

**COMMUNICATIONS
ALLIANCE LTD**



INDUSTRY GUIDELINE

G660:2018

**ASSISTING CUSTOMERS EXPERIENCING DOMESTIC
AND FAMILY VIOLENCE**

G660:2018 Assisting Customers Experiencing Domestic and Family Violence Industry Guideline

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1. Despite anything contained in this Guideline:
 - (a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct, indirect or consequential loss, damage, claim, or liability any person may incur as a result of any:
 - (i) reliance on or compliance with this Guideline;
 - (ii) inaccuracy or inappropriateness of this Guideline; or
 - (iii) inconsistency of this Guideline with any law, Industry Code or Industry Guideline; and
 - (b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Guideline.
2. For avoidance of doubt:
 - (a) You must not rely on the information in this document as an alternative to legal advice from your solicitor or other professional legal services provider.
 - (b) You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this document.
3. These disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

© Communications Alliance Ltd 2018

This document is copyright and must not be used except as permitted below or under the Copyright Act 1968. You may reproduce and publish this document in whole or in part for your or your organisation's own personal or internal compliance, educational or non-commercial purposes. You must not alter or amend this document in any way. You must not reproduce or publish this document for commercial gain without the prior written consent of Communications Alliance. Organisations wishing to reproduce or publish this document for commercial gain (i.e. for distribution to subscribers to an information service) should apply to Communications Alliance by contacting the Communications Alliance Commercial Manager at info@commsalliance.com.au.

VERSION HISTORY

This document constitutes: **Version 1 of Industry Guideline G666:2018**

Date	Version	Comments/Changes
22/10/2018	1	First release

TABLE OF CONTENTS

INTRODUCTORY STATEMENT	3
Background	3
Development of this Guideline	4
1 GENERAL	5
1.1 Related Documents	5
1.2 Objective and Scope of this Guideline	5
1.3 Reading this Guideline	6
1.4 Language	6
1.5 Guideline Review	6
2 CONCEPTS AND BACKGROUND	7
2.1 What is Domestic and Family Violence?	7
2.2 Domestic and Family Violence and Telecommunications	7
2.3 Contracts, Customer Rights, and Coercion	9
2.4 Identifying Domestic and Family Violence	10
3 INITIAL CONSIDERATIONS	12
3.1 The customer knows best	12
3.2 Referring customers to Specialist Domestic and Family Violence Support Services	12
3.3 Communicating Information to customers	12
3.4 First Steps	13
4 STAFF AND TRAINING	14
4.1 Staff structure	14
4.2 Choosing a training provider	15
4.3 Business-wide training	15
4.4 Front-line staff training	15
4.5 Specialised staff training	16
4.6 Internal staff support	17
5 CUSTOMER ACCESS TO ASSISTANCE	18
5.1 Contacting the Provider	18
5.2 Authorised Representatives and Advocates	19
5.3 Dedicated Staff	19
5.4 Communicating in a Supportive and Safe Way	20
6 CUSTOMER ACCOUNTS: PRIVACY AND SAFETY	22
6.1 Account verification	22
6.2 Account information	22
7 ECONOMIC ABUSE AND FINANCIAL HARDSHIP	23
7.1 Financial Hardship	23
7.2 Authorised Users and Sharing of Accounts	24

8	TECHNOLOGY FACILITATED ABUSE	25
8.1	Location and Privacy on Devices	25
8.2	Preventing or Stopping Harassment	25
8.3	Collecting evidence of technology facilitated abuse	26
9	PROCESS FOR KEEPING A MOBILE NUMBER	27
9.1	Standard Forms of Agreement	27
9.2	Process of separating a number	28
APPENDIX 1: ADDITIONAL RESOURCES		32
APPENDIX 2: MOBILE SAFETY FACT SHEET TEMPLATE		33
APPENDIX 3: TRAINING RESOURCES		35
APPENDIX 4: REFERRAL RESOURCES		36

INTRODUCTORY STATEMENT

In Australia one woman is killed every week by a current or former partner, and one in four children are exposed to domestic violence.¹ Domestic and family violence is so prevalent in Australia that, during their lifetime, most Australians will either experience it directly or know someone who has. Domestic and family violence can include emotional, sexual, and financial abuse as well as physical violence.

Customers and staff of telecommunications providers will be affected by domestic and family violence, whether as a victim/survivor, a perpetrator, or by having family or friends who have experienced it. In some cases, this will impact on customers' services and contracts as well. Australians are increasingly relying on telecommunications products and services in their day-to-day lives, but these products and contracts can also be used to compound abuse.

Telecommunications providers have a unique opportunity to support people impacted by domestic and family violence. Appropriate processes can lead to better outcomes for customers and staff.

Providers, both big and small, have come together with experts from community organisations to discuss how best to support customers experiencing domestic and family violence, and how to provide information and education across the industry.

Background

In March 2016, the Royal Commission handed down its report that included a recommendation for changes the telecommunications industry could make to better understand and address domestic and family violence.

Recommendation 108

The Victorian Government, through the Council of Australian Governments, encourage the Commonwealth Government [within 12 months] to:

- amend the National Credit Code to include family violence as a ground for financial hardship and develop an awareness campaign to ensure that both consumers and credit providers are aware of their rights and responsibilities
- work with the Australian Communications and Media Authority and its related representative bodies and associations to amend the Telecommunications Consumer Protections Code to:
 - list minimum eligibility criteria for access to hardship programs
 - make family violence an express eligibility criterion
 - incorporate a requirement for specific policies for customers experiencing family violence to clarify consent requirements for payment plans when an account is jointly held
 - include grounds for splitting jointly held debt and removing an account holder's name if family violence has occurred.

¹ Over 12 months on average. White Ribbon Australia 2014.

<https://www.whiteribbon.org.au/understand-domestic-violence/facts-violence-women/domestic-violence-statistics/>

Since the Royal Commission's report, the telecommunications industry has undertaken a number of joint activities to support those who have experienced domestic and family violence, in addition to the programs and assistance offered by individual providers.

Telecommunications Consumer Protection Code

In June 2017 Communications Alliance's Industry Consumer Advisory Groups (ICAG) voted to vary the Telecommunications Consumer Protection Code (TCP Code) in line with the Royal Commission's recommendation. The variation expressly provides that family or domestic violence is a criterion for access to Financial Hardship assistance from service providers and encourages providers to consider the unique circumstances of those impacted by domestic and family violence in developing flexible repayment options. The TCP Code variation was registered by the ACMA in August 2017.

The TCP Code has also undergone a full revision (*anticipated publication at the end of 2018.*) The revised Code includes a number of changes, including a reference to this Guideline, additional protections for vulnerable consumers, and new rules on credit assessment on financial hardship.

The revised Code also contains additional clarity on facilitating access to authorised representatives and advocates and an associated Industry Guidance Note to provide a template for use across industry.

Handling of Life Threatening and Unwelcome Communications Code

In March 2017, the revised Handling of Life Threatening and Unwelcome Communications Code came into force after being registered by the ACMA. The Code provides greater protection for Australian consumers against threatening and unwelcome communications, including where that communication is part of domestic and family violence.

Financial Hardship Guideline

The Telecommunications Industry Ombudsman, Financial Counselling Australia and Communications Alliance updated the *Assisting and Responding to Customers in Financial Hardship* guideline. This guideline enables telecommunications providers to better assist those who have experienced domestic and family violence, including identifying family violence as an express eligibility criterion for access to hardship programs as included in Recommendation 108. A revised version of the guideline was published in April 2017.

Development of this Guideline

To build on and connect the tools already in place, a Communications Alliance Working Group was set up to develop a reference document. This was done in consultation with consumer representatives and community organisations, bringing together a wide array of experience and knowledge to develop tools and educate providers.

This Guideline is the result of this work. It represents a starting point and recognises that we in the telecommunications industry still have much to learn about domestic and family violence, and it will be reviewed and updated based on continued engagement with industry participants and community organisations.

1 GENERAL

The development of the Guideline has been facilitated by Communications Alliance through an Industry Working Group, in consultation with consumer groups, Government, and regulatory agencies.

1.1 Related Documents

The Guideline should be read in conjunction with the following documents.

Related Industry Codes and Industry Guidelines, including:

- a) the Telecommunications Consumer Protections (TCP) Code (C628:2018) or as amended from time to time;
- b) the Industry Guidance Note on Authorised Representatives and Advocates (to be published end of 2018)
- c) the Industry Guidance Note on Sales Practices and Credit and Debt Management (IGN 013); and
- d) the Handling of Life Threatening and Unwelcome Communications Code (C525:2017 Incorporating Variation No.1/2018) and the related Industry Guidance Note Handling of Life Threatening and Unwelcome Communications (IGN 010).

Related ACCC Guidelines, which Suppliers must have regard to per the TCP Code:

- a) "Don't take advantage of disadvantage: a compliance guide for businesses dealing with disadvantaged or vulnerable consumers" issued in 2011.
- b) "Debt collection guideline: for collectors and creditors" issued in July 2017.

Related legislation and documents including:

- a) the Telecommunications Act 1997 (Cth)(Act);
- b) the Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth);
- c) the Competition and Consumer Act 2010 (Cth); and
- d) the Privacy Act 1988 (Cth).

External guidance, such as the TIO Financial Hardship Guideline, and guidance by organisations in Appendix 1: Additional Resources, also provide helpful information.

1.2 Objective and Scope of this Guideline

Telecommunications providers range dramatically in size, operations, products, and customers. In recognition of this, this guideline provides a range of methods and tools providers can consider to determine how they can support people impacted by domestic and family violence, as appropriate for their staff and customers.

The Guideline also seeks to raise awareness and knowledge of the types of abuse perpetrated against those impacted by domestic and family violence in the context of the telecommunications sector. It contains information, tools, options and examples of good practices for providers to choose from.

While providers must determine what is appropriate for them and their customers, it is important to consider the chosen strategies as a whole. For example, family violence

experts warn against putting any family violence policies or processes in place without providing appropriate training and support for staff.

1.3 Reading this Guideline

It is strongly recommended that providers read the entirety of the guideline before changing any procedures.

To facilitate understanding of the Guideline, action items are identified in bold, blue text in Chapters 3, and 5-8, but this is not a mandated nor exhaustive list – these are intended as tools for providers to choose from.

Chapter 9 differs from the remainder of the Guideline, as it contains a detailed step-by-step process.

To help providers understand the unique challenges faced by persons impacted by domestic and family violence, there are case studies throughout. The case studies are real. They have been provided by domestic and family advocacy organisations, and names have been changed.

1.4 Language

The language used to talk about domestic and family violence is diverse. In writing this guideline, Communications Alliance consulted with a range of advocacy and community organisations, in addition to individuals.

We have chosen to use the term “domestic and family violence” to avoid confusion, as “domestic violence” and “family violence” are used in different states in Australia, and this is intended to be a national document.

Throughout the guideline we have used a range of terms to refer to those impacted by domestic and family violence. The terms ‘victim’ and ‘survivor’ are both used, as are a range of others. We acknowledge that preferences differ strongly, and that this is a matter of import. We are not in the position to endorse any particular language, and thus have used a variety of terms with the intention of making this document as easy to understand as possible.

Additionally, please note that the term “customer” is used throughout the guideline to refer to either the Customer or the End User of a telecommunications service. In parts of the guideline where it is important to differentiate (for example, when discussing Authorised Users on an account, financial abuse, or other), we have used Customer to refer to the person who has entered into a Customer Contract with the provider.

1.5 Guideline Review

This Guideline is intended to be a living document, with ongoing learnings, discussions, and consultation continuing to build on the information and guidance provided. The Communications Alliance Industry Consumer Advisory Group will continue working with community organisations and Industry to determine how often and when the Guideline should next be updated.

Communications Alliance will also facilitate opportunities for providers and community organisations to ask questions, test ideas, and generally share good practices that are developed through use of this guideline.

2 CONCEPTS AND BACKGROUND

2.1 What is Domestic and Family Violence?

Understanding domestic and family violence, and acknowledging the different forms it takes, is a vital first step in addressing it. As defined in the *Family Law Act*, “family violence means violent, threatening or other behaviour by a person that coerces or controls a member of the person’s family or causes [them] to be fearful.” It includes physical, emotional, financial, technology-facilitated, and other forms of abuse, threats, and control within families and domestic partnerships.

Domestic and family violence is immoral and often criminal, and has devastating consequences on those who have experienced it, as well as their families and communities.

Economic abuse is a form of domestic and family violence that undermines the victim’s ability to leave the situation, or efforts to become economically independent. Financial abuse is about power, control and manipulation of an individual and often occurs with other forms of violence, including physical violence, intimidation and controlling behaviour. It can continue after those who have experienced it have left an abusive partner. Economic abuse (also called ‘financial abuse’) can include coercing someone to put debts in their name, refusing to pay bills or provide money for living expenses, and preventing a person from obtaining employment.

Financial abuse is also often seen in cases of elder abuse. While this guideline has not been specifically drafted to address elder abuse, we encourage providers to be aware of the possibility, and if appropriate this document may be updated in the future to provide information on assisting victims of elder abuse.

Abuse also often takes the form of controlling, harassment, and isolation. These can be facilitated by technology, as further discussed in the next section.

There is an ever-present risk of a perpetrator’s violence escalating. The ability of those who have experienced domestic and family violence to control their privacy and personal security is paramount.

While the vast majority of those who have experienced domestic and family violence are women and children, domestic and family violence in all its forms can happen to anyone regardless of gender, sexuality, religion, culture or age. For this reason, this Guideline is expressed in gender-neutral terms.

2.2 Domestic and Family Violence and Telecommunications

Phone and internet access has become both nearly universal and increasingly important in people’s everyday lives. This is no different – and often even truer – for those who are victims and survivors of domestic and family violence. A mobile phone can be a lifeline, but also a tool of control, and the financial hardship often facing those escaping a violent situation can impact their telecommunications services.

The information in this document can help providers understand this range of circumstances.

Domestic and family violence in the context of the telecommunications sector can take many forms including, but not limited to:

Misusing telecommunications devices and/or services to abuse

(also referred to as “technology facilitated abuse”)

- Monitoring phone calls, social media and emails without the knowledge and approval of the victim.
- The perpetrator loading spyware onto a computer or mobile phone so as to monitor the person impacted without their knowledge.
- Using technology to track the location of a survivor, for the purposes of monitoring, control, stalking, or other, including by installing monitoring software on the phone. Parental monitoring and security services can be used for these purposes.
- Accessing accounts such as email, social media, or messaging to monitor or impersonate.

Abuse via telecommunications service

- Making repeated phone calls, sending text messages or leaving messages on social media in breach of Intervention Orders or Apprehended Domestic Violence Orders.²

Access to the telecommunications account

- The abuser logging in (without permission or legitimately) and closing services, thereby cutting the victim off from contacts.
- Monitoring account activity, including information on phone bills and data usage.
- Fraudulently accessing the personal details of the victim, such as new contact details, and continuing harassment or abuse with this new information.

Financial Abuse via a telecommunications account

- The abuser being an end user or authorised representative of the Customer’s account and using the service in a way that creates a financial or other obligation on the Customer without their permission.
- Securing additional products or services (with or without coercion) under the name of the victim.
- Putting a service in the sole name of someone impacted by domestic and family violence through fraud or coercion, and then through this putting them into debt.
- A perpetrator holding the account in their own name and not paying bills, resulting in disconnection of the survivor.
- The perpetrator cancelling the telecommunications service of the person impacted by domestic and family violence if or when they try to leave.

² The *Handling of Life Threatening and Unwelcome Communications Code* (C525:2017 Incorporating Variation No.1/2018) lays out the requirements on providers in these cases, and the related *Industry Guidance Note Handling of Life Threatening and Unwelcome Communications* (IGN 010) offers additional guidance.

Case Study: Financial Abuse

Jessica sought help from a financial counsellor for financial problems arising from family violence. The financial counsellor obtained her credit report and found that she had a default in relation to a telephone service. The financial counsellor found that telephone services had been acquired by her violent partner in her name online. He had provided a different address, and Jessica didn't know anything about the accounts.

With the lack of information, it was challenging to cancel the accounts and have the credit report default removed.

The mobile phone in particular can be used as both a weapon and a tool. It can be used as a weapon by a perpetrator as outlined above, but it can also be an important tool for survivors. People experiencing abuse can use a mobile phone to reach out for help and stay connected to friends, family and specialist support services. In a large proportion of cases, those who leave a perpetrator are unable to take any personal items with them. Often the ability to stay connected is key to their safety and success, as they need to be able to contact essential services to rebuild their lives.

It is also important for providers to note that their staff can be affected by domestic and family violence, as discussed in the section on Staff and Training.

2.3 Contracts, Customer Rights, and Coercion

The Royal Commission recommended additional changes to the TCP Code to clarify consent requirements for payment plans when an account is jointly held and include grounds for splitting jointly held debt and removing an account holder's name if family violence has occurred.

Unlike other services, such as bank accounts, telephone accounts (whether landline or mobile) are not held jointly (by more than one party).

Under the *Telecommunications Numbering Plan 2015*, the word "Customer" means a person to whom a carriage service provider issues a number. Legally, there can only be one such person – however, a Customer may authorise another person to make changes or incur charges on their behalf on that account. This person would be recorded as an "Authorised Representative" on the account.

Alternatively, a Customer may give a mobile phone to another person (for example, their child or their partner) to use. In this situation, the Customer remains liable for the costs and charges incurred by the end user. The Customer also has the ability to cancel the phone at any time. In these situations, the end user of the phone (in this case the survivor) may believe themselves to be the Customer when they have no rights or obligations under the contract.

These legal distinctions can be exploited by perpetrators in domestic and violence situations.

For example, a perpetrator tactic may be to use fraud and/or coercion to put all internet and phone accounts in the name of the person they are victimising as the Customer, thereby leaving them with the legal burden of paying the bill. In this scenario, the victim could be fearful that a failure to pay would result in disconnection or being pursued by debt collectors. An adverse credit report can adversely affect the ability of a survivor to

re-establish financial independence by hampering attempts to get a loan, secure rental accommodation, or access other services. This can result in someone impacted by domestic and family violence, and their children, becoming homeless.

Case Study: Coercion

Sabreen is in her mid-20's and has two young children. Her relationship with her husband has been characterised by a long history of abuse including physical violence. Her husband took her to the local shopping centre one weekend where he insisted that Sabreen sign up to multiple telecommunication contracts with multiple telecommunication providers. They went from store to store signing up to multiple telephone services, smart watches and iPads. Sabreen only agreed to sign the contracts in her name due to intimidation by her husband and threats of further violence. She remained silent during the entire sales process.

Her husband subsequently took all the devices and sold them online to pay for his substantial drug habit. Sabreen received no benefit from the contracts. After fleeing the family home, Sabreen did not have access to any paperwork regarding the contracts she entered into nor did she have any information about the current whereabouts of the handsets.

Another example is where a perpetrator has put all internet and phone accounts in their own name as the Customer, while the victim is the end user of a mobile phone on that account. Even though the person being abused is using the phone, where the perpetrator is the legal Customer, the perpetrator has ultimate control over the service. In a case where someone experiencing domestic and family violence makes several phone calls to domestic violence support services and real estate agents with a view to leaving the abuser, as the Customer of the phone account, the perpetrator has the ability to monitor the call history. They may be able to discover that the person they are abusing is planning to leave and then cancel the service as a strategy to exert control and prevent them from leaving.

With the legal and contractual obligations to Customers, telecommunications providers cannot split jointly held debt as recommended by the Commission (as there is no 'jointly held debt'). However, this Guideline may help providers consider how they can assist people impacted by domestic and family violence within their legal obligations. Additional considerations for specific circumstances where a victim or abuser is the authorised user on the contract are addressed the section on Economic Abuse and Financial Hardship and the section on Keeping A Mobile Number.

2.4 Identifying Domestic and Family Violence

Generally, a provider will only become aware of domestic and family violence once it has been disclosed by someone impacted or an advocate. The remainder of this document focuses on what actions providers can take once they are aware.

It can be challenging to identify domestic and family violence, particularly as a growing number of interactions with consumers are via online methods. Additionally, it is often difficult for staff members at call centres or retail outlets to identify if someone has experienced domestic and family violence.

However, there are signs of possible domestic and family violence which may help providers assist customers to protect their safety and privacy as quickly and

appropriately as possible. These signs may include when a customer of a telecommunications service:

- expresses concern about their privacy, safety or the disclosure of information to another person on the account;
- expresses concern regarding the possible existence of spyware on their mobile phone, computer or tablet;
- expresses concern in relation to the ability of another party to track their location;
- appears reluctant to involve another party associated with the service, such as the Customer, another Authorised Representative, or end user of the account;
- mentions that an intervention order/apprehended domestic violence order (or equivalent) is, or has recently been, in place.

Staff members to whom a case of domestic and family violence is identified, or who are in a situation where they become aware of the above signs, will benefit from additional support. Further information is provided in the Staff and Training section of this document.

3 INITIAL CONSIDERATIONS

There are a range of ways in which providers can assist people who are impacted by domestic and family violence. There are also unique challenges and risks providers should be aware of.

This Chapter provides key initial considerations for providers, which apply across all of the options and steps in the following Chapters.

3.1 The customer knows best

It is vital for providers to understand that every instance of domestic and family violence differs, and every customer knows best how to keep themselves safe.

The first step in any action is to **check with the customer how they wish to proceed**. Whether removing an abuser as an Authorised User on the account, or determining what notes to include in the customer file, or other actions, each customer will be able to best determine how to keep themselves safe. Someone impacted by domestic and family violence should be informed of the options available and empowered to choose the most appropriate assistance for them.

3.2 Referring customers to Specialist Domestic and Family Violence Support Services

It is important to note that telecommunications providers are not equipped to provide support to customers of a telecommunications service for non-telecommunications matters.

If a customer identifies that they are impacted by domestic and family violence and request additional information or services, it can be helpful to **refer them to external legal and support organisations for non-telecommunications matters**.

Staff are more likely to make appropriate referrals if they have details of key referral points, and don't have too many to choose from. A list of support services is provided in Appendix 4: Referral Resources.

If a provider believes a Customer, an end user, their children, an employee, or any other person is in immediate danger, the matter should be referred to Police (Triple Zero).

3.3 Communicating Information to customers

Across all contacts with a customer who is experiencing domestic and family violence, it is vital to ensure information being shared is not endangering them.

Before any information is sent to a customer – including something like a Mobile Safety Facts Sheet, or new account details – **suppliers should verify with the Customer that the information will be sent in a safe way**.

Concerns can include the perpetrator having access to the victim's email accounts, a letter being sent to a shared address, or a text message to a phone that the perpetrator has access to.

Specific and additional steps for safety include:

- **Contacting at correct address:** Where a survivor has left a perpetrator and changed contact details (address, phone, email, or other), it is vital that their new details are kept private. **Carrying out additional checks when setting up new accounts or changing account information** to ensure all contact details have been appropriately updated will ensure that communications - such as mail and emails - are sent to the correct address.
- **Provide the option to limit automatic communications, such as emails or SMS:** This can be particularly helpful for customers who may be in the process of leaving their abuser, but are still in the same location. An automatic SMS about a new account or other information may arrive at an inopportune time and alert the abuser about the customer's plans to leave.

Further information and considerations on this topic is in section 4.4, Communicating in a Supportive and Safe Way.

3.4 First Steps

When first made aware that a customer is impacted by domestic and family violence, it can be helpful for the provider to **run through the below checklist with them.**

Each of the below considerations is further expanded upon in the Guideline, but initially empowering the customer by making them aware of these options and **asking what actions they would like to take with each** will provide clear guidance to the provider on how to proceed.

1. Review who is authorised to make decisions on their account.
2. Review the services that are activated under their account, including features that are turned on (such as blocked numbers, etc.).
3. Update contact information, including mailing address, phone number, email address, etc.
4. Update passwords and security settings to their online account or app.
5. Discuss any additional account security measures offered by the provider, such as PIN or password, or marking an account in a way that requires additional security.
6. Discuss use and possible limitation of automatic communication from the provider (such as emails or SMS).
7. If they are setting up a new account, make sure they don't have a previous account with the provider; if they do, make sure the perpetrator does not have access to the previous accounts (see steps 1-3).
8. Provide available information on privacy, such as referring them to techsafety.org.au, the eSafety Commissioner's website, or a Mobile Safety Fact Sheet such as in Appendix 2.

4 STAFF AND TRAINING

Providers have a number of legal obligations to abide by when developing and delivering training to their staff, particularly those who interface with customers. For some providers it may be appropriate to add information on domestic and family violence to their training. If provided, it should be relevant for the type of role the staff member has within the company.

Staff training underlies the success of any of the Actions identified in Chapters 3, 5, 6, 7, and 8 of this Guideline.

It is important to note that introducing policies or processes without adequate staff training can increase risks for customers, staff, and the organisation.

Staff who are empowered to support customers experiencing domestic and family violence also need to understand the limits and scope of their role in relation to supporting those who have experienced domestic and family violence.

Good quality training helps to:

- Embed policy and procedure into practice,
- Expel myths about domestic and family violence
- Provide opportunities for informed staff discussion and clarify employee roles, responsibilities, and boundaries.

Business-wide training can improve the safety and wellbeing of staff who have been impacted by domestic and family violence, and their co-workers, while tailored training provides tools appropriate for the role of the staff member. In addition to knowledge of the processes relevant to the individual's role, staff are most able to respond appropriately when they have been provided with an understanding of domestic and family violence and the relevant skills.

Below are some detailed considerations for providers to take into account. There are further training resources, including organisations that provide specialist training and advice, listed in Appendix 3: Training Resources.

4.1 Staff structure

Some providers may be structured in such a way that it is appropriate to have certain staff members or teams with specialised training in managing domestic and family violence cases.

This could take multiple formats, including (but not limited to) the following:

- All relevant cases are immediately referred to the specialised team or staff member, and the customer only communicates with those identified persons;
- Financial hardship cases with domestic and family violence involved are referred to specialised staff within the financial hardship team;
- A staff member or team with training supports or assists front-line staff who are handling cases involving domestic and family violence; or
- A staff member with specialised training in domestic and family violence regularly reviews procedures and policies.

4.2 Choosing a training provider

Training should be provided/developed by or in partnership with a reputable provider who has expertise in domestic and family violence, working with vulnerable people and relevant community sector services. Training providers need to be able to impart an understanding of this complex topic, respond appropriately to disclosures or personal responses by staff and ensure that staff feel safe (considering, for example, some staff in the training sessions are likely to be victims/survivors or perpetrators).

Appendix 3 has a list of relevant training providers for reference.

4.3 Business-wide training

While any training program would be highly dependent on the structure of a company and its customer service teams, providers may consider providing overall awareness raising and education information to any member of their staff.

A significant proportion of employees have experienced domestic and family violence. For many this has affected their ability to work and/or family violence has occurred at the work-place (e.g. calls or visits to work). Business-wide domestic and family violence training for staff can improve the safety and wellbeing of victims/survivors and their co-workers.

It can also support the whole organisation to have an increased understanding and provide a more integrated response. For example, if IT staff have been provided with the relevant information and are updating CRM systems, they may then be aware of the benefits of enhanced customer identity verification processes or be prepared to come up with other creative methods to assist customers impacted by domestic and family violence.

This training may include an overview of family violence, the impact it can have on customers and staff, safety, privacy, duty of care to customers and staff, and how to respond to a colleague who discloses, or is affected by, domestic and family violence.

In accordance with Workplace Health and Safety obligations, staff should also be encouraged to seek support if they are personally experiencing trauma or anxiety as a result of assisting victims or perpetrators of domestic and family violence.

4.4 Front-line staff training

For providers who have customer-facing staff, training for those staff members can help them to:

- Know the appropriate referral and escalation procedures;
- be aware of the possibility of domestic and family violence and the impact it can have on those who have experienced it;
- remain impartial and non-judgemental;
- understand unconscious bias;
- be aware of the family violence needs of multi marginalised populations such as Aboriginal and Torres Strait Islander women and women with a disability; and
- understand the scope and limitation of their role.

While training is helpful for the above goals, it is difficult to train front-line staff for every specific situation they may encounter. Thus, it is also important that they are empowered to ask their supervisors for assistance or information if they are in a situation where they are unsure about the appropriate procedures, or think domestic and family violence may be impacting the customer.

4.5 Specialised staff training

Any staff specifically tasked with assisting customers impacted by domestic and family violence will need additional support and training.

More broadly, dispute resolution and/or financial hardship staff are more likely to be required to have detailed with communications with people experiencing family violence, and to act to protect their privacy/safety and/or offer a range of solutions.

Additionally, managers who supervise relevant staff also should be enabled to provide specific support to them. Their additional training should include an understanding of issues such as vicarious trauma.

Specialised training could include any of the following information and goals:

- understand the nature and effect of domestic and family violence on those who have experienced it, including financial abuse;
- accept the word of those survivors and not request additional evidence of abuse;
- how to verify the customer's identity in circumstances where the customer has escaped a domestic and family violence situation with no belongings and has no access to paperwork or other account information;
- identify where special steps are required to protect the confidentiality of the customer by restricting access to account information and the appropriate procedure for restricting account access;
- identify circumstances where a customer has requested for a person to be removed as an authorised representative on an account and know the procedure for removing that person as an authorised representative;
- assess if a survivor is aware of ways the abuser could be accessing her/his account, and provide options on how to prevent the abuser from finding out the survivor has opened a new account (i.e. suggesting the survivor may want to set up a new private email)
- identify when it is appropriate to take action under the Handling of Life Threatening and Unwelcome Communications Code in relation to unwanted communication to those who have experienced or may be receiving life threatening or unwelcome communications;
- understand the range of financial hardship options which may be appropriate for those impacted by domestic and family violence, such as granting relief from debt, when that is appropriate, and the procedure for granting such relief;
- facilitate the process for survivors to be represented by a domestic and family violence advocate, legal advocate or financial counsellor in relation to discussions regarding their account;
- know how and when to refer victims to specialist domestic and family violence support services.

4.6 Internal staff support

Any staff dealing with domestic and family violence cases, regardless of if they have received specialised training, will benefit from additional support due to the potential trauma and emotional impacts of dealing with such cases.

Also, providers should be mindful that assisting with cases of domestic and family violence may be a trigger to some staff and they may need specialist support. With one in four Australian women having experienced physical or sexual violence by an intimate partner,³ it is likely that staff have been impacted by domestic and family violence, either directly or by knowing someone who has been abused.

As part of their duty of care to staff, providers should examine options for additional support, which may include:

- Regular supervision for staff working with customers experiencing domestic and family violence from experienced practitioners;
- Using a buddy system for staff assisting survivors, to provide support and guidance (which could include training and support from specialist services);
- Access to counselling services, which must be anonymous and not identify staff accessing this by name (including when issuing accounts for payment);
- Having spaces such as quiet rooms or gaming rooms, to allow staff the option to leave their desks and focus on something else;
- Regular checks with staff as to how they're coping which should be separate from day to day supervision; or
- Access to Employee Assistance Programs to discuss personal experiences of domestic and family violence.

³ Cox, P. (2015) Violence against women: Additional analysis of the Australian Bureau of Statistics' Personal Safety Survey 2012, Horizons Research Report, Issue 1, Australia's National Research Organisation for Women's Safety (ANROWS), Sydney; and Woodlock, D., Healey, L., Howe, K., McGuire, M., Geddes, V. and Granek, S. (2014). <http://anrows.org.au/publications/horizons/PSS>

5 CUSTOMER ACCESS TO ASSISTANCE

It can be very difficult for someone impacted by domestic and family violence to disclose abuse. This may be because they fear for their personal safety (and the safety of their children), fear being stigmatised, or fear that they will not be believed. For this reason, it is beneficial if processes are simple and easy to use.

Where appropriate, universal systems and processes that can be accessed by anyone who needs additional security measures, financial assistance, or other help can be more helpful than specific processes that require someone who has experienced domestic and family violence to identify themselves as a survivor.

5.1 Contacting the Provider

Automated phone systems can often be difficult for people impacted by domestic and family violence to use, as they may no longer have access to required information - including the relevant telephone number - due to having to leave their home.

For providers who have the capacity to do so, it would be beneficial to **have a separate and dedicated number or other method of access** to make it easy for a survivor to speak directly to a customer service representative.

Providers should also be aware that victims may not always have access to account numbers or other key information typically used to access an account. It is helpful for providers to **consider alternative options and be flexible in their procedures** in cases involving domestic and family violence.

Case Study: Access to account information

Candy* (name changed) is a 30-year-old refugee. She has been in Australia for about 7 years. Her English, legal, and financial literacy are low.

Candy approached a community advocacy organisation after reviewing her bank statement and noticing that for the past year her telecommunications provider had been deducting \$50 per month by direct debit from her bank account separately and in addition to her mobile phone bill of \$80 per month, which she paid at the post office.

By the time Candy approached the community organisation, she had taken significant steps to try and resolve the issue. She had called her provider to ask why she was being debited. Her provider told her that there were two accounts in her name: a \$50 per month plan and an \$80 per month plan. Candy denied having two plans, and explained that she only had one telephone and was only aware of the \$80 per month plan. She asked for more information about the \$50 per month plan, but she was told that this could not be provided to her as she was not able to provide the account number.

Over further contacts, Candy explained that she did not know what this alleged account was, or why she was being billed. Despite being able to show that money was being taken from her bank account by the provider, the provider claimed that Candy had failed to sufficiently verify herself as the account holder.

This caused additional challenges as the provider did not accept an Authorised Representative document from the community organisation as it did not include the account number.

5.2 Authorised Representatives and Advocates

Providers need to be aware of their obligations regarding customers, Authorised Representatives, Advocates, and end users under the Telecommunications Consumer Protections (TCP) Code, Chapter 3.⁴ Survivors may access assistance from a domestic and family violence advocate, legal advocate, or financial counsellor, and these services can be vital to them.

5.2.1 Facilitating Access to an Authorised Representative or Advocate

The TCP Code currently states that a "Supplier must ensure that a Consumer can appoint an Authorised Representative to act on their behalf,"⁵ and that "a Supplier must ensure that a Consumer can easily use an Advocate to communicate with the Supplier, if the Consumer requires."

This includes allowing those who have experienced domestic and family violence to be represented by a domestic and family violence advocate, legal advocate or financial counsellor in relation to discussions regarding their account, and facilitating the appointment of these representatives by **accepting relevant forms and documentation in a range of easily accessible methods** (as each circumstance will be different, there is no one method which will be appropriate for each customer).

Please see the TCP Code (and connected Industry Guidance Note when published) for more information, including for the distinctions between an Advocate and an Authorised Representative, and for a template to assist in appointing an Authorised Representative.

5.2.2 Determining appropriate contact

If an Authorised Representative is appointed on behalf of a victim of domestic and family violence, a provider should **clarify if that Authorised Representative should be the primary contact for the account**. This is important as the customer may be unable to discuss the account when in the presence of the abuser, and if the provider calls the customer instead of the Representative, it can create a safety risk for the customer.

It is also important to note in matters of debt collection that Part 2 Section 9 of the ACCC/ASIC Debt Collection Guideline (which providers must comply with per the TCP Code) requires collectors and creditors to generally only contact an Authorised Representative if the debtor is represented.

5.3 Dedicated Staff

To enable a customer to access assistance quickly/the best possible assistance, consider which staff members are best placed to assist customers experiencing domestic and family violence. For example, depending on the size and operations of each provider, this may sit best with specialist support teams frontline customer service staff, or with certain identified staff members.

⁴ Please note that the TCP Code is currently undergoing a revision, with anticipated publication in late 2018. Always refer to the most up-to-date registered version of the Code.

⁵ The *Telecommunications Consumer Protection Code* (C628:2015, Incorporating Variation 1/2017): 3.4.1, pg 23.

If a provider chooses to identify specific staff, it should:

- Provide those staff with the contact information for relevant advocate and community organisations.
- Provide specialised training to those staff (further discussed in 'Training').
- Ensure that dedicated staff have the appropriate authority to resolve customer problems in the most appropriate way.

5.4 Communicating in a Supportive and Safe Way

There are a range of practices providers can use to make it easier for survivors to communicate with their provider.

This section provides background information for providers on the importance of considering their communication methods, and possible options to support those who have experienced domestic and family violence.

On a high level, the recommended approach is for providers to:

- **accept the word of those who have experienced domestic and family violence and not require them to provide additional evidence or specific details;** and
- **where possible and wished for by the customer, not require someone to explain that they are experiencing domestic and family violence more than once.**

5.4.1 Case Management

There are multiple possible tools to avoid requiring customers repeat their story. These will depend on the provider's size, staff, and systems and may include:

- **Implementing a 'soft hand-offs' procedure** whereby if a customer has identified as having experienced domestic and family violence and the call needs to be transferred to another customer service representative, the first representative summarises the issue to the second before handing off the call so the customer doesn't have to repeat themselves.
- **Having one specific customer representative** with whom the customer can communicate, and for whom they have a direct method of contact. This can help prevent the need for them to explain their situation more than once. A buddy system could also be used so as to have more than one staff member aware of the customer's situation, and to provide support between staff members.
- **Having a single point of contact** for customers experiencing domestic violence, such as a 1800 number, that is promoted to domestic violence victim support services and advocates.
- **Flag relevant customer files** as being case managed (without identifying the specific circumstances), so that regardless of how the customer contacts the provider for following interactions, they are always referred to the appropriate team or staff member who is aware of their circumstances, without having to include specific notes within the customer's file.

For any procedure, it is important to consult the survivor first.

In some cases, someone may not wish for any information to be included in their customer file for confidentiality or other reasons, and they may be comfortable with

needing to re-explain their circumstances each time they contact the provider. In other cases, someone impacted by domestic and family violence may wish to have their file managed by a specialised team or person to facilitate access to assistance. Good practice is to **discuss the options a provider has with a customer to determine how they wish to proceed.**

5.4.2 Communication

Additionally, providers should be aware of the unique circumstances which could impact how a customer communicates with them. Some examples are:

- Someone impacted by domestic and family violence may at different times be in the presence of their abuser. This may lead to them answering questions differently than previously, or being unable to discuss their case at the moment.
- They may not wish to be contacted, but prefer to contact the provider, so they can discuss their account when they are in a safe place.

One option to address the above challenges is to **ask the survivor whether it is a suitable time to speak when the provider initiates the contact, and check if it is appropriate to leave messages or send emails regarding the account.**

Providers should also consider that:

- It may be difficult for a customer to provide a mailing address, or other contact details including email addresses and phone numbers, if they are in the process of leaving their home and are relying on community resources or friends.
- Someone experiencing domestic and family violence may only be contactable through advocates or authorised representatives, or alternatively may rely strongly on an advocate/authorised representative to handle their account, as they may be continuing to live with their abuser, having to move between locations, or otherwise be uncontactable for safety reasons.

It should also be noted that the 'typical' security identification procedures used when communicating with a customer about their account can be easily bypassed by an abuser who is a family member or intimate partner. This is further discussed under the next Chapter on Customer Accounts: Privacy and Safety.

6 CUSTOMER ACCOUNTS: PRIVACY AND SAFETY

Safety and confidentiality is paramount when assisting customers who are at risk of harm. It is vital that those who have or are experiencing domestic and family violence have control over their privacy and personal security.

Protecting customers can be complex, but should be a priority.

This is an area where specialist assistance and training are important, as there are potential consequences that would often not be considered.

For example, it should not be automatically assumed that if domestic and family violence is involved, the perpetrator should be denied access to the account, as this may inform the perpetrator that the victim is planning on leaving. On the other hand, some survivors face risks when a perpetrator can access their personal details. It is important to **verify with the victim what they wish to do**, as any action taken without their consent may result in an unsafe situation.

6.1 Account verification

Risk of harm can increase when someone impacted by domestic and family violence leaves their abuser. In these cases, perpetrators may seek to use the personal details of their victims to pass routine identity verification procedures and obtain information such as a new address, call history or other personal information in order to continue the abusive behaviour. This is challenging for providers to address, as they have a range of privacy and access obligations to follow regarding customer accounts.

One option is to **give customers the option to change identity verification procedures so that they are not linked to a customer's personal details**. This could be through putting in place an additional account verification procedure based on a PIN or other password.

This could be provided as an option to a range of customers who have heightened security or privacy concerns, preventing the singling out of those who have experienced domestic and family violence. This could have a range of benefits, including in cases of fraud and identity theft as well helping people impacted by domestic and family violence maintain their privacy and safety.

6.2 Account information

As noted in the section on First Steps, as soon as the provider is aware that their Customer is impacted by domestic and family violence, it is important to **check with the customer that all contact information on the account is accurate**, including mailing address, phone number, email address, etc. This is to ensure that the abuser's contact information is not listed inappropriately, which can put the survivor at significant risk.

7 ECONOMIC ABUSE AND FINANCIAL HARDSHIP

Perpetrators can use economic abuse as a way to control their victim and prevent them from leaving the abusive relationship. The Royal Commission into Family Violence noted that of 170 women assisted by Women's Legal Service Victoria's Stepping Stones project, 25% were dealing with a debt accrued against their wishes, without their knowledge, without understanding, or under duress.⁶

As outlined in the information on Contracts, Customers Rights, and Coercion, the nature of telecommunications contracts means that this can happen with these accounts.

Case Study: Economic Abuse

Danielle was subjected to years of emotional, physical and financial abuse. Her ex-husband took her to five telecommunication shops and signed her up to five mobile phone plans. He then sold the handsets to third parties, leaving the debts in Danielle's name. Danielle's ex-husband is now in prison and her credit report is ruined, preventing her from starting a business. She received daily calls from debt collectors about the debts.

7.1 Financial Hardship

Financial hardship assistance is one way to assist people impacted by domestic and family violence. The TCP Code requires providers to have a financial hardship policy and lists domestic and family violence as an express eligibility criterion for access to financial hardship programs. In addition to the requirements in the TCP Code, financial hardship policies may also be adapted to specifically include options which support survivors.

If considering how a financial hardship policy can be adapted to support customers impacted by domestic and family violence, **the procedures, policies, and tools below should be evaluated in light of options a provider already has in place.** Additionally, it is good practice to **consider each case individually and be flexible in applying the policy.**

- Fast-track financial hardship requests where domestic and family violence is disclosed as an issue.
- Ensure the financial hardship team is specifically trained to assist survivors.
- Have a range of options available to assist those impacted by domestic and family violence including:
 - suspending debt until the customer can get their finances back under control;
 - waiving part or all of the debt;
 - where the person who has experienced domestic and family violence is the Customer and the perpetrator is an authorised representative, removing the perpetrator as an authorised representative from the account (after confirming it is safe to do so); or

⁶ Royal Commission into Family Violence: Report and recommendations, page 102; Emma Smallwood, 'Stepping Stones: Legal Barriers to Economic Equality After Family Violence' (September 2015) 6.

- where the person experiencing domestic and family violence is an authorised representative, or end user, and the perpetrator is the Customer, assisting the survivor to set up a new account in their own name.
- Have a range of options available in terms of the obligation to return handsets, including:
 - Allowing a grace period for the return of the phone;
 - Waiving the requirement to return the handset where it is held by the perpetrator and the person experiencing domestic or family violence no longer has access to the phone (Note: Providers may choose to IMEI block a device in such a situation); or
- Exempt a customer in financial hardship as a result of domestic and family violence from further credit management actions while payments are being made to the supplier according to an agreed payment plan or schedule. This includes exempting the customer from the following credit management actions:
 - Restriction, suspension or disconnection of essential telecommunications services;
 - Legal action relating to the outstanding debt;
 - Credit default listing in respect of the outstanding debt; and
 - Payment of additional debt recovery costs (including payment of any interest accrued prior to the customer being identified as in hardship or which has accrued during the customer's period of financial hardship).
- Establish specific arrangements with debt collection agencies so that, if the debt collection agency becomes aware of a domestic and family violence situation as part of their debt collection, they are required to inform the telecommunications provider.

7.2 Authorised Users and Sharing of Accounts

As addressed previously, economic abuse can be committed via coercion, with the abuser coercing the victim (as the account holder) into making them an authorised representative on the account and then driving up debt in the victim's name, with no benefit to the account holder.

While providers will often become aware of these circumstances through Financial Hardship processes, there are circumstances in which the victim/survivor may not request financial hardship assistance, but **it would still be beneficial for a provider to waive part or all of the debt arising from that coercion.**

Revoking Authorisation

If a perpetrator is an Authorised Representative or otherwise on the victim/Customer's account, the Customer may wish to remove them. Providers should make information on how to remove an Authorised Representative available, but should not automatically assume someone impacted by domestic and family violence will want to remove an abuser from their account.

Good practice is to **ensure the Customer knows** who is authorised on their account, that they have the option to remove an Authorised Representative, what steps are required, and exactly what will happen (if the Authorised Representative will be notified, if they will lose access to a phone number, or any other consequences), **so the Customer can choose the action that is appropriate for their circumstances.**

8 TECHNOLOGY FACILITATED ABUSE

A phone can be used by a perpetrator to control and harass. Sending unwanted or abusive texts, stalking, and making threats over the phone are just some examples of the ways perpetrators can misuse phones to abuse those who have experienced domestic and family violence. This is unfortunately a common experience for survivors.

This section lists specific information that may be helpful to give to a customer. It is vital to **check with the customer whether the method of providing any information is secure** – for example, to verify that the perpetrator does not have access to the relevant email account.

Providers should be aware that use of a telecommunications service to abuse or threaten life or property may be a crime under the Telecommunications Act.

8.1 Location and Privacy on Devices

It can be helpful for a provider to **alert someone impacted by domestic and family violence to the possibility that their whereabouts and online communication can be monitored – via devices and/or the telecommunications account**,⁷ and empower them with ways to improve their online and mobile security.

As the apps and other methods for tracking location and invading privacy are complex and quickly evolving, it may be most useful to **refer customers to a service** dedicated to providing them with information and tools on this topic. Two specific resources are:

- Techsafety.org.au, the Women's Services Network (WESNET) Safety Net Australia project: <https://techsafety.org.au/resources/resources-women/>
- The eSafety Commissioner's website: <https://www.esafety.gov.au/women>

Additionally, a fact sheet template is provided in Appendix 2, which can be given directly to relevant customers, or hosted on a provider's website.

8.2 Preventing or Stopping Harassment

The *Handling of Life Threatening and Unwelcome Communications Industry Code* provides a framework for the prompt handling of communications that are life or health threatening, the resolution of Unwelcome Communications, and rules for when to involve the Police.

In situations where the phone or text harassment falls short of fitting within the Unwelcome Communications Code, providers could offer other support mechanisms. The customer may wish to prevent the harassment, or collect evidence.

⁷ Most customers may not be aware that if the abuser is the Customer or an Authorised Representative on an account, they can access approximate historical location data via mobile towers.

Preventing harassment via blocking the abuser

To enable the customer to prevent harassment, the provider could **provide the following information**:

- advice on how to block a person's communications, such as blocking options on devices; or
- advice on how to prevent a person monitoring their communications.

Preventing harassment via changing phone number and/or device

A provider could also **provide the following options – and associated guidance** – to someone impacted by domestic and family violence:

- suggesting they change to a new phone;
- suggesting a change to a new and unlisted telephone number, and provide guidance on how to make a new number unlisted; or
- advice on how to move contacts and apps to a new mobile phone.

8.3 Collecting evidence of technology facilitated abuse

Call records and text messages can be important evidence for people impacted by domestic and family violence, assisting them to access law enforcement support.

While each provider has different abilities and systems to retain text messages and call records, and we acknowledge that there may be privacy considerations in providing copies of these records, there are some steps providers can take to facilitate access to this evidence for survivors.

First and foremost, it is important to **provide clear and understandable information on what records can be provided and how, by explaining the following**:

- exactly what type of records a customer can be provided;
- why certain records cannot be provided;
- the length of time it will take to access records;
- exactly what formal request needs to be provided; and
- the differences in what can be accessed (and for how long) if there is a police request to retain/access records.

Survivors and people assisting them should be aware that Customers can always access phone records, billing records, and other records that must be kept for other regulatory reasons, such as under the Telecommunications Consumer Protections Code.

Finally, providers may wish to **consider waving any fees** typically charged for these requests in cases of domestic and family violence.

9 PROCESS FOR KEEPING A MOBILE NUMBER

This Chapter differs from the rest of the Guideline. It outlines the steps providers could take to facilitate a survivor - who is the end user of a phone number but not the Customer - keeping their phone number when leaving the perpetrator. Specific actions are not identified as it is an overall procedure.

Ongoing access to an established mobile number can be a key lifeline for someone leaving a situation of domestic and family violence. Often a person has had a mobile number for years, and once leaving their home, it may be the only way employers, friends, and family can contact them. It may also be a vital link to providers of support services.

However, if a perpetrator is the owner of the account (the Customer) with their own mobile number, and the survivor is an authorised user on that account and has a separate mobile number of which they are the end user, the survivor's mobile number legally belongs to the Customer (in this case the perpetrator), regardless of the length of time the survivor has been the end user of it.

This can mean that if someone experiencing domestic and family violence chooses to leave an abuser, they lose access to the mobile number they have previously been using.

While the Rights of Use of Numbers Code (C566:2005), relevant regulations/legislation, and current standard forms of agreement present challenges for providers to assist end users to keep their number, work has been undertaken to identify a process which would make exceptions to some existing regulation, until such time as regulation can be modified, to enable an end user to keep their mobile number in cases of domestic and family violence.

It is important to once again note the necessity of letting the person impacted by domestic and family violence take the lead in deciding if they wish to use the below process to keep their mobile number or they may prefer to take a service with a new mobile number in order to avoid the potential for unwelcome communications being sent to the mobile number they presently use.⁸

The general steps involved are presented below, to be adapted as appropriate for each provider. As with the rest of this Guideline, operationalising this will be an ongoing process, and learnings will be incorporated into updates of this Guideline on a regular basis.

9.1 Standard Forms of Agreement

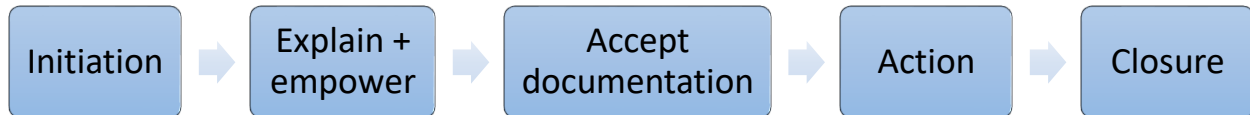
The first step is for a provider to review and if necessary modify their Standard Form of Agreement (SFOA) to determine whether there are sufficient arrangements within the contract that would allow for termination of service to a specific number in the case of needing to disassociate a mobile number from the account where the end user has been the subject of domestic and/or family violence. Providers may need to clarify that

⁸ There is an industry process that deals with the matter of unwelcome communications in Industry Code C525 Handling Life Threatening and Unwelcome Communications.

the Customer will have the service of an end user's mobile number terminated if the end user approaches the provider with a claim of domestic and family violence.⁹

9.2 Process of separating a number

Once a provider's SFOAs are appropriately modified (where required), an end user can initiate the following process.



Initiation

- An end user impacted by domestic and family violence, or their representative (such as a family violence advocate or financial counsellor) should contact the provider, outline their situation, and discuss any arrangements for the end user to be able to keep the mobile number they have been using.
- Providers should ensure that retail and customer service staff are aware of this process, and if they need to direct the end user to a specific team, that they have the correct contact information for that team or can provide that information to the end user.
- If an end user has initiated this process in a store and request the documentation in printed form, print and provide that documentation in store, but ensure the customer has access to or is contacted by whichever staff are appropriately trained for the following step ("Explain and Empower")

Explain and Empower

- The provider clearly explains whether they have a process to enable an end user to keep the mobile number, and if so what that process includes, such as:
 - Providing any required forms or documents or directing the end user to where they may access any necessary forms.
 - If they request via email or mail, verify which email/postal address it should be provided to (do not assume it is the address on the account)
 - If they request it to be sent to a counsellor, advocate, or other representative, do so
 - The outcomes of the process if completed.

⁹ Providers should have regard to section 99 of the [Telecommunications Numbering Plan 2015](#): Recall of an issued number without replacement:

"A carriage service provider may recall an issued number from a customer without issuing a replacement number only if: ...

(g) the supply of the carriage service to the customer is otherwise terminated;"

- The timelines associated with each step of the process.
- Who the ongoing contact person at the provider will be.
- The provider empowers the end user by asking:
 - Who the provider should contact throughout this process (the end user or their representative).
 - How the change should be communicated to the Customer (perpetrator) (further discussed under "Action").
- To the extent possible, the provider takes action to ensure ongoing service to the mobile number by the end user.
 - This may include account barring to stop the number from being upgraded, disconnected, SIM swapped or ported by the perpetrator.

Accept documentation

Which documentation?

An ongoing challenge will be striking the appropriate balance between limiting required documentation from a survivor and preventing misuse of this process for fraudulent purposes.

As previously noted in this Guideline, obtaining documentation can be extremely challenging for someone impacted by domestic and family violence, and this is important for providers to take into consideration. That being said, Communications Alliance also recognises that providers have a responsibility to protect their Customers from fraud. Communications Alliance will facilitate ongoing discussions and feedback on this question, and when appropriate, will update this document with good practices that have been developed through collaboration between providers and consumer advocates.

Considering the unique situation of every person experiencing domestic and family violence, good practice would be to **consider any documentation requirements/process set up by the provider to be a guideline for each circumstance**, and not set in stone. Appropriately trained and empowered staff at the provider should be appointed to review each case and determine the appropriate steps.

Possible documentation

The provider who developed this process has proposed the following:

- Establishing association with the mobile number: this could be accomplished through use of a One Time PIN sent to the end user mobile number and/or relevant proof of association, such as by call history, or other validation tools that the provider may choose to use; and
- Establishing domestic and family violence: this could be established through an Apprehended Violence Order or Family Violence Order, a Court Order, a Statutory

Declaration, or a letter from a women's shelter, financial counsellor, or other community advocate that is able to be verified by the provider.¹⁰

Accepting documentation

It is important for the provider to appropriately facilitate the acceptance of documentation, whether in store, over email, or other method, and to have provided the end user or their representative with the appropriate information of where to send the documentation, including information on the providers procedures to assure confidentiality.

Communicating next steps

In order for someone impacted by domestic and family violence to protect themselves, they must be provided with clear information on the next steps once the above documentation has been received, including exact timing.

Action

Action on Customer (perpetrator) account

As mentioned under "Explain and Empower," it is important to communicate with the survivor about the steps taken on the Customer's account. Removing a number from a perpetrator's account could make them aware that the person impacted is leaving, and thus **initiation of this process must be discussed and agreed with the end user prior to any action being taken.**

Each provider needs to consult legal advice to determine what information must be provided to a Customer when a mobile number is removed from their account. Possible options are:

- To place a note on the account stating that the Customer (account holder) no longer has rights of use over the mobile number, and that all future charges associated with that mobile number from a specific date will be waived.
- To proactively contact the Customer notifying them of the loss of the mobile number.

If the first action is taken, a provider should provide guidance regarding what the Customer should be told if they ask about the loss of access to the mobile number. This should be in consultation with the end user or their representative.

Action on end user's mobile number

The mobile number is separated from the original account.

A new account is set up with the original end user (person impacted by domestic and family violence) as the sole Customer. This may be a prepaid or post-paid service and will

¹⁰ Communications Alliance does not recommend requiring documentation to establish domestic and family violence for any other parts of this Guideline, but is aware that in this circumstance it is necessary due to the legal nature of separating a mobile number from an established account, and to prevent fraudulent misuse.

be subject to the normal identity and credit checks (where relevant) required in association with establishing a new service.¹¹

- Ensure to check with the new Customer (the survivor) that all contact information on the account is correct and is not accessible by the perpetrator.
- Recommend that if there are specific security codes used by the new Customer, they do not use ones which the perpetrator would know or could gain access to (such as a known email account, an account logged in on a device the perpetrator has access to, etc.), or could easily guess (such as a birthdate).
- Providers may offer a complimentary recharge or service credit to give the new Customer an opportunity to set up a new plan without losing service continuity.
- Provider informs the new Customer that they now have the Rights of Use for that number, which includes a right to port the mobile number to a new provider.

Closure

At this point, the process can be considered closed, and the new Customer has full access to the mobile number.

¹¹ The Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination specifies the required identity checks in the case of prepaid services. It does contain a range of options, and we recommend providers be as flexible as possible within these rules, as access to identity documents can often be challenging for a survivor.

Part 3.2 of the Determination also lays out a specific process for exemption to the rules in the case of supplying prepaid services to family violence-affected individuals.

<https://www.legislation.gov.au/Details/F2017L00399>

APPENDIX 1: ADDITIONAL RESOURCES

Below are a range of resources which can provide additional information on how government, advocacy groups, and other industries are working on this issue.

White Ribbon Accreditation

The White Ribbon Workplace Accreditation Program recognises workplaces that are taking active steps to stop violence against women, accrediting them as a White Ribbon Workplace.

White Ribbon Workplaces engender a whole-of-organisation commitment to stop violence against women, meeting 15 criteria under three standards to create a safer and more respectful workplace. The program provides tools to strengthen a culture of respect and gender equality at all levels of the organisation.

Telstra Safe Connections Program

Telstra has partnered with the Women's Services Network (WESNET) since late 2014 to help women impacted by domestic violence to stay safely connected. Telstra provides smartphones, and pre-paid credit; WESNET distributes the phones to frontline domestic violence services across Australia in conjunction with technology safety advice and training.

<https://www.telstra.com.au/content/dam/tcom/personal/consumer-advice/pdf/consumer/cyber-safety-safe-connections.pdf>

Australian Banking Association Industry Guideline: Financial abuse and family and domestic violence policies

In November 2016, the ABA released industry guidelines to provide a voluntary framework for supporting customers impacted by family violence.

https://www.ausbanking.org.au/images/uploads/ArticleDocuments/207/ABA_Industry_Guideline_-_Financial_Abuse_and_Family_and_Domestic_Violence%20Nov%202016.pdf

Essential Services Commission: Moving towards better practice

In May 2017 the Essential Services Commission released a guideline document to provide examples and guidance on ways the Victorian water industry could assist customers experiencing family violence.

<https://www.esc.vic.gov.au/document/water/53784-moving-towards-better-practice-implementing-family-violence-policies-victorian-water-sector-may-2017/>

Economic Abuse Reference Group

A coalition of community organisations, and has produced some guidance on good practice: <https://earg.org.au/good-practice/>

Thriving Communities Partnership

This is a cross-sector collaboration providing a centralised platform for collaboration on combatting customer vulnerability and hardship: www.thriving.org.au

APPENDIX 2: MOBILE SAFETY FACT SHEET TEMPLATE

Quick tips for mobile safety

1. Know the basics

Set your web browser to private or incognito mode so that pages you visit don't appear in your history (note: if there is spyware on your phone, tablet, laptop, etc. browsing is never secure).

Create a strong, easy-to-remember passphrase for each of your accounts, containing three or four words, some capital letters and punctuation. Try not to use the same password/passphrase for all your accounts.

Don't allow your device to remember passwords/passphrases or sign-in to accounts automatically, and keep log-in details to all of your accounts private and safe. (Note: You might want to consider using a password manager to make password management easier and more secure).

Auto-lock your mobile device with a passcode.

Never share passwords or PINS with anyone else.

Regularly change passwords, including on devices used to access communications such as your mobile, tablet, laptop, etc. and broadband access points (e.g. routers).

2. Minimise location sharing

Smartphones can track and may sometimes share your location without you even knowing it. To minimise location sharing we recommend that you:

Check the location services in your mobile device's settings and know which apps are accessing your location.

Check if your location is being shared with another person and consider turning off location sharing for persons who you may not want to share this information with.

Turn off geo-tagging for photos.

Control which apps can access your location.

Decline location access wherever possible when downloading new apps, unless you're sure that the app needs to know your location for basic operation.

3. Keep social media private

Most sites and apps allow users to limit what others see. So regularly check the privacy settings on all your online accounts, especially social media.

And to stay safe, don't share your location when posting, nor 'over-share' details about your identity, life or location.

Be careful when posting images as the image itself may provide information that can identify your location.

4. Increase your phone's security

If you have an Android, limit your phone's ability to download apps or software outside of the Google Play store by turning off "Allow installation of apps from unknown sources" under Settings, Security. Use two-step log in for your accounts. Two-step log-in, or two-factor authentication, provides an extra security measure that asks for a security code,

which is sent to you via email or mobile. Generally, this means that if an unauthorised user tries to access your account, they won't be able to, even if they know your username and password, **however be aware that this requires that the perpetrator has not got access to the email account such verification is sent to, or for SMS that your device does not have an app that forwards messages to another party.**

5. Check for connected devices

Most smartphones have an email account associated with the phone. For iPhones, this is your Apple ID (iCloud). For Android phones, this can be your Google Account. These accounts can be linked to multiple devices that could access your personal information. Check to see if other devices are connected to your account and remove unknown or unwanted devices.

6. Turn off and log out

Turn off Wi-Fi and/or Bluetooth if you aren't using it.

Log out of accounts when you are not using them – whether you logged in using the web browser on your mobile or through an app.

Close apps when you are not using them.

Other safety measures

Signs you are being monitored

Does the perpetrator seem to know most of the things you do on your phone?

Does the perpetrator seem to know your location whenever you have your mobile device with you?

Does the perpetrator have access to your mobile device, social media accounts, bills or passwords?

Remember that there are many ways someone can monitor your phone activity, such as accessing your accounts or tracking your location with a GPS tracker.

If you think someone may be monitoring your mobile device, and you need to block them immediately, put your device in 'flight mode'.

Limit your usage

If you think it is not safe to make changes to your device, then limit the amount of information you are sharing using your device and consider using public telephone boxes, a friend's phone, or computers at your local library instead.

APPENDIX 3: TRAINING RESOURCES

The Women's Services Network (WESNET): WESNET offers a range of training and resources, including tailored training programs.

<https://wesnet.org.au/safetynet/training/>

Good Shepherd Australia & New Zealand: Good Shepherd provides a range of training modules and tailored programs.

<https://www.goodshep.org.au/find-a-service/professional-development/>

Uniting Kildonan: Kildonan's Enterprise Partnerships team consults and trains corporate, government and community organisations that are looking to improve their systems and processes for dealing with vulnerable customers.

<https://www.kildonan.org.au/programs-and-services/corporate-consultancy/>

Women's Information and Referral Exchange (WIRE): WIRE provides in house training packages, speakers, and other resources.

<https://www.wire.org.au/professional-training/>

eSafety Commissioner's Office: The Office of the eSafety Commissioner and WESNET deliver free workshops about technology-facilitated abuse, and can also provide training on this topic tailored to your organisation/staff needs. The Office also provides online training on technology facilitated abuse.

<https://www.esafety.gov.au/women/get-help/esafety-for-women-training>

APPENDIX 4: REFERRAL RESOURCES

This list has been developed by community organisations with the aim of providing key referral points. It is suggested that businesses don't add to the list unless they have a relationship with a particular organisation and/or staff have training that enables them to identify the most appropriate agency in each case.

The Economic Abuse Reference Group (EARG) has developed a Good Practice Guide on Referrals, on how to make it easy for those making the referrals to determine where to refer. This is available on their website: www.earg.org.au

Need	Coverage	Agency	Hours	Contact
Immediate danger	National	Police, Fire, or Ambulance	24/7	000 Use 106 if you are hearing or speech impaired.
Counselling, support, and emergency accommodation	Note: Provide details for state/territory service and the national service in case the local service is unavailable.			
	National	1800 RESPECT	24/7	1800 737 732 www.1800respect.org.au
	NSW	Domestic Violence Line	24/7	1800 656 463 http://dvnsw.org.au/html/contact.htm
	Victoria	Safe Steps		1800 015 188 www.safesteps.org.au
	Queensland	DV Connect Womensline		1800 811 811 http://www.dvconnect.org
	South Australia	Domestic Violence & Aboriginal FV Gateway		1800 800 098
	Western Australia	Women's Domestic Violence Helpline		1800 007 339
	Tasmania	Family Violence Counselling & Support	Weekdays 9am-12am Weekends/ Public holidays 4pm-12am	1800 608 122 http://www.dhhs.tas.gov.au/service_information/children_and_families/family_violence_counselling_and_support_service
	ACT	Domestic Violence Crisis Service	24/7	(02) 6280 0900 https://dvcs.org.au

Counselling & referral for men (perpetrators or those who have experienced domestic and family violence)	Victoria, NSW & Tasmania	No to Violence - Men's Referral Line	NSW & Tasmania: 24/7 Victoria: Mon-Fri 8am-9pm, Weekends 10am-6pm	1300 766 491 http://www.ntvmrs.org.au (online chat)
	National	Mensline	24/7	1300 789 978 https://mensline.org.au (online chat)
Financial/Debt issues	National	National Debt Helpline (financial counselling)	Generally 9-5 local time in each state	www.ndh.org.au 1800 007 007

Mobile Apps

These mobile apps may provide resources to those who have experienced domestic and family violence. However, domestic violence service apps should only be downloaded if they have safe, secure control and access to their phone.

- [Penda](#): Penda is a free, national app with legal, financial, and personal safety information and referrals for women who have experienced domestic and family violence.
- [Daisy](#): Daisy is an app developed to connect people experiencing violence or abuse to services in their local area. The app includes safety features to help protect your privacy.
- [Smart Safe](#): A mobile phone app that supports women to collect evidence of family violence safely.
- [Tech Safety](#): Contains information that can help someone identify technology-facilitated harassment, stalking, or abuse and includes tips on what can be done.
- [Live Free](#): (Victoria specific) Provides information and access to local and state based resources and support.
- [Aurora](#): (NSW specific): Information, support, and services about domestic violence in NSW.

Additionally, WESNET has a handout for survivors on choosing a safety app, available at: https://techsafety.org.au/wp-content/uploads/2016/12/WESNET_SafetyAppConsiderations.pdf

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.



**Published by:
COMMUNICATIONS
ALLIANCE LTD**

**Level 12
75 Miller Street
North Sydney
NSW 2060 Australia**

**Correspondence
PO Box 444
Milsons Point
NSW 1565**

**T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507**

Care should be taken to ensure the material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact Communications Alliance