COMMUNICATIONS ALLIANCE LTD

INDUSTRY GUIDELINE

G660:2023

ASSISTING CONSUMERS AFFECTED BY DOMESTIC AND FAMILY VIOLENCE

Incorporating Variation No.2/2024

G660:2023 Assisting Consumers Affected by Domestic and Family Violence Industry Guideline

Incorporating variation No.2/2024

First published as Communications Alliance G660:2018
Second edition as Communications Alliance G660:2023

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

Notwithstanding anything contained in this Industry Guideline:

Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

- reliance on or compliance with this Industry Guideline;
- inaccuracy or inappropriateness of this Industry Code/Guideline; or
- inconsistency of this Industry Code/Guideline with any law; and
- 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 Industry Code/Guideline.

The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

INTRODUCTORY STATEMENT

Domestic and family violence (DFV) refers to the use of power, control, and coercion by one party against another to create a dependency, isolate, monitor, or restrict them. The majority of those affected are women in a heterosexual relationship with the male perpetrator. However, it is important to understand and recognise that there are many other forms of DFV; violence and abuse can present in any relationship, from intimate partnerships, immediate and extended family groups, communal and extended kinship connections, to carer and guardianship arrangements, and can affect people of any ages, gender, sexuality, culture, education, wealth, or community.

It is a significant health and welfare issue in Australia:

- One woman is killed every 7-9 days, and one man every 29 days by a current or former partner[1].
- Intimate partner violence causes more illness, disability, and death than any other risk factor for women aged 25-44[2], with younger women, those of Aboriginal and Torres Strait Islander descent, and those living with disability experiencing higher rates of violence[3].
- One in four (23% or 2.2 million) women and one in 13 (7.8% or 704,000) men experienced physical and/or sexual violence by an intimate partner at least once since age 15[4].
- One in four women and one in six men have experienced partner emotional abuse since age 15[5].
- 14.8% of Australians over 65 reported experiencing abuse in the past year, with the main perpetrators being the affected person's intimate partner or intergenerational family member[6].

Addressing DFV is a whole-of-community responsibility. It requires government, communities and the corporate sector to work individually and cooperatively to identify and respond to challenges.

Recognising that telecommunications services serve as a lifeline to those experiencing abuse – while the same connections may also be used as a vehicle to commit abuse - the telecommunications industry is uniquely positioned to respond and support those affected by DFV.

---

[1] Australian Institute of Health and Welfare. (2022). *Family, domestic and sexual violence*. Retrieved from https://www.aihw.gov.au/reports/domestic-violence/family-domestic-and-sexual-violence.
[2] Relationships Australia NSW. (2022). *What is Family and Domestic Violence*. Retrieved from https://www.relationshipsnsw.org.au/what-is-domestic-and-family-violence-a-definition/.
[3] Relationships Australia NSW. (2022). *What is Family and Domestic Violence*. Retrieved from https://www.relationshipsnsw.org.au/what-is-domestic-and-family-violence-a-definition/.
[4] Australian Institute of Health and Welfare. (2022). *Family, domestic and sexual violence data in Australia* . Retrieved from https://www.aihw.gov.au/reports/domestic-violence/family-domestic-sexual-violence-data
[5] Australian Bureau of Statistics. (2022, August 24). Domestic Violence: Experiences of Partner Emotional Abuse. ABS. https://www.abs.gov.au/articles/domestic-violence-experiences-partner-emotional-abuse.
[6] Qu, L., Kaspiew, R., Carson, R., Roopani, D., De Maio, J., Harvey, J., Horsfall, B. (2021). National Elder Abuse Prevalence Study: Final Report. (Research Report). Melbourne: Australian Institute of Family Studies. (p. 72).

This Guideline is designed to help retail Carriage Service Providers (RSPs) identify and appropriately assist consumers affected by domestic and family violence.

It provides practical, operational-level guidance about the policies, training, and supporting materials RSPs should have in place to enable them to recognise DFV and provide appropriate and safe help to consumers affected by it.

Annie Leahy

Chair

Domestic and Family Violence Guideline Working Group

May 2023

Code revision history

This Guideline (G660:2023) updates and replaces *Assisting Customers Experiencing Domestic and Family Violence Industry Guideline* (G660:2018).

Key changes captured in the May 2023 version include:

- a restructure of the Guideline to better support its practical implementation;
- expanded coverage to include:
    - the full range of telecommunications consumers, products, and services, including small business customers and fixed services;
    - updated information about the forms of DFV that may present; and
- updated figures, links and references.

Updates were made to the Guideline in June 2023 to reflect the publication of new Industry Codes that contained specific protections for those affected by DFV:

- C525 Handling of Life Threatening and Unwelcome Communications Industry Code; and
- C556 Number Management – Use of Numbers by Customers Industry Code.

Updates were made to the Guideline in March 2024 to reflect the publication of new *Telecommunications (Financial Hardship) Industry Standard 2024* that contained specific protections for those affected by DFV.

Summary of chapters

Chapters 1-6 of this Guideline describe how DFV might present in a telecommunications context and emphasise the need for RSPs to have clear organisational structures, dedicated training, policies and supporting materials to ensure support can be provided to DFV affected consumers in an accessible, safe and trauma-informed manner.

The remaining chapters provide specific guidance on implementing a DFV policy - outlining recommended actions to support DFV-affected customers to safely manage their accounts, address safety issues, find options to safely respond to DFV, and assist during debt and financial hardship events.

The appendices set out recommended resources and support for RSPs, their consumers and staff and detail the process for managing right of use of numbers.

Acknowledgements

Thank you to the Communications Alliance members who shared their time and knowledge to review this Guideline: Telstra, Optus, TPG Telecom, Vocus, Aussie Broadband, amaysim and Pivotel.

The Working Group also wish to acknowledge the following stakeholders and thank them for their engagement, case studies, knowledge-sharing and openness during the information-gathering and consultation stages of this review: Australian Communications and Media Authority (ACMA), eSafety Commissioner, Telecommunications Industry Ombudsman (TIO), Australian Communications Consumer Action Network (ACCAN), Consumer Action Law Centre (CALC), WESNET, Woman's Legal Service Victoria, Economic Abuse Reference Group (EARG), 1800RESPECT, Katherine Women's Legal Service, DV Service Management, DV Safephone, Telco Together Foundation, Thriving Communities Partnership, Relationships Australia, and the Australian National University's Centre for Social Research & Methods.

TABLE OF CONTENTS

1. GENERAL

1.1. Introduction

1.1.1. All retail Carriage Service Providers (RSPs) should have policies, systems and processes to recognise and safely and appropriately respond to domestic and family violence.

1.1.2. This Guideline is designed to provide a framework and practical guidance to assist RSPs with this task.

1.1.3. It was developed through a working committee of industry specialists, facilitated by Communications Alliance, with considerable input and advice provided by specialist DFV services, legal services, consumer groups, and government agencies.

1.1.4. Case studies used throughout the Guideline to show how DFV issues may present are real and have been provided by RSPs and stakeholders. All identifying information has been removed.

Note: Using this guideline - structure and copyright

This Guideline is designed to provide practical guidance to assist RSPs to develop or enhance their DFV policies, systems, and supporting material. Smaller organisations may find it particularly useful to follow the structure of this Guideline when writing their own DFV Guidelines and/or to include sections of this Guideline in their own policies.

Communications Alliance grants permission for parts of this Guideline, including case studies, to be used in full in RSPs' own Guidelines, with appropriate acknowledgment. For Communications Alliance review and research purposes, it is requested that you advise Communications Alliance of such use by emailing info@commsalliance.com.au.

1.2. Objectives

1.2.1. The objectives of the Guideline are to:

(a) raise RSPs' awareness of DFV and how it may present for telecommunications consumers;

(b) assist RSPs in acknowledging the responsibilities, issues and challenges faced by their organisations when dealing with DFV;

(c) understand and manage DFV matters within the context and constraints of other telecommunications industry legal and regulatory obligations; and

(d) provide a framework and range of best practice recommendations to assist RSPs in developing and implementing – or if already in place, updating and enhancing – policies, systems, tools, and processes that safely and appropriately:

(i) support people affected by DFV; and

(ii) educate, train, and support staff.

1.2.2. The objectives of each chapter are summarised at the start of each chapter.

Note: definition of domestic and family violence – and other key terms

It is critical that RSPs understand the full scope of behaviours and scenarios covered by the shorthand term 'domestic and family violence' and DFV. Refer to Chapter 2: Terminology, definitions and acronyms, for more comprehensive definitions and context.

1.3. Scope

1.3.1. The Guideline is designed to cover the following:

(a) all presentations of DFV.

(b) all telecommunications services (e.g. mobile and fixed) and products (e.g. prepaid or post-paid). However, some guidance may relate to specific service or product types.

(c) residential and small business *consumers*.

1.3.2. Without aiming to narrow its application, advice in this Guideline is focused on DFV as it most commonly presents in connection with telecommunications products and services.

1.3.3. The Guideline cannot and does not attempt to guide RSPs' customer service-response in every DFV scenario; certain DFV situations are most appropriately and safely dealt with by referral to a specialist DFV service.

Additional information on referral resources is provided in Appendix 1: Referral resources for *consumers*.

Note: support for large business, enterprise and government customers

While this Guideline focuses on RSPs servicing residential and small business *consumers*, carriage service providers need to consider what support they offer for their large business, enterprise, and government customers, where the *affected person* is the *end user* of a telecommunications service provided to them by their employer.

RSPs also need to consider how to support their own employees affected by DFV.

Information about employer obligations in relation to DFV, including tools and tips, is available on the Fair Work Ombudsman's website.

1.4. How to use this Guideline

1.4.1. This Guideline is intended to develop or enhance individual RSPs' approaches when managing DFV matters.

1.4.2. It is recommended that this Guideline is read in its entirety before developing or reviewing organisational-specific policies and supporting materials.

1.4.3. This Guideline should be read in conjunction with:

(a) legislation and regulation (mandatory), including the current versions of:

(i) the *Telecommunications Act 1997* (Cth);

(ii) the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth);

(iii) the *Competition and Consumer Act 2010* (Cth);

(iv) the *Privacy Act 1988* (Cth);

(v) the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*;

(vi) the *Telecommunications (Financial Hardship) Industry Standard 2024*; and

(vii) the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017*.

(b) industry codes (mandatory):

(i) C628 Telecommunications Consumer Protections (TCP) Industry Code;

(ii) C525 Handling of Life Threatening and Unwelcome Communications Industry Code; and

(iii) C556 Number Management – Use of Numbers by Customers Industry Code.

(c) guidelines and guidance notes, including:

(i) ACCC industry guide: "Consumer vulnerability: A business guide to the Australian Consumer Law", November 2021*;

(ii) ASIC, ACCC industry guide: "Debt collection guideline: for collectors and creditors", April 2021*;

(iii) ACMA industry guide: Statement of Expectations for Vulnerable and Disadvantaged Consumers, May 2022;

(iv) IGN 010 Communications Alliance Industry Guidance Note: Customer Process – Handling of Life Threatening and Unwelcome Communications;

(v) IGN 017 Communications Alliance Industry Guidance Note: Authorised Representatives and Advocates;

(vi) ASIC, ACCC consumer guide: "Dealing with debt collectors: your rights & responsibilities", December 2020; and

(vii) IGN 013 Communications Alliance Industry Guidance Note: Sales Practices and Credit and Debt Management.

Additional resources are provided in Appendix 2: Support resources for RSPs.

Note

Relevant clauses of obligatory documents are referenced in respective sections of this Guideline. The term 'must' is only used where it relates to an obligation associated with a mandatory instrument.

* Suppliers must 'have regard' to these guides under the TCP Code.

1.5. Guideline review

1.5.1. The Guideline is intended as a living document and changes may be considered at any time to ensure it remains useful and relevant. The need for a complete revision will be assessed on the advice of the Communications Alliance Industry Consumer Advisory Group (ICAG) at least every two years.

1.5.2. Minor updates will be managed through the ICAG as required.

1.5.3. Comments or questions are welcomed at any point and should be directed to Communications Alliance: info@commsalliance.com.au.

2. TERMINOLOGY, DEFINITIONS AND ACRONYMS

2.1. Terminology

2.1.1. The terminology used to identify and describe violence and abuse between intimate partners, immediate and extended family, communal and kinship relationships, and carer and guardianship arrangements is diverse, with no consistency nationwide on its scope and use.

2.1.2. All terms used in the Guideline are defined in clause 2.2: Definitions. For clarity, key terms used in the Guideline are italicised and linked to their complete definitions the first time they are used in each clause or section.

2.1.3. Where telecommunications-specific terminology is used, unless otherwise stated, definitions align with the meanings defined in the TCP Code.

The importance of language

Communications Alliance acknowledges the importance and complexity behind the language used to identify and describe the different types of abuse, the different relationships affected by abuse, and the different parties to that abuse.

Categorisation of abuse is a naming convention. It is not intended to limit any response to DFV or its presentation. There are shared characteristics across all forms of abuse, there is often more than one 'type' of abuse occurring at once, and some terms are used interchangeably.

The key characteristic is the use of power, control, and coercion by one party against another to create a dependency, isolate, monitor, or control over them.

Terms such as 'domestic violence', 'domestic and family violence', 'family violence', 'domestic harm', 'domestic abuse', 'domestic control', 'elder abuse', 'abuse of older people', 'carer abuse', 'violence against women', 'gender-based violence', 'coercive control', and 'intimate partner violence' are often used, some interchangeably, some to refer to specific abuse types. Other presentations of DFV include economic and financial abuse, technology-facilitated abuse, cultural and religious abuse and animal abuse.

The terminology to describe the parties to domestic and family violence is similarly fraught, with common descriptors including 'victim', 'survivor', 'victim-survivor' on one side, and 'perpetrator', 'offender', 'abuser', 'person using violence' on the other.

All definitions have their pros and cons. None is perfect.

The definitions used throughout the Guideline were agreed after much deliberation to:

- take account of the significant work done by others to analyse and consult on terminology;
- be directly relevant to the telecommunications sector and its regulatory environment;
- be consistent with the terminology used in the earlier version of this guideline as much as possible (while noting that the term DFV is now defined to cover a wider range of abuse types more clearly, including abuse of older people and the abuse of people living with disability) – see clause 2.2: Definitions; and
- be gender-neutral and inclusive.

2.2. Definitions

In this Guideline:

Act

means the *Telecommunications Act 1997* (Cth).

Advocate

means a person nominated by a *consumer* to deal with an RSP on the *consumer's* behalf. An *advocate* cannot make changes to the *consumer's* account without the *consumer* being present (either physically, on the phone, or digitally) and agreeing to such action. The *advocate* can discuss the *consumer's* account without the *consumer* being present.

Affected person

means a person that has been affected by *domestic and family violence*. The *affected person* may be the *consumer*, *customer* or *end user*, including prospective, current, and past telecommunications service users.

Authorised representative

means the person who has authority from a *consumer* to deal with an RSP on their behalf. This includes the power to make changes to the *consumer's* account without the *consumer* being present.

Carriage service provider

has the meaning given by section 87 of the *Act*.

Carrier

has the meaning given by section 7 of the *Act*.

Coercive control

describes a pattern of behaviour by a person(s) to dominate, manipulate and control another person, thereby depriving that person of their freedom and sense of autonomy.

Consumer

has the meaning given by clause 2.1 of the TCP Code. This meaning includes residential and small business *consumers* (as defined in the TCP Code).

Customer

means the person who has a contract with the RSP. This can be an individual or a small business. A reference to a *customer* includes a reference to their *authorised representative*.

Domestic and family violence

refers to a wide range of behaviours by a person(s) designed to create a dependency or to isolate, monitor, dominate, or control another person.

The term 'domestic and family' does not seek to limit the definition to the immediate family or the domestic home. Abuse and violence occur within many personal relationships – intimate partners, immediate and extended family, communal and extended kinship relationships, and carer and guardianship arrangements.

'Violence' in this context consists of physical violence and other types of abuse that cause harm. Examples of abuse include *life threatening communications*, *unwelcome communications*, *economic and financial abuse* and *technology-facilitated abuse*.

Economic and financial abuse

is a form of DFV and includes actions by a perpetrator to exploit an *affected person's* economic or financial position and reduce self-sufficiency.

End user

means the person using a telecommunications service. An *end user* may or may not also be the *customer*. A reference to an *end user* includes a reference to their *authorised representative* or *advocate*.

Life threatening communication

has the meaning given to it by C525 Handling of Life Threatening and Unwelcome Communications Industry Code.

Long term assistance

has the meaning given to it by the *Financial Hardship Standard*.

Perpetrator

means the person(s) using *domestic and family violence* against an *affected person*.

Retail carriage service provider

means a *carriage service provider* that provides telecommunications products and services to *consumers*.

Rights Of Use Holder

has the meaning given in C556 Number Management – Use of Numbers by Customers Industry Code, or the equivalent Number Management Rules Part 1 – Use of Numbers by Customers, as part of an industry-managed numbering scheme.

Short term assistance

has the meaning given to it by the *Financial Hardship Standard*.

Technology-facilitated abuse

is an all-encompassing term to describe a form of DFV where technology (which may include telecommunications services) is used to control, intimidate, threaten and harass.

The abuse can present in many ways, ranging from the perpetrator simply withholding or restricting the affected person's access to services or making unwelcome contact via a communications device to the sophisticated use of the technology to facilitate abuse such as cyberstalking or digital impersonation.

Trauma-informed response

means a response developed with an awareness of the signs and symptoms of trauma, with supporting material in place to handle the issues safely while reducing the risk of re-traumatisation (either of the affected person and/or any staff involved in any DFV response).

The five guiding principles of a trauma-informed response are (1) safety (physical and emotional); (2) choice; (3) collaboration; (4) trustworthiness; and (5) empowerment.

Unwelcome communications

has the meaning given to it by C525 Handling of Life Threatening and Unwelcome Communications Industry Code.

Vicarious trauma

is the impact of ongoing, indirect exposure to other people's trauma, including repeated exposure to the details of traumatic circumstances or events. Indirect exposure to trauma can have the same harmful effect on health as experiencing trauma directly.

2.3. Acronyms

ACCC

means the Australian Competition and Consumer Commission.

ACMA

means the Australian Communications and Media Authority.

ASIC

means the Australian Securities and Investments Commission.

DFV

means *domestic and family violence*.

MMS

means Multimedia Message Service.

RSP

means retail Carriage Service Provider.

ROU

means Rights of Use.

SMS

means Short Message Service.

TIO

means the Telecommunications Industry Ombudsman.

3. RECOGNISING DFV IN THE TELECOMMUNICATIONS SPACE

Summary

It can be challenging to recognise DFV, particularly as those affected may not recognise themselves as a victim or survivor.

The information in this chapter is designed to complement specialist staff education about how to recognise and deal with DFV. It begins by looking at possible 'red flags' that may indicate that a consumer is affected by DFV. It then describes the more common abuse 'types' as they present to RSPs. Case studies provide illustrated examples.

Information for RSPs about how to address or reduce the risk of abuse is provided in the chapters following.

3.1. Indicators of domestic and family violence

3.1.1. In addition to disclosures that clearly and unequivocally reference DFV (e.g. 'I'm escaping domestic violence'), any indication that a *consumer* is concerned about their privacy or safety could be a 'red flag' for DFV. Examples may include *consumers*:

(a) mentioning that they are a party to a protection order*;

(b) enquiring about the disclosure of information to another person on the account;

(c) appearing concerned about any suggestion or requirement to involve another party to the account in any discussions or communications (note that this can extend to concern about the involvement of an *authorised representative*);

(d) indicating that they are facing financial difficulty or hardship due to the actions of another party;

(e) remaining silent during a sale or account enquiry while another party does all the talking;

(f) raising concerns about another person's ability to monitor their calls, SMS or other communications;

(g) enquiring about changing numbers, requesting to block specific numbers, or asking how to stop unwelcome communications;

(h) expressing concern or asking questions about the ability of another party to track their location through their device;

(i) raising questions or concerns about the installation of spyware on their device; or

(j) being concerned about any suggestion that their physical address should be recorded.

***Note: protection orders**

RSPs should be aware that that there are alternative terms for protection orders, such as 'intervention order', 'domestic violence order' or 'apprehended violence order', that may be used by affected people. This reflects the various names for protection orders across different jurisdictions in Australia.

3.2. How DFV may present to an RSP

3.2.1. This section describes the more common abuse 'types' as they present to RSPs, with illustrated examples provided through case studies. This information should be read in conjunction with the succinct descriptions of each abuse type provided in the linked definitions.

Coercive control

3.2.2. *Coercive control* may present as a perpetrator:

(a) forcing the *affected person* to add the perpetrator as an *authorised representative* on the *affected person's* account;

(b) restricting the *affected person*'s access to telecommunications services. This may be through physical action (e.g. removing a device, disconnecting an internet connection) or non-physical means (e.g. screen time limits or restrictions, abuse of parental controls on devices);

(c) forcing the *affected person* to sign up for devices or services for others (see also *economic abuse*);

(d) using telecommunications services to monitor the *affected person*'s movement, calls, communication, internet usage, etc.; or

(e) using a third party to control or manipulate the *affected person* (e.g. threatening a child/access to a child in joint custody, having the third party send *unwelcome communications*).

Case study: *coercive control*

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 telecommunications contracts with multiple telecommunications providers. They went from store to store signing up to numerous telephone services, smart watches and iPads. Sabreen only agreed to sign the contracts in her name because of the intimidation and threats of further violence. She remained silent during the entire sales process.

Sabreen's husband subsequently sold all the devices online. She received no benefit from the contracts and had no information about whereabouts of the handsets.

(Case study provided by an RSP)

Physical violence or harm and life-threatening communications

3.2.3. Physical violence or harm *and* *life-threatening communications* may present as the *perpetrator*:

(a) committing actual physical violence or harm to the *affected person*;

(b) seeking to intimidate and induce fear through the threat of physical violence or harm;

(c) making a *life-threatening communication* via a telecommunications service (call, SMS or MMS) or enabled by a telecommunications service (social media, email, messenger apps etc.). This communication may lead a person to believe, on

reasonable grounds, that action is required to prevent or lessen a serious and imminent threat to the life or health of an *affected person*.

Note: *life threatening communications*

Examples of *life-threatening communications* are listed in C525 Handling of Life Threatening and Unwelcome Communications Industry Code and include an event such as a person being seriously injured; a bomb threat; an extortion demand; a kidnapping; and a threat to public safety.

Case Study: life-threatening communications

Hamish was in an abusive marriage. When the relationship ended, the perpetrator remained in the family home, while Hamish and their three children moved to live with his parents.

The perpetrator makes daily threats, by SMS and phone, to take the children. A protection order is in place; however, the perpetrator continues to send Hamish up to 200 messages a day. He constantly feels threatened and has ongoing concerns for the children's safety.

(Case study provided by Relationships Australia)

Technology-facilitated abuse and unwelcome communication

3.2.4. *Technology-facilitated abuse* may present as:

(a) *unwelcome communications* (calls, SMS, MMS, social media, messenger apps, sharing pictures and video recordings.);

(b) physical and/or cyber stalking;

(c) sharing harmful content (e.g. sharing intimate personal images or videos);

(d) restricting access to telecommunications products and services;

(e) digital impersonation or identity theft; or

(f) unauthorised access to online accounts.

3.2.5. RSPs can be important sources of information and evidence of technology-facilitated abuse.

3.2.6. RSPs must act cooperatively to investigate and prevent the use of a telecommunications service to make unwelcome communications (see Chapter 8: Account management and security). This includes specific protections for the management of DFV *unwelcome communications*.

Case study: unwelcome communications

April called her RSP and asked questions about how she could block certain phone numbers - including private or unknown numbers - from contacting her. During the conversation, April was short of breath, spoke quickly and sounded close to tears.

As the call continued, April disclosed that she has been getting multiple unwanted messages and calls from a person that she does not want to have any further contact with. April advised that she is "at my wit's end with this" and wants to change numbers. However, she's worried that this would cause problems with family, friends, and work.

(Case study provided by 1800 RESPECT)

Economic and financial abuse

3.2.7. *Economic and financial abuse* may present where the *perpetrator*:

(a) controls access to finances, income, and employment;

(b) may have influenced or coerced the *affected person* to take on debt or to put financial obligations in their name; or

(c) refuses to pay bills or provide money for living expenses for the dependent *affected person*. This may include dependent children, a financially dependent intimate partner, immediate and extended family, communal and kinship member or carer or guardianship arrangement.

Case study: *economic abuse*

Suzette, a woman in her mid-seventies, received a bill that included services that she did not know she had signed up for. Suzette asked her RSP whether a mistake was made, explaining that she does not use her device for anything more than calling and texting, so would not sign up for additional services.

In discussions with her RSP, Suzette discloses that her son manages her finances, with bills coming out of her bank account. She admits that he had signed her up for services (that she didn't request) in the past, but that it was for a shared service and that she is sure he wouldn't have done it again. However, she is unable to ask him directly because he has told her not to contact him during working hours. Suzette sounds tearful on the phone and asks the RSP's staff to "please don't contact my son about this?".

(Case study provided by 1800 RESPECT)

3.3. Understanding and accepting limitations

3.3.1. While RSPs should attempt to recognise and respond to potential DFV flags, they also need to recognise their limitations and understand:

(a) how and when to refer to a specialist DFV support service. This is critical for both the safety (physical, emotional, mental health) of the *affected person* and the staff member managing the contact; and

(b) that even with the best systems and processes in place, they may not be able to identify every *affected person*. The challenge may be particularly marked when the *affected person* may not recognise certain behaviour as DFV and may not identify with the label of 'victim', 'survivor', 'abuse' or 'violence'. A mix of reactive and proactive DFV policies will enable RSPs to support the *affected person* appropriately.

See also Chapter 6: Developing a DFV policy.

4. ORGANISATIONAL CULTURE AND STAFF STRUCTURE

Summary

To ensure an efficient, effective and safe response to DFV, RSPs need to consider how DFV issues will be managed and supported within their organisation.

This chapter considers the importance of organisational culture and looks at how RSPs can ensure that DFV issues are appropriately considered in staff structure.

4.1. Organisational culture: championing the cause

4.1.1. Managing DFV is a company-wide issue. Therefore, it is essential that DFV policies and processes fit the company, and are understood, supported, and championed from the CEO level down.

4.2. Staff structure

4.2.1. RSPs need to ensure that DFV issues are evaluated in their organisational staff structure, with responsibilities, reporting, support, and communication relationships clearly defined and customer touchpoints for DFV (e.g. financial hardship) considered.

4.2.2. Appropriate arrangements will depend on the RSP's structure and size. Options may include (but are not limited to):

(a) Creating/developing a dedicated, specialised DFV team to:

(i) receive and manage all DFV cases (with support from other business areas as required); or

(ii) provide specialist advice and assistance to front-line staff handling DFV cases.

(b) Identifying a specialist DFV staff member to receive and manage or assist with DFV cases (as above); or

(c) a hybrid model whereby the RSP's financial hardship team manages DFV-linked financial hardship cases, either by specialists within that team or with support from the specialist DFV team (noting that not all DFV cases will have a financial hardship element).

4.2.3. RSPs must ensure that specialist staff have the authority and training to resolve matters effectively, efficiently, and appropriately, in line with TCP Code obligations.

Note: the impact of gender when supporting an *affected person*

RSPs should be aware that an *affected person* may not want to communicate with staff of a specific gender. Specialist teams should, therefore, ideally include a mix of genders.

4.3. Case management

4.3.1. The safety and security of the *affected person* is paramount. Therefore, processes and procedures should be designed to:

(a) safeguard the *affected person's* connection to a telecommunications service;

(b) avoid or minimise the need for the *affected person* to constantly repeat their story (keeping the customer journey as stress-free as possible).

4.3.2. There are several ways to safeguard connection and minimise the need for repetition, including:

(a) allocating a specific customer representative contact to each DFV case and providing the affected customer with the direct contact details of this representative. Alternatively, a buddy system could be set up to allow more than one staff member to be across an *affected person's* case. (This option provides for staff members to support each other.);

(b) discreetly flagging relevant customer files to show that they are being case managed; and

(c) specifying that a specialist team automatically and discretely manages all case-managed matters.

Note: record keeping considerations

It is strongly recommended that any customer account records that may be easily accessed do not identify the *affected person's* specific circumstances, to minimise the risk that the perpetrator is alerted to anything. This may include keeping a separate customer service record for the DFV matter.

As with other aspects of DFV management, it is important to ensure that the *affected person* is comfortable with arrangements, and that their safety and privacy are appropriately considered. Some people may be uncomfortable with any information on their situation being associated with their account and would prefer to re-explain their circumstances on each contact to avoid the risk of records being accessed by a perpetrator. RSPs should be guided by the directions of the *affected person*.

5. STAFF TRAINING AND SUPPORT

Summary

A safe, efficient and effective response to DFV requires staff are properly trained and supported.

This chapter begins by looking at RSPs' legal and regulatory obligations in this space, both to their staff and to their customers. It then considers the recommended training and support mechanisms to achieve best practice in this area.

5.1. Overarching obligations

5.1.1. Under Australian workplace health and safety (WHS) laws set out in the *Work Health and Safety Act 2011* (Cth), RSPs (as far as is reasonably practicable):

(a) must ensure the health and safety of their workers while at work; and

(b) must not put other people at risk from work carried out as part of the conduct of their business.

5.1.2. To fulfil this obligation, it is essential that an RSP's DFV policies and processes are supported by appropriate training and supervision and that the staff's health and well-being are monitored.

5.1.3. The TCP Code extends obligations towards vulnerable customers by requiring RSPs to interact with disadvantaged or vulnerable *consumers* appropriately, courteously, and in a fair and accurate manner.

5.2. Company-wide training

5.2.1. RSPs should deliver dedicated DFV awareness training to all staff during onboarding, with annual refreshers.

5.2.2. This training should:

(a) embed DFV policy, procedure, and supporting materials into practice in a *trauma-informed* manner;

(b) discuss the nature and impact of DFV and provide opportunities for informed staff discussion (in a tailored, sensitive, and culturally safe way), with a focus on how DFV relates to telecommunications services;

(c) include information about how to recognise common forms of DFV associated with a telecommunications service;

(d) address how staff should manage and respond to DFV-associated issues that may arise, and know:

(i) when and how to escalate matters; and

(ii) how and where to seek support.

(e) guide staff on how to remain impartial and non-judgemental and understand unconscious bias; and

(f) educate staff on internal escalation, support, and assistance pathways, including support available to them as employees (see also clause 5.5 Staff support).

5.3. Specialist staff training

5.3.1. RSPs should ensure company wide DFV training is supplemented by tailored DFV training appropriate to specific staff roles and responsibilities, including for:

(a) frontline customer service staff;

(b) specialist DFV staff; and

(c) staff working in areas likely to deal with DFV-related issues (e.g., sales, credit, collections, financial hardship, fraud, privacy, and escalated complaint management).

5.3.2. In addition to issues covered in the business-wide training, frontline staff training should (as appropriate to their role):

(a) include training on recognising and responding to life-threatening communications (including calling Triple Zero);

(b) ensure staff are familiar with checklists, processes and procedures designed to empower and educate *affected persons* about DFV-related risks associated with their communications services and options to address them;

(c) include training, guidance and support on *vicarious trauma*. This should include information about how to recognise and reduce the risk of experiencing it, as well as ensuring staff are aware of and have access to appropriate support systems;

(d) ensure staff understand the specific legal and regulatory obligations relevant to their role as it relates to DFV (e.g. the management of financial hardship requests for the *affected person*); and

(e) support staff to understand the boundaries and scope of their role, including providing resources to enable staff to provide referrals to appropriate support providers (see also Appendix 1: Support resources for consumers).

Note: free and unbilled calls to support services

Some RSPs offer some of the referral resources listed in Appendix 1: Support resources for consumers as a free and unbilled call (meaning a call will not appear on the customer's invoice or usage history).

This is a safety feature and RSPs providing this service should advise their customers of this feature accordingly.

Note that for the *affected person's* safety, RSPs should also recommend that the *affected person* also deletes the call from the call history on their device.

5.4. Training development and delivery

5.4.1. It is strongly recommended that RSPs work with a reputable training provider with DFV expertise to develop and review DFV staff training. This will allow material to reflect both current best practice on DFV-specific issues and the RSP's company-specific needs (e.g. to support the RSP's policy and supporting materials).

A list of DFV training providers is found in Appendix 3: Training resources for RSPs.

5.5. Staff support

5.5.1. Dealing with DFV is challenging and can threaten staff's well-being, including through *vicarious trauma*. To fulfil their duty of care to ensure that staff are safe at work, RSPs must ensure that DFV-related support is available to all employees, including (but not limited to) frontline customer service staff.

5.5.2. It is strongly recommended that RSPs seek advice from/consult with Human Resource experts and external DFV specialists when developing or reviewing their staff support options.

5.5.3. Staff support should be included as a compulsory, routine component of all processes to ensure that staff's mental well-being is actively managed. In addition, policies and procedures should clearly articulate how additional support can be accessed.

5.5.4. It is strongly recommended that RSPs ensure all staff have access to counselling services or an Employee Assistance Program. To maintain employee privacy, access to the service should be anonymous. This includes ensuring that individuals are not named when issuing accounts for payment.

5.5.5. Appropriate support arrangements for specialists will depend on the RSP's size and organisational staff structure. However, the following principles/options are likely to be relevant to all RSPs:

(a) staff should be able to 'opt out' of dedicated support roles associated with managing DFV matters;

(b) support to staff should be provided proactively and should be separate from any day-to-day supervision;

(c) support should be easily accessible and include an internal support option. For example, RSPs may set up a buddy system for specialist staff to ensure that they have a 'go to' person within the organisation to 'download to' and seek support and guidance from*;

(d) external support options from specialist DFV providers should be considered in addition to internal support. This ensures access to neutral, third-party support, as well as specialist expertise;

(e) preventative activities through the delivery of pro-active mental health initiatives (for RSP staff offering DFV specialist support and/or all staff) to mitigate the risk of harm;

(f) careful workforce planning is critical to ensure appropriate rostering (e.g., enough staff, with proper skill mix), frequency of scheduled breaks and flexibility to take breaks when needed, and maintenance of leave balances; and

(g) RSPs may consider providing spaces such as quiet rooms or gaming rooms, allowing staff to leave their desks and focus on something else.

*** Note: internal support for staff**

For organisations with more than one DFV-specialist, a buddy is likely to be another specialist. Where there is no other specialist to buddy with, an appropriate buddy would likely be a manager/supervisor.

6. DEVELOPING A DFV POLICY

It is essential that RSPs have their own company specific DFV policies and supporting material to ensure a safe and comprehensive DFV response that fits their size and structure. This should be supported by regular staff training.

This chapter starts by looking at the overarching principles and considerations that should apply when dealing with DFV. It then outlines key components included in DFV policies, procedures and processes.

6.1. Company-specific policies and supporting materials

6.1.1. RSPs should develop company-specific policies and supporting materials for dealing with DFV. Recommended resources include:

(a) a corporate-level policy that sets out the RSP's expectations for supporting and managing DFV;

(b) process documentation that outlines the support and assistance that should be offered to consumers that are, or are suspected by the RSP to be, affected by DFV;

(c) procedures for the frontline and specialist staff to work through to ensure that account, safety, privacy, and confidentiality risks are reviewed and options for managing them are discussed and agreed upon with the *affected person*;

(d) a checklist for support staff to follow and to use to record agreed and completed actions to ensure a comprehensive and methodical response; and

(e) a mix of mandatory and recommended scripts to enable a consistent response to identified problems when and if appropriate.

Note: using scripts

Scripts and similar resources are likely to be only relevant at point-of-first contact, for high-level interactions between an affected person and generalist staff.

Scripts are generally not recommended for DFV-specialist staff who should have the training and autonomy required to allow them to take a flexible, customer-led and *trauma-informed* approach.

6.1.2. Policies and supporting materials should:

(a) emphasise safety;

(b) be *trauma-informed*;

(c) ensure that responsibilities, communication channels, support, and escalation requirements (external and internal) are clear; and

(d) link and reference mandatory consumer obligations. RSPs should be aware that people affected by DFV are vulnerable. RSPs must ensure their response is aligned with their obligations under the TCP Code (see also clause 7.2: Accessing support and assistance).

6.1.3. It is strongly recommended that a staff member with specialised training in DFV and/or an external DFV specialist provides input to and regularly reviews and updates policies and supporting material. This assists the development of a DFV policy that is appropriate, supportive and effective for the RSP and its consumers and staff.

A list of support resources for RSPs, including DFV specialist services that can assist with policy development and supporting materials, is provided in Appendix 2: Support resources for RSPs.

6.2. Safety

6.2.1. All internal support material must emphasise that safety is always the priority.

See also clause 5.1: Overarching obligations.

Life threatening situations

6.2.2. Where there is concern about the immediate physical safety of the *affected person*, staff or the public, the RSP must escalate the situation to emergency services.

6.2.3. RSPs must know their legal and regulatory obligations to respond to *life threatening communications* under C525 Handling of Life Threatening and Unwelcome Communications Industry Code. Policies and supporting materials must appropriately reflect these requirements.

Case study: *life threatening and unwelcome communications*

Janette experienced psychological, emotional, financial, and physical abuse, culminating in a physical attack on her in October 2021. Following this attack, the perpetrator continued to send abusive text messages, up to 30 times each day.

Janette's case worker contacted her RSP to see what support could be offered.

Janet's RSP referred to its unwelcome communications policy and procedures and engaged with the perpetrator's RSP. It established that the pattern of unwelcome communications matched the conditions described under the relevant Code and took action accordingly. After a series of warning letters and based on continued unwelcome communications, the service of the perpetrator was suspended by their RSP.

(Case study provided by an RSP)

Unwelcome Communications

6.2.4. RSPs must know their legal and regulatory obligations to respond to *unwelcome communications* under C525 Handling of Life Threatening and Unwelcome Communications Industry Code. Policies and supporting materials must appropriately reflect these requirements.

6.2.5. Staff should be trained to recognise a pattern of *unwelcome communications*. This means communications that can be confirmed by the RSP and:

(a) are made regularly;

(b) occur ten or more times in a 24-hour period;

(c) occur three or more times over a period of more than 24 hours and less than 120 hours; or

(d) a *consumer* has brought to the attention their RSP, and which their RSP and the A-Party Supplier agree, have been made regularly.

Communicating with the Consumer

6.2.6. It is essential that responses to DFV are consumer-led; the *affected person* knows best how to keep themselves safe, and RSPs should seek their advice on how and when they wish to be contacted.

6.2.7. It should be easy for an *affected person* to contact their RSP.

See also Chapter 7: Customer access to assistance and support.

6.2.8. Where possible, RSPs should avoid initiating contact with the *affected person* unless they have specifically requested a call (e.g. at an agreed time).

6.2.9. For voice calls, RSPs should always check with a 'yes/no' question whether it is safe to talk. This should apply even when calling at a previously agreed time - be mindful that circumstances change, and the perpetrator may unexpectedly be present.

6.2.10. RSPs should check with the *affected person* to confirm a safe and secure contact method before leaving voice messages or sending any written communication (SMS, emails, etc.). This includes, but is not limited to:

(a) sharing fact sheets or tips on safety;

(b) any information relating to a new account; and

(c) automatic communication (email, SMS etc.) sent to acknowledge a customer's interaction with the RSP or any other communication that may alert a perpetrator to the *affected person's* plans or attempts to break away from the abuse in any way.

See also clause 7.3: Customer authentication requirements.

See also Chapter 8: Account management and security.

Note: safety considerations when contacting an *affected person*

Any RSP contact with an *affected person* has the potential to alert the perpetrator that the victim speaking about the abuse and/or attempting to escape from the abuse – and that others are aware of the abusive situation. It is, therefore, a critical safety issue to ensure that all communications are safe and secure.

Be mindful that an *affected person's* safety profile may change minute-to-minute; staff should consider confirming with the *affected person* if it is still safe to talk if they suddenly start behaving differently, stop communicating or answer questions differently.

Communication with an *authorised representative* or *advocate* may be a safer option (see also Chapter 7: Customer access to assistance and support).

RSPs should also be aware that the *affected person* may be difficult to contact if they are in the process of escaping a situation and do not yet have access to a secure phone or a physical or email address. RSPs should ensure that they can safely accommodate such situations, recognising that all outward-bound (RSP to consumer) communications may need to be actively managed.

7. CUSTOMER ACCESS TO ASSISTANCE AND SUPPORT

Summary

People affected by DFV need to be able to contact their RSP easily and safely for help and support. It can be challenging for someone impacted by DFV to disclose abuse, but they are more likely to feel comfortable doing so if they know that their RSP has processes and support in place and will offer a safe and sympathetic response.

This chapter considers how RSPs can facilitate safe and easy contact for *affected persons*. It covers contact mechanisms and support (including the use of advocates and translators) and case management issues (including challenges with account verification and authorisation).

7.1. Proving visible, safe and easily accessible support

7.1.1. RSPs should use all relevant channels to inform the public about the support available to people affected by DFV. For example:

(a) **website**: prominently publishing information on their website about:

(i) their DFV policy,

(ii) how to contact them for assistance; and

(iii) available external support resources.

See also clause 7.1.6(a).

(b) **retail:** displaying information about DFV in-store and making hard and soft copies of their DFV policy available to any *consumer* who asks for it.

(c) **contact centre:** prominently publishing information about specialist DFV contact channels and support resources.

7.1.2. RSPs should advise DFV support services and advocacy groups of the specialist DFV contact channels and support resources available.

7.1.3. A range of contact channels should be available to facilitate quick, easy, accessible, inclusive and direct contact between an RSP and an *affected person.* Options may include:

(a) a specialist phone support number;

(b) a dedicated web form with a 'call back' option;

(c) a specialist chat function or chatbots;

(d) email; and

(e) retail support - if safe and viable.

Note: automated phone systems

Automated phone systems can be difficult for people affected by domestic and family violence to use, as they often require the caller to enter identifying information (or access a device) that they no longer have access to (for example, if they have fled, leaving documentation at home).

Dedicated contact mechanisms are recommended to allow direct access to a DFV specialist who has the authority and training to be able to manage the situation appropriately.

7.1.4. RSPs should take a 'no wrong door' approach to people affected by DFV. This means if an *affected person* makes contact via a general contact channel (rather than the specialist DFV contact channel), RSPs should develop processes to ensure a warm transfer of the *affected person* to the appropriate team for support, thereby avoiding the need for the customer to repeat their story. In addition to minimising the contact time (a safety issue), this avoids possible trauma to an *affected person* from needing to repeat their circumstances.

7.1.5. Where no dedicated contact channel exists, it is strongly recommended that RSPs follow the training recommendations in Chapter 5: Staff training and support to ensure that all staff can provide appropriate support.

7.1.6. The *affected person's* privacy and safety should be considered from the first contact. Therefore, it is strongly recommended that:

(a) webpages and chat functions with any information on DFV include a quick exit button prominently displayed on the page. The *affected person* should also be advised to clear the browser history when exiting the page (with support provided if the affected person is unsure how to do this);

(b) phone calls relating to DFV are free-rated and not identifiable (i.e. calls made to identified services do not appear in usage records, on bills or on invoices), noting that DFV-related call channels may include both calls to the RSP (e.g. to its specialist support line) and calls to external support services (such as those listed in Appendix 1: Support resources for *consumers*); and

(c) staff in retail stores understand and can appropriately manage safety issues when providing information on DFV (e.g. be prepared for a change of subject should a possible perpetrator approach).

See also Chapter 9: Navigating DFV safely through the sales process.

Note: communication and trauma

Trauma can negatively impact an *affected person's* ability to communicate. For example, it can affect the consistency of their communication, how contactable they are, their memory, and their reaction to requests. This may cause delays to responses or actions required by their RSP.

RSPs should, therefore, allow for the impact of trauma in processes and procedures and be understanding and empathetic in all dealings with *affected persons*.

7.2. Access to support and assistance

Responding to undisclosed or unconfirmed DFV

7.2.1. It is strongly recommended that RSPs do not require the *affected person* to disclose DFV or the circumstances of the abuse to their RSP to access DFV support or assistance.

7.2.2. If circumstances of an interaction indicate a *consumer* or *end user* may be affected by DFV, RSPs should proactively offer the same support and assistance they would if DFV was explicitly disclosed.

Evidence and supporting materials

7.2.3. RSPs should accept the word of the *affected person* that they are experiencing DFV and not request additional evidence or details when providing general assistance.

7.2.4. It is strongly recommended that RSPs not require the *affected person* to provide evidence or supporting material of the abuse to access DFV assistance and support.

Exceptions may include instances where legal or regulatory obligations require supporting evidence. If supporting materials (e.g. a statutory declaration or letter from a support service) are required (e.g. during a fraud investigation or when undertaking an ROU change for a service), RSPs should request only the minimum amount of information to enable them to meet their legal or regulatory obligations. Consideration should be given to the re-traumatising impact of any request for supporting materials.

7.3. Customer authentication requirements

7.3.1. All RSPs must comply with the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (*Customer ID Determination*). The *Customer ID Determination* requires RSPs to multi-factor authenticate *customers* before undertaking high-risk transactions on a telecommunications account. How a customer must undertake multi-factor authentication and high-risk transactions are both defined in the *Customer ID Determination*.

7.3.2. As people in vulnerable circumstances (including those affected by DFV) may not have access to materials required for multi-factor authentication, the *Customer ID Determination* outlines alternative authentication options that RSPs must have in place for people in vulnerable circumstances.

7.3.3. Where an alternative authentication option is utilised, RSPs must notify the *customer* that a high-risk transaction has been undertaken. However, where the transaction involves DFV, the *Customer ID Determination* states that this requirement does not apply.

Case study: *using alternative options for customer authentication*

Jo is a woman living with an intellectual disability. Her partner, Daniel, is her primary caregiver and she also has access to a disability support worker who comes every Thursday. Early in their relationship, Daniel offered to help Jo by looking after all of Jo's billing accounts, including for her phone and was added as an authorised representative with her RSP.

At first, this seemed like a good solution. But then Daniel used Jo's computer and phone to log in and change all of her passwords, security questions, and location settings, including the passwords Jo used to access her phone account.

This meant that Jo's access to her phone and internet – her main sources of connection with friends and family outside – was dependent on her staying in a relationship with Daniel. Jo spoke to her disability support worker about how she might go about setting up a new account. However, as Daniel had all of her IDs, paperwork and account information, she was worried that she would be unable to set up a new account without alerting him.

As Jo did not have the required information, her RSP worked with her on alternative authentication options to have her disability support worker appointed her as an additional authorised representative. Once this was completed, Jo and her new authorised representative were able to set up a new account, which allowed her to maintain contact with the people and services she needs. This was done without alerting Daniel of the changes to her old account.

(Case study provided by the eSafety Commissioner)

7.4. Authorised representatives and advocates

7.4.1. RSPs must have processes and systems in place to:

(a) facilitate the appointment of an *authorised representative* or *advocate* for a customer's account; and

(b) ensure that the *affected person* knows their right to be represented by an *authorised representative* or *advocate*.

7.4.2. RSPs must have separate processes for appointing *authorised representatives* and *advocates*, consistent with each role's powers and authorities under the TCP Code. Staff should be trained on these differences.

7.4.3. RSPs should ask the *affected person* whether they wish the *authorised representative* to be the primary contact for the account. This option will benefit *consumers* that need help discussing their account with their RSP safely.

7.4.4. RSPs should be careful to ensure that processes and training emphasise the importance of checking the account's confirmed primary contact before initiating any contact and contacting only the nominated person; contacting the *consumer* directly may place the *affected person* in danger.

Note: obligations to support the use of authorised representative and advocates

It is a TCP Code requirement that RSPs make it easy for *consumers* to appoint and use *authorised representatives* and *advocates*.

Authorised representatives and advocates can provide vital assistance and support to an *affected person* by assisting them manage their telecommunications account. More than one representative or advocate can be appointed to assist in different tasks, with friends, family, translators, domestic and family violence advocates, legal advocates, or financial counsellors all able to be appointed to the roles.

In matters of debt collection, RSPs acting as collectors and creditors must only contact an *authorised representative* if the debtor is represented (TCP Code cl 6.10.1 and Part 2 Section 9 of the ACCC/ASIC Debt Collection Guideline).

Case study: *authorised representatives*

Lee had debts with three RSPs, acquired in circumstances of financial abuse. To help them manage the debts, they sought the assistance of a lawyer to act as an authorised representative on all three accounts.

Two of the three RSPs efficiently managed the request for Lee's lawyer to act has an authorised representative, and promptly dealt with the lawyer's request to waive the money owed due to Lee's circumstances.

The third RSP did not appropriately respond to Lee's request. They failed to properly action Lee's instruction to appoint the lawyer as an authorised representative and refused to communicate in writing with the lawyer. When the lawyer attempted to make phone contact, they were met with long hold times and unhelpful service, with no dedicated contact point and a different customer service representative each time. Despite re-iterating Lee's vulnerability and experience of DFV, the lawyer was unable to make progress.

After 4 months of attempted contact, the lawyer was finally advised that Lee's debt needed to be resolved directly with the debt collection company. No further assistance was offered.

(Case study provided by ACCAN)

8. ACCOUNT MANAGEMENT AND SECURITY

Summary

This chapter looks at the detailed steps that should be taken to review and manage an *affected person*'s telecommunications service to address the common issues presenting in all cases of DFV: privacy, safety, security and financial matters.

The principles of a consumer-led, trauma-informed approach (emphasising empowerment and safety), outlined in previous chapters, apply throughout.

8.1. Maintaining connection

8.1.1. Once an RSP becomes aware of DFV (or potential DFV), it should protect the *affected person's* service(s) from disconnection. This may include, for example, mirroring protections or safeguards in place for financial hardship customers.

See also clause 4.3: Case management.

Note: The importance of maintaining connection

The loss of service is a major disruption for anyone, but for an *affected person* the consequences can be particularly significant and far-reaching.

Disconnection can directly threaten an *affected person's* safety, preventing them from contacting help or support when they need it. It disrupts access to government services, employment, finance and safely support mechanisms, placing the *affected person* in a position of greater vulnerability and disadvantage.

It can also affect issues such as child custody, with Family Courts increasingly requiring parties to use a specified number or family planner app as a method of monitoring interactions in child custody matters. To comply with the court order in such circumstances, an *affected person* must retain access to their service. Interruption of access may place an *affected person* in breach of their Family Court order.

8.2. Identifying appropriate account management options

Overview

8.2.1. To identify and address possible account management, security and privacy concerns associated with an *affected person's* service and the relevant options for addressing them, RSPs should:

(a) confirm whether the *affected person* is the *customer* or an *end user* of the telecommunications service(s);

(b) listen to the *affected person's* concerns about their privacy, safety and security;

(c) briefly discuss other possible security concerns with the account and services as currently set up (see also Table 2: Affected customer account security checklist);

(d) discuss the options available to the *affected person* to protect their privacy and security; and

(e) seek their instruction on how to proceed.

Options for affected customers

8.2.2. Where the *affected person* is the *customer*, options for increasing the security and safety of the services include:

(a) **new account, new service(s):** setting up a new 'clean slate' account, with new service(s) (e.g. a new mobile number) (for further details, see clause 8.4);

(b) **new account, existing service(s):** securing the *customer's* existing service(s) by creating a new, 'clean slate' account and transferring the *customer's* existing service(s) (e.g. their fixed line service) to the new account, (for further details, see clause 8.5);

(c) **existing account, new service(s):** providing a new service(s) in association with an existing account or changing the phone number associated with an existing account (for further details, see clause 8.6); or

(d) **existing account, existing service(s) with security refresh:** refreshing account authorisations and contact information to remove or limit the perpetrator's access and control (for further details, see clause 8.7).

Options (a) and (b) are the most secure options and are, therefore, likely to be the recommended options for most customers.

Options for affected end users

8.2.3. Where the *affected person* is the *end user* and the perpetrator is the *customer*, options for providing a safe and secure service for the *affected person* are limited to:

(a) **new account, new service(s)**: setting up a new 'clean slate' account in the *end user's* name, with new service(s) (e.g. a new mobile number) (for further details, see clause 8.4); or

(b) **new account, existing service(s):** securing the *end user's* existing service(s) by separating it from the current account and providing it under a new 'clean slate' account (for further details, see clause 8.5).

8.2.4. Table 1 (overleaf) summarises account and service set-up options for *customers* and *end users* affected by DFV outlined above. Each option is then described in more detail in the subsequent sections.

Table 1: Customer account management options

Option	Suitable when the *affected person* is the:		Pros	Cons	More information
	Customer	**End user**			
Clean slate accounts	√	√	– Best way maintain privacy, particularly when a new service is also provided.	– Regulatory obligations require ID documents that may be inaccessible to those fleeing DFV.	Clause 8.3
Post-paid			– Enables RSPs to tailor options for supplying a service and device to the *affected person*.	– Credit assessment requirements may be a barrier, depending on the nature of the service they are seeking.	
Pre-paid			– Regulatory exemption processes are available to overcome ID barriers.	– Regulatory obligations require ID documents that may be inaccessible to those fleeing DFV.	
New account, new service(s)	√	√	– Protects the *end user's* privacy: the *perpetrator* won't know the new account and service details.	– Will need to update their contacts with their new phone number(s).	Clause 8.4
New account, existing service(s)	√	√ phone × other services	– No need to change phone number(s) – Enables constant contact with important contacts.	– Perpetrator can continue to harass using the number(s). – Perpetrators may be able to gain access to the new account	Clause 8.5
Existing account, new service(s)	√	×	– Fewer ID and credit assessment barriers – May prevent contact from the *perpetrator*	– Difficult to ensure ongoing account privacy. – high risk of the perpetrator finding out the details of the new service through the existing account. – Affected persons will need to update their number with all important contacts.	Clause 8.6
Existing account, existing service(s) with security refresh	√	×	– Quick, fewest barriers to action	– Difficult to ensure ongoing account privacy – high risk of perpetrators finding out new security details. – Least secure and effective option	Clause 8.7

8.3. Creating a 'clean slate' customer account

8.3.1. It is strongly recommended that RSPs create an entirely new customer account for an *affected person*: a 'clean slate' account. This is the most reliable way of managing the risk of the *perpetrator* gaining unauthorised access to the account or service, as it ensures the *affected person*'s new account is not in any way linked to any older accounts, or any services or security settings associated with either the *affected person* or the *perpetrator* on the RSP's systems.

8.3.2. When setting up a new clean slate account, RSPs should:

(a) take care to ensure that links are not automatically created that connects the new clean slate account to any old accounts (e.g. accounts may be automatically linked by the system where a credit card number or form of identity is recognised as already in the system).

(b) specifically advise the *affected person* to use completely new identifiers when setting up a new clean slate account, to reduce the risk of the perpetrator guessing details and gaining unauthorised access. This means (as applicable):

(i) new contact information, including a new email address;

(ii) new passwords and PINs; and

(iii) new security questions/answers.

(c) take measures to ensure that the perpetrator is not alerted to the creation of the new clean slate account. This may include confirming that automated alerts are redirected or stopped.

8.3.3. The *affected person* should receive information about how to maintain and protect the privacy and security of their new clean slate account, to reduce the risk of unauthorised access.

See also Table 2: Affected customer account security checklist.

8.3.4. RSPs should ensure their policies for the creation of a new clean slate account support continued connectivity for the *affected person*. The most appropriate account structure for each *customer* (pre-paid or post-paid) will depend on their circumstances and preference. The *affected person* should guide RSPs on what is appropriate for their needs.

Note: managing barriers to creating new accounts

When opening new clean slate accounts, RSPs must comply with their regulatory obligations to prove the customer's identity and/or requirements for a credit assessment or credit check.

Meeting these requirements can be problematic for people affected by DFV, as the abuse may mean that they do not have access to their identity documentation; may not have a bank account that is secure and separate from an abusive family member; and may not have a good credit record.

Pre-paid services may be the most viable option for affected consumers unable to overcome banking or credit rating barriers. However, where financial abuse is not a concern, the *affected person* may opt to use post-paid services.

8.4. New account, new service(s)

8.4.1. Where possible, all new services (e.g. a new mobile number or fixed service) should be set up under a new clean slate account. New services can be created following the RSP's usual procedures, following the appropriate security and safety requirements.

See also Table 2: Affected customer account security checklist.

8.4.2. It is recommended that RSPs also provide the following advice to the *affected person* concerning the transition from their 'old' service to their new service (as relevant):

(a) all voice services: advise the *affected person* that copies of voicemails will be lost. An *affected person* may need time to correctly preserve voicemails for use in future, as they may wish to use copies of voicemails to as evidence of abuse.

(b) for mobile services: advise the *affected person* to ensure their contacts are stored securely and not on the SIM of the current service (i.e. ensure contacts are stored on the device or on a cloud service).

(c) for fixed line services: to support the security of their service, advise the *affected person* to update their Wi-Fi router password (i.e. not to leave the password as the 'admin' or default option).

Creating a new post-paid service

8.4.3. Where an *affected person* requests a new post-paid service, RSPs must comply with their TCP Code obligations for the responsible provision of a telecommunication service.

8.4.4. RSPs (and the *customer*) should be mindful that the risk of financial abuse is more significant for a post-paid than a pre-paid service, because of the risk of collections and debt on a post-paid service.

See also Chapter 7: Account management and security.

See also Chapter 9: Navigating DFV safely through the sales process.

Activating a new pre-paid service

8.4.5. Under the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* (the Prepaid Determination), RSPs are required to verify a user's identity before activating a new pre-paid service.

8.4.6. When creating a new pre-paid account, RSPs should ensure that mechanisms are in place to facilitate pre-paid service activation for *affected people* without access to the required identity information.

8.4.7. It is recommended that RSPs offer a complimentary recharge or service credit when first activating the service. RSPs may also consider the provision of a prepaid device. These actions can alleviate financial stress and help address safety concerns while the *affected person* separates their affairs from the *perpetrator*.

Note: exemptions to identity check requirements for prepaid services

RSPs may seek an exemption from the regulator (ACMA) on verification requirements under part 3.2 of the Prepaid Determination.

Alternatively, RSPs can seek approval for a Compliance Plan from the ACMA under Part 5 of the Prepaid Determination for alternative methods for obtaining information and verifying the identity of *customers*.

It is recommended that RSPs discuss the available options directly with the ACMA.

Case study: *connecting a prepaid service, where the* affected person *has no access to ID*

A DFV support worker contacted RSP Blue's DFV team seeking to activate a prepaid mobile service on behalf of their client, an *affected person*. The client's circumstances meant that they were unable to provide ID at the point of activation. The client had not been a customer of the RSP Blue before.

RSP Blue had developed an exemption process for the ID requirements under the Prepaid Determination. The exemption, which had been authorised by the ACMA, allowed the RSP to provide the *affected person* with an additional 90 days to provide their ID documentation. This enabled the *affected person* to maintain a telecommunications service while they gained access to their ID, as. RSP Blue was able to activate the prepaid mobile service and provide the *affected person* with a working SIM (with credit) and a handset.

Over the next month, RSP Blue sent notifications to remind the user that their ID still need to be provided (within the designated timeframe).

(Case study provided by an RSP)

8.5. New account, existing service(s)

8.5.1. Where an *affected person* wishes to keep existing services active (i.e. keep the same phone number), RSPs should have processes in place to facilitate:

(a) moving existing service(s) to a new clean slate account;

(b) support for *end users* of a mobile service moving their existing service(s) to a new clean slate account.

See also Table 2: Affected customer account security checklist.

Note: managing the rights of use of a number(s)

The ability to manage a number - including initiating transfers, ports or disconnections - rests with a *customer* as the *rights of use (ROU) holder*. This means an *end user* cannot manage a number, even if they have used it for years and it is their known contact number with friends, family and support services.

However, there are mechanisms to allow a *customer's* ROU to a number to be terminated and for the number to be transferred to the *end user*. This provides a path for an *affected consumer* to safely retain the number they use, even where they are not the *customer*.

Under section 99 of the *Telecommunications Numbering Plan 2015*: "A carriage service provider may recall an issued number from a customer without issuing a replacement number only if: […] the supply of the carriage service to the customer is otherwise terminated;"

Additionally clause 4.3.3 of C556 Number Management – Use of Numbers by Customers Industry Code sets out: "A CSP may make a Listed Carriage Service subject to terms and conditions as outlined in a Standard Form of Agreement and a breach of these terms or conditions may result in Disconnection of the Listed Carriage Service and the Customer will lose ROU of that Number."

Transferring a service

8.5.2. Where the *affected consumer* is the *customer*, existing services can be moved to a new clean slate account in line with the RSP's usual procedures.

8.5.3. Where the *affected consumer* is the *end user* of an existing fixed line service, the services can be moved to a new clean slate account in line with the RSP's usual procedures.

Transferring an end user's mobile service: managing the rights of use (ROU) of a number(s)

8.5.4. Where the *affected person* is the *end user* of a mobile service (and the perpetrator is the *customer)*, RSPs must manage the separation and transfer of any number(s) in line with their obligations under the *Telecommunications Numbering Plan 2015* and C556 Number Management – Use of Numbers by Customers Industry Code. This means processes must be in place to:

(a) terminate the right to the perpetrator *customer* to use the number(s),

(b) disassociate the number(s) from the perpetrator *customer* account; and

(c) transfer the number to the *affected person's* new clean slate account in line with the RSP's usual procedures.

Additional guidance on managing the ROU transfer and number(s) disassociation process is found in Appendix 4: Separating the Rights of Use of a number.

8.5.5. RSPs should review and, if necessary, modify their Standard Form of Agreement (SFOA) to ensure sufficient arrangements within the SFOA to enable termination and disassociation of mobile number(s) from an account where the *end user* has been affected by DFV by the *customer*.

8.5.6. RSPs may remove a number from quarantine and issue the recalled number(s) in a period shorter than 6 months to an affected person who is the former *customer* or authenticated *end user* (see clause 4.7.2 of C556 Number Management – Use of Numbers by Customers Industry Code.

8.5.7. RSPs holding a churned or ported number in quarantine following disconnection may issue the number(s) to an affected person who is the former *customer* or authenticated *end user* (see clause 4.7.3 of C556 Number Management – Use of Numbers by Customers Industry Code.

Note: do not use a transfer of title or change of ownership process in place of terminating the ROU

The ROU process is different to a Transfer of Title (ToT) or Change of Ownership (COO).

ToT/COO processes are not appropriate solutions for ROU issues for affected *end users*, as the *customer* (the perpetrator) will see the *end user*'s details in the transfer documentation. The *customer* may also prevent the ToT by disputing the transfer.

Case study: *managing the rights of use of a number(s)*

Georgia was subject to years of emotional and financial abuse at the hands of her husband. Her phone number was on her husband's account. It was her main connection to family, friends, and support services (including government services and her bank). When Georgia decided to leave her husband, he called his RSP and had her number blocked so she could not make or receive calls or messages.

Georgia contacted the same RSP when her phone stopped working. The RSP worked with her to restore contact by separating the number from her husband's account and placing it on a new account in her name. The RSP also provided information and support to Georgia to help her keep her new clean slate account and phone service safe and secure.

(Case study provided by an RSP)

8.6. Existing account, new service(s)

8.6.1. Where the *affected person* is the *customer*, a new service can be set up under their existing account.

8.6.2. This option is generally not recommended, as there is a risk that the perpetrator may become aware of/access the new service through the existing account. However, as it is relatively quick and easy to set up (particularly where an e-SIM can be provided), it may be an appropriate solution (or interim solution) in some circumstances.

8.6.3. RSPs providing this solution to *affected persons* should be particularly carefully to review and confirm all account details with the *customer*.

See also Table 2: Affected customer account security checklist.

Changing a customer's number

8.6.4. Where the *affected person* is the *customer*, they may opt to change the public number(s) associated with their account (see clause 4.6 of C556 Number Management – Use of Numbers by Customers Industry Code).

8.6.5. This option is generally not recommended, as there is a risk that the perpetrator may become aware of/access the new number through the existing account. However, as it is straightforward and quick to arrange and can take effect almost immediately (as it does not require a new physical SIM), it may be an appropriate solution (or interim solution) in some circumstances.

8.6.6. RSPs must provide the option for a change of number to a customer affected by DFV at no cost (see clause 4.6.3 of C556 Number Management – Use of Numbers by Customers Industry Code).

8.7. Existing account, existing service(s) with security refresh

8.7.1. Where the *affected person* is the *customer*, they may choose to keep their existing account and service(s). This is likely the least secure option and is not generally recommended. However, it may be appropriate in limited circumstances.

8.7.2. RSPs should work with the *customer* to comprehensively review the account and seek their instruction about how they would like to address (as far as possible) any account vulnerabilities.

See also Table 2: Affected customer account security checklist.

8.7.3. *Customers* should be explicitly advised to use completely new contact and security settings to reduce the risk of the perpetrator guessing security information and gaining unauthorised access.

8.7.4. Care should be taken to ensure any action taken does not place the *affected person* in danger. RSPs should ensure that the perpetrator is not alerted to changes on the account. This may include confirming that automated alerts are redirected or stopped.

See also clause 7.3: Customer authentication requirements.

8.8. Affected customer account security checklist

Table 2: Affected customer account security checklist

Issue	Recommended action
Have any *life-threatening communications* been made?	– Follow the life-threatening communications process*.
What contacts are listed on the account?	– Confirm the required contact details. – Remove the perpetrator and any other contacts as requested.
Who is authorised to make decisions? Are there any *authorised representatives* on the account?	– Confirm authorised representatives for the account. – Remove or cancel authorisations as requested.
Review and update customer security information.	– New passwords and PINs. – New security questions/answers. – Update password on WI FI router.

Review the communications sent about the account and service.
 	
When are they sent, and where are they directed?
	– Consider contact pathways used in association with the account:
	  – mailing address(es) (postal and residential),
	  – phone number(s),
	  – email address(es), and
	  – apps and self-service account websites.
	– Change contact details as appropriate, including:
	  – a new email address; and
	  – new contact number(s).
	– Provide the option to limit automatic communications, such as emails or SMS.

What service(s) is activated on the account? Are there any services that the customer is unaware of?	– Disconnect or change services if safe and appropriate. – Follow the recommendations in Chapter 10.
How are payments set up on the account?	– Review and update as necessary the payment methods on the account.
Authorised representatives and contacts.	– Have processes to prevent a perpetrator from having themselves listed on an account as an authorised user.
Are there any links or connections to other accounts (current or deactivated accounts)?	– Ensure all links or connections are removed.
Provide safety and security information and education on available support services to the customer.	– Provide advice and assistance to help the customer address/manage the issues; or – Provide advice about where to seek further information or assistance. – Consider the recommendations in Appendix 1.
Is there a pattern of *unwelcome communications* on the account?	– Follow the *unwelcome communications* process*.

Educate the *affected consumer* about options to prevent or respond to unwelcome communications	– These might include:
	  – suspension or disconnection of the perpetrator's service*;
	  – using handset features to block specific numbers;
	  – changing their number(s) free of charge (see clause 8.6.6);
	  – offering a new service.

***Note: Life threatening and unwelcome communications and DFV**

Obligations for managing *life threatening* and *unwelcome communications* are set out in C525 Handling of Life Threatening and Unwelcome Communications Industry Code.

This includes options to suspend or disconnect the service from which unwelcome communications originate and specific protections for the management of DFV matters.

8.9. Telecommunications records as evidence

Telecommunications records can be used as evidence of DFV. The police and courts may use them to substantiate claims and prosecute perpetrators.

Records may be requested directly by (and sent directly to) by the *affected person,* or by a law enforcement body, court of law or other entity authorised to do so under law (e.g. a court order or subpoena),

RSPs' obligation to respond to records requested under law are separate to their obligations to provide records directly to the *affected person.*

8.9.1. When dealing with record requests from an *affected person,* RSPs should:

(a) provide clear instruction to the affected person about the paperwork required in order for their access request to be actioned (e.g. in line with privacy regulation and the RSP's privacy policy);

(b) clearly explain the type of record that they can and cannot provide, and why; and

(c) be clear on the length of time it will take to access records.

8.9.2. RSPs should also discuss with the *affected person* the possible safety risks associated with their request for records proving DFV (i.e. abuse may escalate should a perpetrator become aware of the requests). RSPs may wish to suggest that the *affected person* seek advice from a specialist DFV organisation about potentially safer evidence-gathering options.

8.9.3. Once records are ready to send, RSPs should only provide them to requestor once it has been confirmed that it is safe to do so.

See also clause 6.2: Safety

8.9.4. RSPs should waive any fees charged for record requests in cases of DFV.

Note: Mobile Apps

Mobile apps may offer a safer and more secure method of collecting and retaining evidence of DFV (including *technology facilitated abuse*) than an RSP's records.

RSPs should refer an *affected person* to an appropriate resource for further information. For example, the App Safety Centre, collated by WESNET: https://techsafety.org.au/resources/appsafetycentre/

9. NAVIGATING DFV SAFELY THROUGH THE SALES PROCESS

Summary

This chapter looks at how an RSP should manage a sale that may involve DFV. The focus is to seek to protect the safety of the affected person, other customers, and sales staff, in both retail environments and contact centres.

The principles of a consumer-led, trauma-informed approach (emphasising empowerment and safety), outlined in previous chapters, apply throughout.

This chapter should be read in conjunction with previous chapters, particularly Chapter 3: Recognising abuse in the telecommunications space and Chapter 5: Staff training and support.

9.1. Overview

9.1.1. Sales staff should receive specialist DFV training tailored to their sales environment (i.e. retail or contact centre) and supported by clear, accessible procedures.

9.1.2. For retail representatives (staff that engage with customers face-to-face), training and procedural information must make it clear that the physical safety of the RSP's staff and other customers is paramount.

See also clause 5.1: Overarching obligations.

9.1.3. Other recommended topics include:

(a) how to recognise DFV, with examples focusing on the staff's specific sales environment (see also Chapter 3: Recognising DFV in the telecommunications space);

(b) information about how to safely manage suspected DFV during the sales process;

(c) that any action should be consumer-led, trauma informed and done in collaboration with the *affected person* (where it is safe to do so);

(d) that there is no requirement for the *affected person* to disclose DFV to be offered relevant assistance and support (see also clause 7.2: Accessing support and assistance); and

(e) the possible risks and consequences of different responses to suspected DFV to ensure that staff understand the purpose of the processes.

9.2. Managing DFV during the sales process

9.2.1. The aim of DFV management during the sales process is to:

(a) minimise any risk of physical violence toward the *affected person*, sales staff or any other people present;

(b) minimise the likelihood that any actions taken will place the *affected person*, staff or any other people present at risk of harm; and

(c) prevent or minimise the potential longer-term harms to the *affected person* should they unwillingly or unwittingly be made contractually responsible for telecommunications products or services that it is not in their interest to have.

9.2.2. Where DFV is identified or suspected, processes should be in place to empower sales staff to recommend or choose a course of action that they feel is most appropriate to – and safest for - the circumstances. Options include (presented in order of effectiveness – and likely reverse order of safety):

(a) declining a sale (e.g. "we are unable to sell to you at this time");

(b) pausing a sale (e.g. "there's a problem that needs to be further investigated before we can confirm that sale"); or

(c) referring the sale (e.g. allowing a sale to proceed but flagging the sale for immediate follow-up by a manager specialist team (such as specialist staff training in DFV, fraud or credit management)).

Case Study: *DFV during a retail sale*

Shania visited an RSP retail store seeking to set up a service separate from her existing account and mentioned safety concerns about her partner. The store representative identified this interaction as a potential DFV matter and - informally as part of information about services offered by the RSP - explained that the RSP has a dedicated team to support customers with safety and security concerns.

The sales representative was aware that completing a sale or account change could potentially trigger notifications to unintended parties (and therefore endanger Shania). They therefore proactively offered to contact the dedicated team while Shania was still in store, to ensure that a specialist team could appropriately assess and manage the risks. Shania agreed and requested that the team contact her for a confidential discussion. She was prompted to provide a safe phone number and nominate a time when the team could safely make contact to provide her with the specialist advice needed.

(Case study provided by an RSP)

9.2.3. To minimise safety risks, the reason a sale is declined, paused or referred should not be disclosed to the impacted *consumer(s)*, and there should be no suggestion that the action relates to DFV (or suspected DFV). RSPs may mirror processes already in place to prevent a sale where identity theft or fraud is suspected (e.g. staff trigger a 'failed credit check assessment' or 'system error' message by surreptitiously entering a specific code in the system or selecting a specific check box).

9.2.4. Processes should be in place to:

(a) enable and encourage the sales representative to seek support from senior staff or internal DFV specialists at any point during the process;

(b) support the sales representative should a perpetrator (or the *affected person*) seek to escalate a declined, paused or referred sale. This should include instructions on what retail staff should do should they feel physically threatened at any point during the process (linking to the store's general policies and procedures on managing security issues and emergencies); and

(c) require staff to report DFV concerns after the fact (whether or not a sale was confirmed) to:

(i) allow specialist staff to review the case and consider any appropriate follow-up (to support the *affected person*); and

(ii) ensure appropriate support is provided for the sales representative.

Case Study: *DFV during a contact centre sale*

Cherie called her RSP and advised them that her partner had deliberately broken her phone. She is worried, as she can't afford a new phone.

RSP representative Hilda answers Cherie's call. Hilda, who has recently completed DFV training, is concerned that Cherie's demeanour and statement about her issues suggest that she may be affected by domestic and family violence. Hilda asks Cherie if it is okay to transfer her to a specialist team who will be able to assist her and provide tailored options to help keep her connected. Cherie agrees to the transfer. Hilda warm transfers Cherie to a specialist DFV agent and informs the agent of her concerns and the background of Cherie's matter.

(Case study provided by an RSP)

9.2.5. RSPs should, as part of their sales training and processes, ensure that sales staff do not proactively suggest that a service or device contract be placed in the name of a person accompanying the person for whom a credit assessment was denied. This is a commonly used method of economic abuse, which occurs more readily when suggested by sales staff.

9.2.6. It is strongly recommended that RPS have processes to reactively respond to claims from *affected customers* that services in their name were obtained through coercion, fraud or impersonation. These processes should be separate from processes used to respond to traditional fraud claims.

See also Chapter 10: Financial hardship, debts and defaults.

Note: DFV and fraud

Services obtained through common fraud and through coercion share many features.

Perpetrators of both fraud and DFV may use coercion to get themselves appointed as an *authorised representative* on the *affected person's* account and proceed to purchase telecommunications products and services in the account holder's name.

Alternatively, perpetrators of DFV may commit fraud to gain access to, or take services out in the name of, their victim: a perpetrator will often have all the required factors of personal and account knowledge of the *affected person* to impersonate them and fraudulently commit to a sale in the *affected person's* name.

Although common fraud and DFV may result in the same outcome – i.e. those affected finding themselves legally and financially liable for telecommunications products and services that they do not gain any benefit from – RSPs should be careful not to assume that the same process is suitable for both situations. As emphasised in previous chapters, responses to DFV need to be *trauma-informed*.

10. FINANCIAL HARDSHIP, DEBTS AND DEFAULTS

Summary

This chapter outlines opportunities for an RSP to support an *affected person* who presents in financial hardship or is identified as an *affected person* during collections activity and debt management.

10.1. Overarching considerations

10.1.1. RSPs have specific obligations under the Financial Hardship Standard and TCP Code towards any *customer* experiencing financial hardship, debt management or credit management issues. Dedicated DFV training for staff in financial hardship and collections roles should include the following:

(a) how to recognise DFV, with examples focusing on the staff's specific role (see Chapter 3: Recognising abuse in the telecommunications space);

(b) options to safely manage suspected DFV during the financial hardship and collections pathway; and

(c) training to cover the possible risks and consequences of different responses to suspected DFV to ensure that staff understand the purpose of the processes.

10.1.2. Where the *affected person* is a *customer* in financial hardship, debt management or credit management, it is strongly recommended that:

(a) RSPs assign specialist DFV staff to support the *customer* (see also clause 4.2: Staff structure);

(b) there is no requirement for the *affected person* to disclose DFV to be offered relevant assistance and support (see also clause 7.2: Accessing support and assistance); and

(c) RSPs consider additional options or accommodations to assist the *customer*.

10.1.3. RSPs should advise all *customers* with financial hardship, debt management or credit management issues to contact a financial counselling service for independent financial advice and provide them with relevant contact information.

Further information is found in Appendix 1: Referral resources for consumers.

10.2. Financial hardship

10.2.1. RSPs must be aware of their obligations under the *Telecommunications (Financial Hardship) Industry Standard 2024* (*Financial Hardship Standard*).

10.2.2. The *Financial Hardship Standard* requires that RSPs have a readily accessible financial hardship policy. DFV is an express eligibility criterion for access to financial hardship assistance options.

10.2.3. Customers requiring financial hardship assistance may not be empowered to request it. The Financial Hardship Standard requires RSPs have processes and training to support staff in initiating a conversation about access to financial hardship options.

10.2.4. Any financial hardship arrangement for an *affected person* should be *trauma-informed*.

10.2.5. Under the Financial Hardship Standard, RSPs cannot require evidence of DFV when providing *short term assistance*. However, there are limited cases where it may be appropriate to seek additional information, including when providing *long term assistance*:

(a) where the amount to be repaid is more than $1000;

(b) where the *customer* has been a customer for less than 2 months; or

(c) to mitigate the risk of fraud.

See also clause 7.2: Accessing support and assistance

Case Study: *Financial Hardship*

Kayla had fled to a DFV refuge, along with her children. With no secure home location or consistent income, she had accumulated data and device debt on her telecommunications service.

Kayla contacted her RSP to advise of her situation, however she was not placed in its financial hardship program. As a result, while in the refuge, Kayla was unable to make her regular payment and her service was disconnected.

Kayla contacted her RSP again, noting that continued access to the telecommunications services was essential both for her and for her children (to maintain their education). On this occasion, her RSP did place her into its financial hardship program. The debt associated with the service was waived and Kayla was offered a monthly repayment on the device, which she accepted. Kayla was able to keep connected to services and support.

(Case study provided by ACCAN)

10.3. Debt management

10.3.1. RSPs must follow the credit management and debt management processes required under the *Financial Hardship Standard*.

10.3.2. Where an affected *customer's* account has fallen into debt, it is recommended that RSPs consider the following options when managing debt associated with DFV matters, in addition to the measures outlined in the TCP Code:

(a) ensure any discussion of debt is *trauma-informed* (see clause 6.3: Developing a trauma-informed response);

(b) fast-track financial hardship requests;

(c) waive part or all the *customer's* debt where appropriate (e.g. for accounts created under fraud or coercion (see clause 9.2.5);

(d) offer flexible payment plan options for legitimate outstanding debts;

(e) have a range of options available specifically concerning devices and equipment on the account, including:

(i) allowing a grace period for the return of a device or equipment;

(ii) working with the *customer* to develop a repayment plan; or

(iii) waiving the requirement to return any device or equipment the *customer* no longer has possession of and waiving any associated debt. RSPs may choose to IMEI block a mobile handset stolen or misused by a perpetrator.

Note: Suspension of credit management

It is a requirement under the TCP Code that where a payment plan is being discussed or in place, RSPs must suspend credit management action, subject to specific exclusions (as outlined in the TCP Code).

10.4. Disputing default

10.4.1. If an *affected person's* account has been default listed and the circumstances of the account indicate DFV may be present, RSPs should consider the effect of DFV on the debt issues. Where it is determined that the failure to pay was through no fault of the *customer*, the default may be considered as listed in error and should be removed.

10.4.2. Once an RSP is aware that a debt relates to DFV and that the failure to pay was through no fault of the *customer*, the RSP must manage the default dispute in line with expectations for credit management in the TCP Code.

10.4.3. Where a customer's debt has been sold, it is recommended that the debt is recalled from the debt buyer.

Note: Credit reporting data exchange rules

Clause 16 of the Principles of Reciprocity and Data Exchange (PRDE, the credit reporting data exchange rules) contains exemptions for cases of domestic or elder abuse.

10.4.4. RSPs should establish specific arrangements with debt collection agencies so that if the debt collection agency becomes aware of a DFV situation as part of their debt collection, they must inform the RSP that sold the debt.

Case Study: *Default dispute*

Franka was subjected to years of emotional and financial abuse. Her abusive partner, who had a poor credit history, had coerced her into signing up to mobile phone plans on his behalf. He then sold the handsets to third parties. Once she separated from her abusive partner, Franka was unable to continue to make payment on the account. In time, her account was sent to a debt collector and a credit default was listed against her name.

Franka subsequently sought support from a financial counsellor, to restore her finances. The financial counsellor contacted Franka's former RSP and advised them that the sale and account involved DFV. The RSP referred the case to a specialist in its DFV team, who accepted that the initial sale occurred under coercion and arranged for debt associated with Franka's account to be bought back from the debt buyer and for the debt to be waived. This also resulted in the credit default listing being removed from Franka's name.

(Case study provided by an RSP)

Appendix 1: Referral resources for consumers

Summary

This appendix has been developed with the aim of providing key referral points for consumers affected by domestic and family violence.

Location	Agency	Hours	Contact
Immediate danger			
National	Police, Fire, or Ambulance	24/7	000 112 106 (hearing or speech impaired)
DFV support, counselling and emergency accommodation			
National	1800 RESPECT	24/7	1800 737 732 www.1800respect.org.au
National	Non-emergency Police assistance line	24/7	131 444
National	Ask Izzy (Service and support referral tool)	24/7	https://askizzy.org.au/
National	Mensline (Men's generalist phone and online counselling service)	24/7	1300 789 978 https://mensline.org.au (online chat)
National	13 YARN (Aboriginal & Torres Strait Islander crisis support line)	24/7	13 92 76 https://www.13yarn.org.au/
National	Qlife (LGBTI peer support and referrals)	3 pm to Midnight 7 days	1800 184 527 https://www.qlife.org.au/
NSW	Domestic Violence Line	24/7	1800 656 463 https://www.speakout.dcj.nsw.gov.au/
Victoria	Safe Steps	24/7	1800 015 188 www.safesteps.org.au
Queensland	DVConnect Womensline	24/7	1800 811 811 http://www.dvconnect.org
Queensland	DVConnect Mensline	9 am – Midnight, 7 days	1800 600 636 https://www.dvconnect.org/mensline/

Location	Agency	Hours	Contact
South Australia	Domestic Violence Crisis Line	24/7	1800 800 098
South Australia	Local domestic, family and sexual violence support services	Online resource	https://www.sa.gov.au/topics/family-and-community/safety-and-health/domestic-violence-and-sexual-assault
Western Australia	Women's Domestic Violence Helpline	24/7	1800 007 339 https://www.wa.gov.au/service/community-services/community-support/womens-domestic-violence-helpline
Western Australia	Men's Domestic Violence Helpline	24/7	1800 000 599 https://www.wa.gov.au/service/community-services/community-support/mens-domestic-violence-helpline
Tasmania	Family Violence Counselling & Support	Weekdays 9 am - 12 am Weekends/ Public holidays 4 pm-12 am	1800 608 122 https://www.health.tas.gov.au/health-topics/family-violence/family-violence-counselling-and-support-service-fvcss
ACT	Domestic Violence Crisis Service	24/7	(02) 6280 0900 https://dvcs.org.au
Northern Territory	NT Legal Aid Commission (not a dedicated DFV service, however, can support referrals)	Monday to Friday, 8 am to 4.30 pm	1800 019 343
Northern Territory	Local domestic, family and sexual violence support services	Online resource	https://nt.gov.au/law/crime/domestic-family-and-sexual-violence/get-help-for-domestic-family-and-sexual-violence
Financial/Debt matters			
National	National Debt Helpline	Monday to Friday, 9 am – 5 pm, local time in each state	1800 007 007 www.ndh.org.au

Location	Agency	Hours	Contact
Technology-facilitated abuse matters			
National	ReportCyber (Reporting cyber abuse, Note: EXCLUDES situations where an active court order is in place)	24/7	https://www.cyber.gov.au/acsc/report
National	The eSafety Commissioner (Reporting image-based abuse or serious adult cyber abuse)	24/7	https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/report-to-esafety-commissioner
National	WESNET (Technology Safety Resources for Survivors Toolkit)	24/7	https://techsafety.org.au/resources

Appendix 2: Support resources for RSPs

Summary

This Appendix provides a range of DFV resources and support materials developed by government, advocacy groups, and other industries.

Telco Together Foundation: Telco Industry Domestic and Family Violence Action Framework

The TTF DFV Action Framework sets a pathway for Australian telco service providers of all sizes and types to support their customers and employees experiencing Domestic and Family Violence. The Framework contains four Action Plan option, relevant and available to all Australian telcos, regardless of their current DFV response. It includes practical actions, resources and support and recommends referring to the Communications Alliance DFV Guideline for the development of DFV Action Plan content.

https://industryimpacthub.org/dfv-action-framework/

WESNET and the Safety Net Australia Project

WESNET provides educational resources, training and information to highlight the structural drivers of domestic and family violence, intimate partner violence and gender-based violence and improve programmatic responses.

This includes the Safety Net Australia Project, a free resource that discusses technology, privacy, and safety in the context of intimate partner violence, sexual assault, and violence against women.

https://wesnet.org.au/ | https://techsafety.org.au/

Telecommunications Industry Ombudsman: Guides for Family Violence

The TIO has developed a guide for people affected by DFV with phone or internet problems related to financial hardship and economic abuse, privacy or safety issues, or technology-facilitated abuse.

https://www.tio.com.au/guides/family-violence

Ask Izzy

Ask Izzy is a free website that connects people in need with support services (including housing, a meal, money help, and family violence support) in their local area.

It can also be utilised by service providers, government agencies and corporate hardship teams across Australia to help clients find support.

https://about.askizzy.org.au/

Thriving Communities Partnership and the One Stop, One Story Hub

This is a cross-sector collaboration providing a centralised platform for collaboration on combatting customer vulnerability and hardship.

Thriving Communities Partnership also supports the One Stop, One Story Hub. The OSOS Hub enables frontline workers in corporate and community organisations to connect and refer their

clients to a range of supports through a single access point. This process aims to make it simpler for people in need to access support, reducing the burden and complexity involved in contacting each individual support program.

www.thriving.org.au

https://thriving.org.au/what-we-do/the-one-stop-one-story-hub

Our Watch

Our Watch is a national leader in the primary prevention of violence against women and their children in Australia.

https://www.ourwatch.org.au/

White Ribbon

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.

https://www.whiteribbon.org.au/Workplaces-and-Schools/Workplace-Accreditation

Economic Abuse Reference Group

A coalition of community organisations, EARG has produced some guidance on good practice, including a Good Practice Guide on Referrals, on how to make it easy for those making the referrals to determine where to refer.

https://earg.org.au/good-practice/

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

In April 2021, the ABA released industry guidelines to provide a voluntary framework for supporting customers impacted by family violence.

https://www.ausbanking.org.au/wp-content/uploads/2021/05/ABA-Family-Domestic-Violence-Industry-Guideline.pdf

https://www.ausbanking.org.au/wp-content/uploads/2021/07/ABA-Financial-Abuse-Industry-Guideline.pdf

Essential Services Commission: Moving towards better practice

In 2019 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/better-practice-responding-family-violence
https://www.esc.vic.gov.au/electricity-and-gas/codes-guidelines-and-policies/family-violence-resources-businesses#toc--better-practice-in-responding-to-and-engaging-survivors-of-family-violence

Appendix 3: Training resources for RSPs

This Appendix provides a range of providers which offer DFV training or training resources.

Women's Information and Referral Exchange (WIRE)

WIRE provides in-house training packages, speakers, and other resources.

https://www.wire.org.au/training/family-violence-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 offers online training on technology-facilitated abuse.

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

Good Shepherd Australia & New Zealand

Good Shepherd provides a range of training modules and tailored programs.

https://goodshep.org.au/services/training-and-advisory/

Uniting Kildonan

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

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

No to Violence

No to Violence works with men who use family violence and the sector that supports them to change their abusive and violent behaviour.

https://ntv.org.au

Appendix 4: Separating the rights of use of a number

This Appendix provides a practical outline of how an *end user* affected by DFV can gain control of a number where the current *ROU Holder* of the number is the perpetrator.

See also clause 8.5: New account, existing service(s).

Initiation

1. An *end user* advises the RSP that they are affected by DFV and are seeking support to keep their number(s) connected. The number(s) is active on the perpetrator's account, with the perpetrator the *customer* (the *ROU Holder*).
2. The RSP advises the *end user* of their options for connection (see Table 1: Customer account management options).
3. The *end user* advises the RSP that they wish to keep a number(s) that is connected on the perpetrator's account.
4. The *end user* establishes an ongoing association with the number(s). This can be achieved in various ways, such as a One Time PIN sent to the mobile number, knowledge of the account and call history, or other validation tools that the provider may use.
5. The RSP may request additional information before progressing the request (however, RSPs should consider the expectations in clause 7.2: Accessing support and assistance).
6. The RSP takes action to ensure there is no service disruption for the *end user*. This may include stopping the number from being upgraded, barred, disconnected, SIM swapped, or ported by the *ROU Holder*.
7. The RSP should outline the timeline of this process to the *affected person*, particularly if there is a risk that the current *customer* will be notified of any account changes.

Disconnection and separation

1. The number(s) is disconnected on the *customer's* account.
2. Any charges associated with disconnection should be waived. It is also recommended that any mobile payment plans, or early exit fees related to the termination, are waived for the safety of the *affected person*.
3. The mobile number is separated from the original account.

Recalling and activating the number on a new account

1. A new account is set up with the original *end user* as the new *customer*. This may be a prepaid or post-paid telecommunications service and will be subject to the normal identity and credit checks (where relevant) required to establish a new service.

   See also Chapter 8: Account management and security.
2. The number is recalled and activated on the new account. RSPs can recall an issued number without replacement on a former account where the supply of the carriage service to the *customer* is otherwise terminated (which occurred during 'Initiation').
3. RSPs can inform the new *customer* that they are now the *ROU Holder* for that number, which includes a right to port the mobile number to a new provider.
4. RSPs should advise the new *customer* to utilise new privacy and security settings to prevent the perpetrator from gaining access to their new account (see Table 2: Affected

customer account security checklist). Importantly, RSPs should check with the new *customer* that all contact information on the account is correct and is not accessible by the perpetrator.

Communication with and responses to the former ROU Holder

1. RSPs should consult legal advice to determine what information can be provided to the former *ROU Holder* (the perpetrator) when action is taken under this process, in line with privacy obligations. Possible options include:
    a. placing a note on the account stating that the former *ROU 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. This note could include a reference that the former *ROU Holder* has lost the use of the number due to a breach of their contract or SFOA and the RSP's legal obligations under the Telecommunications Act; or
    b. proactively contacting the former *ROU Holder,* notifying them of the loss of the mobile number, including information that all future charges associated with that mobile number from a specific date will be waived.
2. An RSP should guide their frontline staff to respond to enquiries from the former *ROU Holder* for the loss of a number under this process. Possible options include:
    a. clear guidance to staff that under no circumstances should they advise the former *ROU Holder* that the termination occurred due to DFV issues;
    b. having appropriate support for frontline staff in the event the perpetrator escalates and engages in any antisocial behaviour (see also clause 6.2: Safety);
    c. placing a note on the account stating that the former *ROU 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. This note could include a reference that the former *ROU Holder* has lost the use of the number due to a breach of their contract or SFOA and the RSP's legal obligations under the Telecommunications Act; or
    d. having requests from the former *ROU Holder* referred to a specialist team to discuss the disconnection.

Participants

The G660:2023 review was conducted by the Domestic and Family Violence Guideline Working Group, as part of the activities of the Communications Alliance Industry Consumer Advisory Group (ICAG).

The Working Group consisted of the following organisations and their representatives:

Organisation	Representative(s)
Telstra	Fiona Wade Fiona Madigan Mark Sulikowski
TPG Telecom	Alexander Osborne
Vocus	John Sexton
Aussie Broadband	Eric Erikson Cameron Foley Nick Venn
Optus	Vladimir Flores
Amaysim	Susan Craig
Pivotel	Keri Crossen

The Working Group was chaired by Annie Leahy, TPG Telecom.

Project management and drafting support was provided by Peppi Wilson, Communications Alliance.

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

Correspondance
PO Box 444
Milsons Point
NSW 1565

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