Defending phone and internet accounts from fraudsters

Systemic Investigation Report, November 2021

Telecommunications Industry Ombudsman

We investigated complaints about fraudulent access of telco accounts

Every year, we receive complaints from consumers who fell victim to fraud after their telco account was accessed without their authorisation. We identified and monitored trends in these complaints. We conducted systemic investigations into how telecommunications providers secure customer accounts from fraudsters, as well as consumers' own responses to fraudulent activity.

We received complaints from consumers who were victims of fraudulent account access

With so many consumers working from home during the COVID-19 pandemic, phone and internet fraud has become increasingly prominent. Australians lose millions of dollars annually from fraud and scams, often facilitated through phone or internet services.

In the last financial year, we received over 500 complaints from consumers who said they had fallen victim to telco related fraud.

We identified a trend of complaints from consumers who reported falling victim to fraudulent account access.

When we talk about *fraudulent account access*, we mean any malicious activity by a third party used to gain access to a consumer's phone or internet account and act without their authorisation.

Consumers commonly reported that after a fraudster was able to gain access to their telco account, the fraudster:

- ordered new telco services and devices (often mobile handsets) on their account
- used their telco service to make expensive international calls, or
- stole their mobile number by transferring it to a new SIM card in the fraudster's possession. In many cases, the stolen mobile number was used to gain access to their bank account or other accounts (such as email or MyGov accounts).

Consumers experienced financial and non-financial loss

Consumers who had fraudsters purchase services and devices on their accounts told us they were often left with a bill for hundreds or thousands of dollars. These large debts sometimes resulted in their accounts being suspended or other services being disconnected.

Consumers who lost control of their mobile number had money stolen from their bank accounts. They also reported being unable to contact family and friends.

For small businesses, losing access to a customer-facing mobile number can result in lost revenue and trade.

While many complaints resulted in financial loss, some consumers also reported risks to their safety.

Fraudulent account access can reveal consumers' personal information. For instance, a consumer's place of residence may be revealed to an ex-partner or estranged relative which can risk their personal safety.

Fraudulent account access can take time to resolve and cause significant inconvenience for consumers

Consumers whose telco account had been accessed fraudulently reported spending many hours resolving issues with their telco provider, as well as other relevant organisations such as police, road authorities and banks. Some consumers reported their account was compromised more than once.

Some consumers said they only realised they were a victim of fraud when they applied for a home loan, which was rejected because they had a default recorded on their credit file. Fraudsters may take steps to ensure all correspondence is sent to an address they control, meaning bills or other account notices never reach the consumer.

Fraudulent account access can also be costly to providers

Telecommunications providers are also adversely affected by fraudulent account access. Providers have told us they allocate significant time and resources to investigating and resolving fraud complaints.

Some investigations revealed fraudsters were able to gain access to a consumer's account because providers did not conduct proper identity checks or incorrect advice was given to consumers about how to secure their telco account.

Resolving the consumers' complaints can require the provider to waive thousands of dollars in disputed charges.

Where the complaint involves a breach of privacy leading to risks to a consumer's personal safety, a provider may need to offer the consumer compensation.

Repeated incidents and poor account security practices may impact customer relationships and cause longer term reputational damage.

The telecommunications industry and the ACMA are responding to the challenges of fraudulent account access

We are pleased to see the telecommunications industry and the Australian Communications and Media Authority (ACMA) have taken steps to combat fraudulent account access.

These steps show they have recognised stronger identity verification processes allow providers to better protect their customers' accounts.

Such processes also assist providers' compliance with their privacy obligations. Providers have an obligation to take reasonable steps to protect customer personal information from misuse, interference, loss, unauthorised access, modification, or disclosure.[1]

In April 2020, the ACMA introduced an industry standard[2] that requires providers to add extra identity verification when transferring customers' phone numbers from one provider to another. In November 2021, the ACMA proposed new rules which would require extra identity checks for other high risk transactions.

Over the past year, peak industry body Communications Alliance has also been working on improving the framework to authenticate the identity of customers making transactions involving their telco service.[3]

While these initiatives help to address some of the issues we found, providers and consumers must remain vigilant about the constantly evolving behaviour of fraudsters.

1. *Privacy Act 1988* (Cth) sch 1 ('Australian Privacy Principles' APP 11).
2. Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.
3. Communications Alliance Media Release dated 13 October 2021.

Our key findings about fraudulent account access

Over the last year, we conducted four systemic investigations into how telecommunications providers secure customer accounts from fraudsters, as well as consumers' own responses to fraudulent activity.

This report shares the key findings from our systemic investigations and complaints we received. We found there were four common themes which contribute to fraudsters gaining access to telco accounts.

We explore what consumers have told us about their experiences with fraudulent account access, and highlight improvements made by providers to combat fraudulent account access.

We also offer tips to providers and consumers to help safeguard phone and internet accounts from fraudsters.

OUR KEY FINDINGS

1. Weak security processes can help fraudsters gain access to telco accounts
2. Fraudsters can exploit delayed responses by providers to breaches of account security
3. Consumers can fall victim to fraud if they don't know what to look out for
4. Fraudsters' tactics and methods are constantly evolving

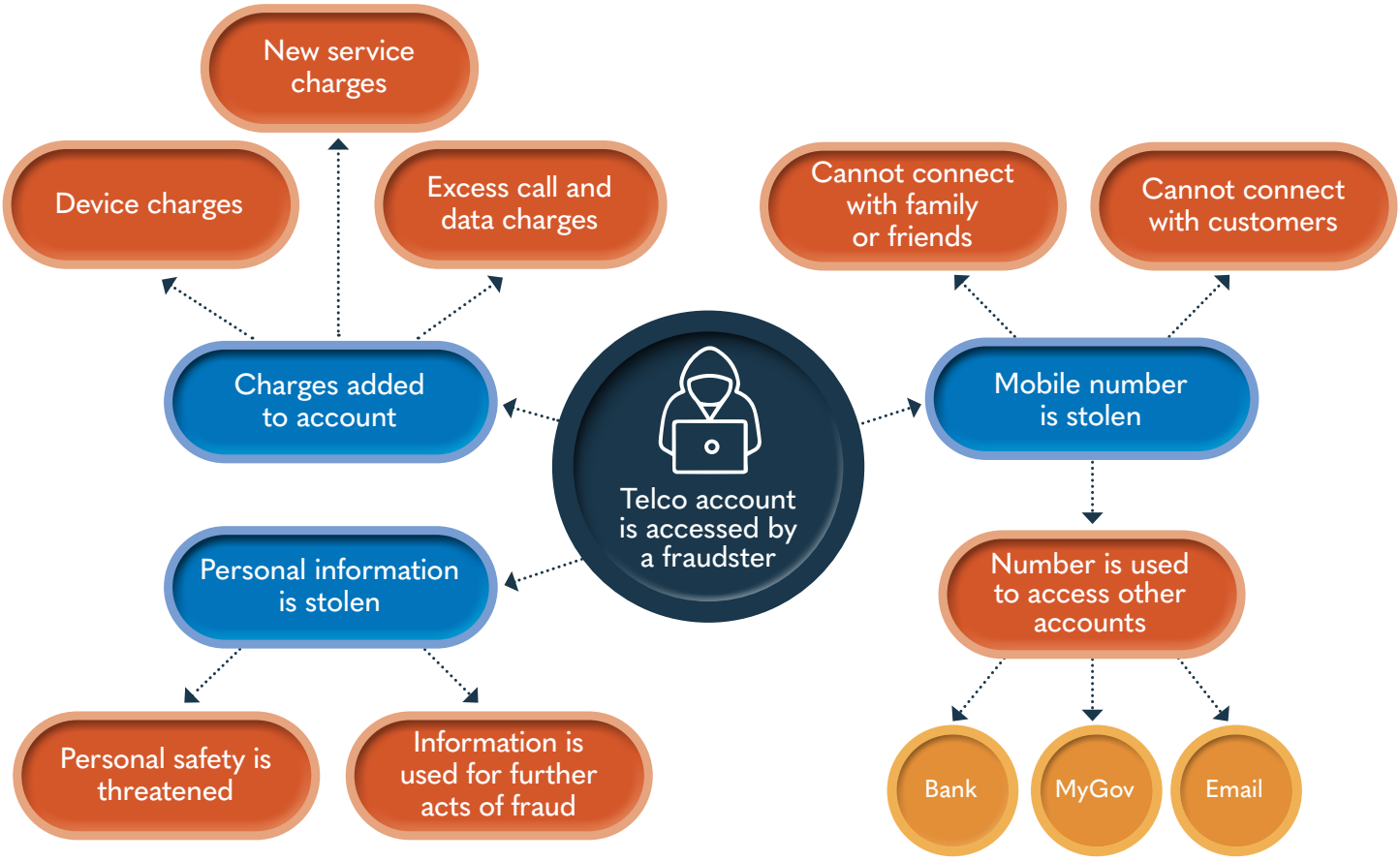
In a picture: The importance of securing telco accounts

A consumer's telco account houses a large amount of personal information (especially if linked to an email address hosted by the same provider). Accessing a telco account allows a fraudster to control a consumer's mobile phone number or acquire new services and equipment. This makes a telco account a valuable target for fraudsters looking to obtain devices or collect personal information about a consumer.

A consumer's mobile phone number is a valuable target for fraudsters. This is because mobile phone numbers often play a vital security role when logging into or resetting passwords for other important accounts, including banking and finance accounts, social media accounts, web and email accounts, and government services, including MyGov.

If a fraudster gains access to a consumer's mobile phone number, they may be able to use it to reset passwords for these accounts, locking the consumer out and allowing the fraudster to take control.

How fraudulent account access can impact consumers



Finding 1: Weak security processes can help fraudsters gain access to telco accounts

Weak provider account security processes can allow fraudsters to gain access to personal information and conduct malicious activity.

A low bar to identity verification can be exploited by fraudsters

Where a provider only requires minimal or basic information about a consumer to verify their identity and give them account access, this can be exploited by fraudsters.

For example, our systemic investigations found fraudsters were able to access telco accounts by giving the provider a consumer's mobile number and some basic information about the consumer.

The basic information is sometimes already known by the fraudster or may be easily found in the public domain or through social media.

Providers do not always apply security measures consistently

While we found some providers had robust security measures in place, their staff members did not always follow them or apply them consistently.

One provider gave consumers the option of using robust multi-factor authentication, such as one-time passwords or an authenticator app.

However, this provider also offered other security measures which were not supported by its systems, such as passwords and PINs. This meant staff did not always ask for the password or PIN when someone wanted to access the account. A consumer may believe their account is secure when it is not.

During our investigation, the provider agreed to provide feedback and training to staff to ensure they provided the correct advice about available security options.

Some account security processes had key gaps

We found some account security processes used by providers had key gaps, which could leave consumers vulnerable.

In one systemic investigation, there was a gap in the provider's process for checking identity document information. During our investigation, the provider agreed to use a government database to verify details of identity document information.

In another systemic investigation, we found a gap in the provider's process when a consumer could not pass its usual security check. The alternative security check offered by the provider was less stringent than its usual security check. The provider agreed that, in most cases, it would direct consumers to confirm their identity in store where the consumer could not pass its usual security check.

Case study

Delaney deals with the flow-on effects of an unauthorised SIM swap

Delaney's mobile service stopped working. When she called her provider, Mode Telco, it told her she had approved a SIM swap, which she hadn't. She visited her local store and had her mobile number returned to her within the hour.

During this hour, the fraudster accessed Delaney's email and multiple cryptocurrency accounts, and used her mobile number to obtain codes to reset her passwords. Over the next three weeks, further attempts were made by fraudsters to access Delaney's accounts.

When we asked Mode Telco to investigate Delaney's complaint, it found a fraudster had impersonated a Mode Telco staff member to gain access to Delaney's account and process a SIM swap. Mode Telco said this fraudster was able to provide enough information and credentials to trick Mode Telco's staff into believing the fraudster was acting under Delaney's instructions.

Delaney said after her accounts had been compromised, she spent hours contacting various agencies, including her bank, superannuation fund, Medicare, and her internet provider. She also had to replace her identity documents and credit cards.

Mode Telco offered to cover the cost of replacing Delaney's identity documents and any remaining charges on Delaney's account so she could transfer her service to another provider.

*Names of all parties have been changed.

Case study

Ivka's ex-girlfriend accesses her account to harass her

Ivka had an abusive ex-girlfriend and contacted ScoopTel to discuss extra protections for her account. ScoopTel told Ivka it would add a four-digit PIN to her account, which she would have to repeat whenever she called ScoopTel.

Over the next couple of months, Ivka discovered her ex-girlfriend had been able to access her account and changed her email address to one her ex-girlfriend controlled. Her ex-girlfriend was then able to view Ivka's telephone bills and see who she had been calling. Her ex-girlfriend was also able to find out the phone numbers of Ivka's friends and make nuisance calls to them.

When we investigated Ivka's complaint, ScoopTel said it gave incorrect advice when it told Ivka the four-digit PIN could stop unauthorised access. ScoopTel said it only needed a caller to provide basic information before allowing the caller to access the account.

ScoopTel offered to let Ivka transfer to another provider. Ivka agreed to stay with ScoopTel but accepted compensation.

*Names of all parties have been changed.

Finding 2: Fraudsters can exploit delayed responses by providers to breaches of account security

When a provider does not respond quickly to an account security breach, the fraudster can exploit the delay to take control of a consumer's account.

Some providers do not always act quickly when notified of a security breach

When a consumer reports a potential account security breach to their provider, if the provider delays responding, the fraudster can use this time to access the consumer's personal information.

Consumers experienced delays when:

- their provider kept them on hold for long periods of time when they tried to report a security breach
- they could not contact their provider to report a security breach outside of the provider's regular business hours
- they were not able to get through to their provider at all
- frontline staff did not know the process to follow when notified of potential fraud or gave them inconsistent advice, such as to wait for a response or fill out a statutory declaration form
- frontline staff did not block fraudulent activity on an account as promised
- their account was accessed multiple times by a fraudster even after reporting the security breach.

A delayed response from a provider can make the impact of a security breach worse

When providers are slow to secure a consumer's account, this can give fraudsters additional time to conduct fraudulent activity using the consumers account. This might include:

- ordering expensive handset devices and leaving the consumer with the cost of the plans and devices
- using the consumer's service and personal information to access their bank account and withdraw funds
- using the consumer's service and personal information to access their government agency accounts and email accounts.

This can expose affected consumers to considerable financial and non-financial loss. Where a breach of privacy has occurred, providers may have to pay significant amounts of compensation to settle a consumer's complaint - a cost that could have been avoided had the provider acted more quickly.

Some providers are putting more control in the hands of consumers

We have seen some providers make improvements to reduce response delay.

During one investigation, a provider said it would implement a way for consumers to lock down their accounts, preventing further transactions from taking place. An option like this could improve response times for consumers who realise their personal information or account credentials have been stolen.

Case study

Multiple fraudulent services were taken out on Mohammed's account

Mohammed received a bill with charges for a mobile service he did not recognise. After trying to call Brite Talk and being on hold for several hours, he went to a Brite Talk store to dispute the charges.

The store staff told Mohammed the charges were incorrect and to simply continue paying his normal monthly charges. Three months later, Mohammed received a demand letter from debt collectors, saying he owed thousands of dollars.

Mohammed went back to the Brite Talk store, as he still could not reach Brite Talk by phone. He found out that a fraudster had ordered services using his account and had them delivered to an unfamiliar address in a different state. The store staff said debt collection would be put on hold, and agreed to put an additional password on his account.

Within a few months, more unfamiliar services showed up on Mohammed's account. This time, a Brite Talk employee contacted him and agreed not to approve any more purchases unless he went to a store with photo ID.

Brite Talk failed to implement this additional security measure, and fraudsters ordered more services using Mohammed's account, leaving him with thousands of dollars in charges. After months of disputing the charges, Mohammed complained to us. Brite Talk agreed to waive all the charges, acknowledging it should have intervened sooner.

*Names of all parties have been changed.

Case study

Xing's provider ReliableNet did not act after multiple reports of a security breach

Xing received a text message saying a SIM swap had occurred and to call ReliableNet back if Xing had not authorised it. At the time, Xing could not report the fraud, because it was outside ReliableNet's office hours.

The next morning at 8am, Xing called ReliableNet. ReliableNet said to wait to be contacted in three to five business days. That same day, Xing received another text message saying a new SIM had been ordered on their account. Their number stopped working.

Xing called ReliableNet a second time. This time, ReliableNet told Xing to complete a statutory declaration, which Xing did immediately.

By 2pm the same day, a fraudster gained access to Xing's email account and changed Xing's password, resulting in Xing being locked out of their email. Xing called ReliableNet for a third time.

This time they asked for a four-digit PIN to be placed on the account for extra security, and a new mobile number.

When we investigated Xing's complaint, we found the fraudster was able to access Xing's account after a PIN had been added because ReliableNet failed to ask for the PIN.

ReliableNet agreed to transfer Xing's number to a different provider, waived all outstanding handset repayment charges, and offered $1,500 in compensation for the privacy breach.

ReliableNet also asked for permission to use Xing's story as a training model for its staff.

*Names of all parties have been changed.

Finding 3: Consumers can fall victim to fraud if they don't know what to look out for

Consumers can fall victim to fraud if they do not know what to look out for and how to protect their personal information from misuse. Consumers can educate themselves on common types of fraud, protect their passwords, and ask their provider what extra security measures are available.

Fraud often involves impersonation

Often fraudsters will impersonate organisations such as the Australian Taxation Office, banks, public utilities, and debt collectors. Sometimes fraudsters will also impersonate telco providers.

Fraudsters may use this technique to obtain personal information about consumers, which can then be used to conduct fraudulent activity. Or they might trick consumers into providing account passwords, PINs, or one-time codes. Sometimes we have seen fraudsters trick consumers into agreeing to have new mobile phones delivered to the fraudsters' address.

Common methods fraudsters will use to trick a consumer include:

- offering consumers incentives for providing their personal information (such as a discount or free phone)
- pressuring the consumer with a time-sensitive offer.

Some passwords can be easy for fraudsters to guess

Sometimes fraudsters can gain access to a consumer's account by guessing their account password or PIN.

Fraudsters may attempt to access a consumer's account by trying weak or common passwords. Alternatively, they may be able to guess passwords (or the answers to "security questions") by collecting information about a consumer from social media websites.

Consumers are not always aware of what security measures are available

Some consumers are unaware of extra security measures that can be added to a telco account.

Providers are increasingly offering additional options for consumers to secure their accounts, such as multi-factor authentication.

This provides an additional layer of security and limits the damage a fraudster can do to a consumer's account. Even if a fraudster steals a consumer's password, they may not be able to access the account, make changes, or place orders for goods and services.

WHAT IS MULTI-FACTOR AUTHENTICATION?

Multi-factor authentication usually involves sending a one-time code to a consumer's mobile before processing an order or authorising an account change.

If the consumer cannot receive the one-time code, some providers require the consumer to go to a store and present valid photo ID.

Some providers will offer alternate methods to consumers who cannot reasonably go to a store, due to a disability, distance, or technological restraints.

Case study

Sam falls prey to a COVID-19 deception

Sam received a call from someone claiming to be from his telco, Bluestone Connect. The person offered to apply a discount to all Sam's services as a special COVID-19 assistance measure.

The person who called Sam knew all of his account details, so Sam was convinced they were calling from Bluestone Connect. The person asked Sam to tell them the confirmation codes he had received by SMS to provide the discount, which Sam did.

Sam received a flood of emails thanking him for upgrading his phone plan, followed by a fraud alert email from Bluestone Connect. He then received a call from Bluestone Connect, checking whether he had upgraded his services and ordered new phones. Sam said he had not ordered anything.

Sam later found out from Bluestone Connect that a fraudster had used his account to order multiple new mobile handsets. He also made a statutory declaration and reported the fraud at a police station.

Sam was charged cancellation fees for the cancelled mobile services and handsets. He disputed the charges with Bluestone Connect, but Bluestone Connect stopped responding to his requests for updates. After Sam complained to us, Bluestone Connect eventually agreed to refund the charges.

*Names of all parties have been changed.

Case study

Anastasia unknowingly gave her personal information to fraudsters

A fraudster contacted Anastasia pretending to be from her provider, Token Fones. The fraudster offered to upgrade Anastasia's plan, and asked Anastasia for account and identity information. Anastasia was keen to get the plan upgrade, so she provided the information.

Anastasia later realised that the person she spoke to was a fraudster and found out that changes had been made to her Token Fones account without her knowledge. The fraudster had changed her home and email addresses to ones that Anastasia did not recognise.

Later, Anastasia received a text message from Token Fones, which included an order confirmation. Anastasia immediately contacted Token Fones, who said someone had ordered a new mobile service using her account. Anastasia also realised that her home and email addresses had been changed again.

Token Fones cancelled the mobile service, but charged thousands of dollars to Anastasia's account. After we investigated Anastasia's complaint, Token Fones eventually agreed to waive the charges.

*Names of all parties have been changed.

Finding 4: Fraudsters' tactics and methods are constantly evolving

Fraudsters are continually changing their methods and tactics to find gaps in providers' security measures. Providers who act proactively may be able to prevent new and evolving account security breaches.

Fraudsters can exploit providers' legitimate security measures

Some fraudsters may exploit, mimic or adopt providers' messaging or communication styles so messages appear as if they are coming from a consumer's provider.

A common tactic can involve a fraudster tricking a consumer into providing the one-time code sent by their provider. The fraudster then uses this one-time code to order services in the consumer's name.

Providers may reduce complaints by taking steps to keep up with fraudsters

In a number of systemic investigations, we've seen providers improve their approach to combating fraud, including attacking fraud from multiple angles.

It has been encouraging to see some providers making proactive improvements to account security and customer authentication processes. For example, we have seen providers increase their use of robust measures like multi-factor authentication and government document verification services.

We have also seen providers update the information they send to consumers in response to common types of fraud, both on their websites, when confirming orders, or in one-time code messages.

In one systemic investigation, a provider introduced clearer SMS customer communications about the use of one-time codes and how to stop an unauthorised action. These SMS communications clearly stated that the provider would never ask for a one-time code over the phone - suggesting that anyone doing this may be a fraudster.

This kind of messaging is important because it provides a warning at the point the consumer may be interacting with a fraudster.

More broadly, providers have recognised they cannot tackle fraudsters' evolving tactics alone.

Aside from referring fraud cases to law enforcement bodies for investigation, we have also seen providers come together as an industry to try and combat fraud. Over the past year, peak industry body Communications Alliance has been working on improving the framework to authenticate the identity of customers making transactions involving their telco service.

Providers who have approached fraud from multiple angles have reduced the number of complaints received by our office about fraud. Actions these providers have taken include advances in technology, stronger communications with consumers, and more stringent requirements for the approval of high risk transactions.

Systemic investigation case study

PinkTel adapts its account security processes to combat fraudsters

In April 2021, we notified PinkTel about a possible systemic issue with the way fraudsters were exploiting its legitimate security measures. PinkTel's customers were being targeted in a series of calls, in which fraudsters were using sophisticated tactics to circumvent PinkTel's security measures to order handsets in customers' names.

During our investigation, we found fraudsters would call a PinkTel customer and identify themselves as a respresentative of PinkTel. The fraudster would offer the customer a free mobile handset for being a loyal customer.

The fraudster would then exploit PinkTel's security measures using the customer's mobile number. They were able to get PinkTel to send a legitimate SMS with a one-time code to the customer. The fraudster would ask the customer to read out the one-time code to confirm the free handset. Once the customer had provided the one-time code, the fraudster was able to order handsets in the customer's name, but have them delivered to an address of the fraudster's choosing.

In many of the complaints we investigated, the fraudster already knew detailed information about the customer's account, which convinced the customer the call was legitimate.

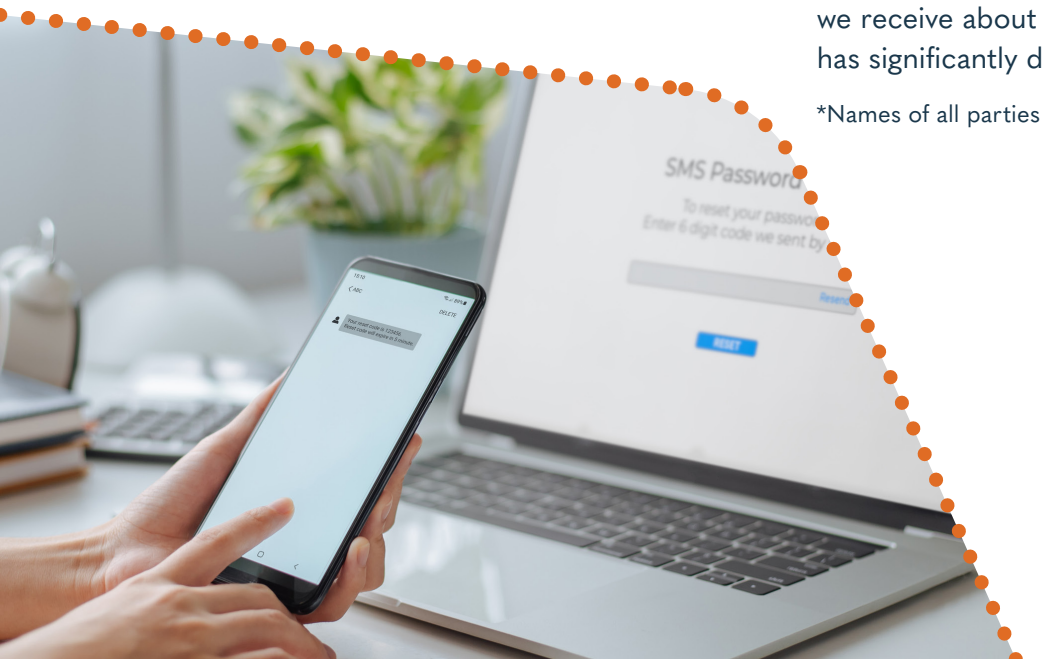
We worked with PinkTel to combat fraudsters' tactics to trick customers into believing they were dealing with a real PinkTel representative.

PinkTel conducted a comprehensive review of its account security measures and made improvements to its account security process, including:

- amending the wording of SMSs, specifically noting PinkTel would never call and ask a customer for confirmation of a security SMS
- ensuring customers who contact PinkTel are advised that PinkTel would never call a customer to ask for their security or login information
- sending alert SMSs to customers when an attempt is made to change the customer's delivery address
- requiring customers to directly confirm orders for new handsets before processing the order
- removing customers' personal details in emails confirming orders to prevent any further personal information from being stolen by a fraudster
- publishing information on its website warning customers about potential fraud.

Since making these changes to its account security processes, the number of complaints we receive about fraud from PinkTel customers has significantly decreased.

*Names of all parties have been changed.



Tips for phone and internet providers

Telecommunications Industry Ombudsman

Tips for providers to help protect consumers against fraudsters

Ensure account security processes are strong for high risk transactions

- Providers should ensure account security processes keep up with industry codes and regulations as they develop.
- Providers should conduct additional security checks for high risk transactions, which do not solely rely on easily obtainable information about the consumer.

  High risk transactions include:
  - requesting a SIM Swap
  - porting a phone number to another provider
  - adding an Authorised Representative to an account
  - changing contact details
  - ordering new products or services.
- Providers should always verify the legitimacy of identity document information.

Ensure consumers can quickly and easily report a potential security breach

Providers should consider:

- reducing hold times for fraud complaints
- having a 24/7 hotline or extended phone hours to report fraud
- a direct telephone or online messaging service for consumers seeking to report fraud
- allowing consumers to block any activity on their account, unless the activity is done instore with photo ID
- allowing staff to add a 'fraud' flag to the front of a consumer's account, rather than relying on customer interaction notes (where they can be missed).

Regularly review and update account security measures

- Providers should regularly review their fraud complaints, particularly call recordings, to identify potential security gaps or areas of improvement.
- Providers should review their SMSs and emails containing one-time codes to ensure they contain clear instructions for consumers to report a fraud.
- Staff should be well-trained in responding to a consumer's report of a potential security breach, including advising consumers on how to secure their account.

Educate consumers about ways to secure their account

- Providers should regularly inform consumers about how they will normally contact them and the information they will ask a consumer to provide.
- Providers should publish information about fraud, their security measures, and links to relevant sources (ScamWatch, IDCare, the police) on their website and distribute via email, post, or social media.

Tips for phone and internet consumers

Telecommunications Industry Ombudsman

Tips to help consumers protect their account from fraudsters

Make your phone or internet account as secure as possible

- **Use strong passwords**. Never use the same password for multiple accounts. Consider using password management software instead of storing them in text.
- **Ask your provider about the availability of extra security.** One example is Multi-Factor Authentication.

Limit the amount of personal information available in the public domain

- **Put your social media on private**, so personal information about you cannot be viewed by the public.
- **Lock your mailbox** to reduce the chances of bills or other letters containing your personal information being stolen.

Make sure you're really speaking with your provider

- **If someone calls you offering you a deal that seems too good to be true**, consider ending the call, looking up your provider's phone number, and calling directly to enquire about the deal.
- **Familiarise yourself with how your provider normally communicates with you**, so you can know what to look out for.
  - Sometimes SMSs and emails from fraudsters may have spelling and grammar errors, unfamiliar links, or strange formatting.
  - Other times, they may look genuine and even include company logos, but may ask for information that the real company would not ask for.
- **If you're unsure whether you are speaking to your provider, hang up and contact your provider directly.** For example, most providers do not call consumers to ask for one-time codes that have been sent to the consumer.

Report any strange activity to your provider immediately

- **If your provider sends you a notification saying you have changed your account details or made a new order, and you did not authorise any changes,** this could mean someone recently attempted to fraudulently access your account.
- Contact your provider as soon as possible.

What to do if you think you've fallen victim to fraudulent account access

- Report the fraud to your local police, IDCare, and your provider.
- If money has been taken from your bank account, contact your bank.
- If products or services have been added to your phone or internet account, contact your provider.
- Further information about hacking, identity theft, phishing, and remote access scams can be found at the ACCC's ScamWatch (www.scamwatch.gov.au).

When you can complain to us

We can handle complaints about your phone or internet provider, where your telco account has been accessed fraudulently and you cannot resolve the issue with your provider.

We cannot handle complaints about fraudsters or scammers and their behaviour. However, you can report their behaviour to ScamWatch or the police.

tio.com.au
1800 062 058 (free call)

Contact us

The Telecommunications Industry Ombudsman is a free and independent dispute resolution service for people and small businesses who have an unresolved complaint with their phone or internet service.

You can complain through our website at **www.tio.com.au** or by calling **1800 062 058**.

You can post a letter to **PO Box 276, Collins Street West, VIC 8007** or fax it to **1800 630 614**.

If you need to use a language other than English, call the Translating and Interpreting Service on 134 450 and they will help you speak with us. They are a free service.

Calls to the above numbers on mobile phones may incur charges.

Getting someone to help you

You can also ask someone else to complain for you or your business, such as a friend, family member, or financial counsellor. Ask for our authorisation forms over the phone or find them on our website.

Telecommunications Industry Ombudsman