures. It is important to ensure these procedures keep up with evolving technological risks.

# The Telecommunications Industry Ombudsman

The Telecommunications Industry Ombudsman provides a free and independent dispute resolution service for residential consumers and small businesses who have an unresolved complaint about their phone or internet service in Australia.

## About

The Telecommunications Industry Ombudsman Ltd was established in 1993, and is a company limited by guarantee. *The Telecommunications (Consumer Protection and Service Standards) Act 1999* requires telecommunications providers to be members of the Telecommunications Industry Ombudsman and to comply with the decisions of the Ombudsman.

## Scope of service

Dispute resolution services include:

- Dealing with individual and systemic complaints
- Promoting fair and effective resolution of complaints.
- Providing information and analysis to community, government and members.

## Telecommunications service providers

Telecommunications service providers are businesses or individuals who are carriers or provide carriage services.

Carriers – persons who own a telecommunications network unit to supply carriage services to the public. The carrier must be licensed through the Australian Communications and Media Authority.

Carriage service providers (CSP) – those who supply standard telephone services, public mobile telecommunications services, or carriage services that enable end-users to access the internet, including carriage service intermediaries who arrange for the supply of such services.

## The telecommunications industry sector

The telecommunications industry regulators are the Australian Communications and Media Authority (ACMA) www.acma.gov.au and the Australian Competition and Consumer Commission (ACCC) www.accc.gov.au.

Government and the regulators set policy and regulations for the telecommunications sector.

Communications Alliance is the peak body for the Australian communications industry www.commsalliance.com.au.

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communications consumer organisation representing individuals, small businesses and not-for-profit groups as consumers of communications products and services www.accan.org.au.

# Systemic Issues

The Telecommunications Industry Ombudsman's systemic investigation power allows the organisation to identify issues with the telecommunications industry's regular systems, processes or practices and issues that may cause detriment to residential consumers and small businesses. By investigating issues, raising awareness and working with telecommunications providers to make recommended changes, the Telecommunications Industry Ombudsman drives improvements in the delivery of telecommunications services and better outcomes for consumers and the telecommunications industry.

In financial year 2017/18 the Telecommunications Industry Ombudsman dealt with 212,786 enquiries and complaints from residential consumers and small businesses. As a high volume complaint resolution service, the Telecommunications Industry Ombudsman is well placed to identify and report on systemic issues residential consumers and small businesses face with their phone and internet services.

The Telecommunications Industry Ombudsman is committed to providing reporting on systemic insights to improve industry practices and reduce consumer complaints. Systemic reports are intended to raise awareness of industry-wide issues and promote ways to improve services.

The Telecommunications Industry Ombudsman considered and investigated 80 possible systemic issues. It notified providers about 52 possible systemic issues, and 30 systemic matters resulted in the provider agreeing to or making changes to its system, process or practice.

19 different providers implemented changes to address the systemic issue raised by the Telecommunications Industry Ombudsman. The types of changes implemented by providers included:

- Improving procedures in the areas of network coverage troubleshooting, credit management and account holder verification
- Correcting a customer service hotline error which had potential privacy consequences
- Monitoring and providing staff training on misleading sales conduct, and
- Updating standard form consumer contracts to make terms fairer.

This example illustrates how the Telecommunications Industry Ombudsman undertakes industry-wide systemic issues investigations. After noticing a pattern of telephone number loss during National Broadband Network migration, we wrote to 23 retail NBN service providers to better understand the circumstances behind the complaints and what providers believe to be the underlying causes. The results of this survey allowed the Telecommunications Industry Ombudsman to prepare a systemic insights paper with recommendations for retail service providers to reduce the incidence of number loss. The paper was published in July 2018.

# How to make a complaint

1. Residential consumers and small businesses should first try to resolve their complaint with their phone or internet provider.

2. If the complaint remains unresolved, the residential consumer or small business can contact the Telecommunications Industry Ombudsman by visiting www.tio.com.au or calling 1800 062 058.

3. The Telecommunications Industry Ombudsman determines whether it can deal with the complaint.

4. The Telecommunications Industry Ombudsman works with the parties to resolve the complaint.

5. The Ombudsman has the power to decide the resolution of the complaint.

# Contact us

| | |
|---|---|
| By Phone | 1800 062 058* |
| Online | www.tio.com.au |
| By fax | 1800 630 614 |
| By post | PO Box 276 Collins St West VIC 8007 |

If you need an interpreter, please contact us through the Translator and Interpreter Service (TIS): 131 450

The Telecommunications Industry Ombudsman's Privacy Policy explains how we collect, use and handle your personal information. Ask us for a copy or find it at www.tio.com.au/privacy

*Free from landlines. If you are calling from a mobile, you can ask us to call you back.