Appendix 6:

This is an online document accessed via page 85 of the DFV Action Framework.
If you have printed or saved this, check the IIH website for updated versions at industryimpacthub.org/domestic-and-family-violence/dfv-action-framework-resources/.
The version number is in the header. Last updated: 11 April 2024

Government and Industry expectations of telcos regarding their response to Domestic and Family Violence (DFV)

Below is a historical snapshot of some of the developments, guidelines, Codes and Standards produced by Government and the Telecommunications Industry between 2016 and 2024 relevant to a telco's response to DFV. These are relevant to telcos when developing their DFV Action Plans.

These are in chronological order.

The content included here is commentary, not a summary of the relevant document. Please review the full document referenced.

There are other useful documents produced by, for example: eSafety, Wesnet, Champions of Change Coalition, Thriving Communities Partnership, the Commonwealth Bank, Our Watch, the Water Industry, the Economic Abuse Reference Group, the Australian Banking Association, the Essential Services Commission, the Energy Industry.

Some of the historical references provided here are also reflected in Appendix 5: Statistics and Appendix 7: Useful Resources.

Appendix 6:

Royal Commission into Family Violence

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

Recommendation 108

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

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

Assisting and Responding to Customers in Financial Hardship guideline.

In April 2017, The Telecommunications Industry Ombudsman, Financial Counselling Australia and Communications Alliance revised this guideline. It enables telecommunications providers to better assist those who have experienced domestic and family violence, including identifying family violence as an express eligibility criterion for access to hardship programs as included in Recommendation 108.

Appendix 6:

Industry Guidance Note IGN 017. Authorised Representatives and Advocates

In July 2019 Communications Alliance Issued this Guidance Notice (IGN) for industry, consumers, and consumer groups. It is intended to educate all three of these groups to streamline the appointment process while continuing to protect consumers from fraud.

It is in addition to the relevant clauses in the TCP Code (Clauses 3.5 and 3.6, TCP Code C268:2019), and must be read in conjunction with those clauses.

The IGN has 3 key purposes:

1) Clarify the differing roles of Advocates and Authorised Representatives in the telecommunications industry (Sections 3 and 4);
2) Provide information on the range of information and processes Suppliers might require or put in place for a consumer to appoint an Advocate or Authorised Representative (Section 5); and
3) Suggest a standardised method by which Suppliers can communicate this information (Section 7).

Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020

In February 2020, the ACMA issued this Standard. The objectives of this industry standard are, without limitation, to:

a) prevent the unauthorised porting of mobile service numbers;
b) reduce harm to customers from the unauthorised porting of mobile service numbers; and
c) require gaining carriage service providers to take reasonable steps to confirm that the person requesting a port:
    i) is the rights of use holder of the mobile service number to be ported; and
    ii) has direct and immediate access to a mobile device associated with that mobile service number.

Appendix 6:

Telecommunications Industry Ombudsman Report: Meeting The needs of Consumers impacted by Family Violence

In December 2020, the TIO produced the findings of a systemic investigation through this report. The investigation found the needs of consumers experiencing family violence were not always met by telco's standard systems and processes.

The Report's media release said that Ombudsman Judi Jones says her organisation is here to help both consumers and telcos. Ombudsman Jones said "This report makes recommendations for telcos wanting to improve their service to better meet the needs of their customers experiencing this vulnerability. I encourage providers to think deeply about changes they can make to best support consumers impacted by family violence.

"We acknowledge the good work of family violence specialists, the telco industry and consumer advocates in this space. We are all on the same journey as many organisations in improving our understanding of the impacts of family violence. We will continue to monitor and evaluate our approach as our understanding evolves".

Children and technology-facilitated abuse in domestic and family violence situations

In December 2020 eSafety published this report.

eSafety commissioned research on the dynamics and impact of technology-facilitated abuse involving children in the context of domestic and family violence in 2019-20.

The research drew on a survey and focus groups of professionals who work with domestic violence cases, and interviews with mothers who are survivors of domestic violence, young people impacted by technology-facilitated abuse in domestic violence situation and fathers in men's behavioural change programs.

The research investigated:

- the role of technology in children's exposure to domestic and family violence
- the impact of technology-facilitated abuse on children and young people
- professionals' knowledge about technology-facilitated abuse involving children in the context of domestic and family violence
- young and adult survivors' perspectives of technology-facilitated abuse
- perpetrators' perspectives on technology and communication with their children
- strategies and resources to protect children from technology-facilitated abuse.

Appendix 6:

Family violence inquiry targets encryption

March 2021, The House of Representatives Standing Committee on Social Policy and Legal Affairs made 88 recommendations in their March 2021 report from the Inquiry into family, domestic and sexual violence. Recommendation 30 included a number of proposed measures relating to technology-facilitated abuse, including that:

- The Government should consider regulating to enable law enforcement agencies to access a platform's end-to-end encrypted data, by warrant, in matters involving a threat to the physical or mental wellbeing of an individual or in cases of national security.

Telecommunications (Consumer Complaints Handling) Industry Standard 2018

In April 2021, the ACMA issued a compilation of the *Telecommunications (Consumer Complaints Handling) Industry Standard 2018* that shows the text of the law as amended and in force on 1 April 2021 (the ***compilation date***). acma.gov.au/how-telcos-must-handle-complaints

Online Safety Bill

In June 2021 the Online Safety Bill was passed by the Senate.

Introduced with the Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021, the bill:

- Retains and replicates certain provisions in the *Enhancing Online Safety Act 2015*, including the non-consensual sharing of intimate images scheme;
- Specifies basic online safety expectations;
- Establishes an online content scheme for the removal of certain material;
- Creates a complaints-based removal notice scheme for cyber-abuse being perpetrated against an Australian adult;
- Broadens the cyber-bullying scheme to capture harms occurring on services other than social media;
- Reduces the timeframe for service providers to respond to a removal notice from the eSafety Commissioner; brings providers of app distribution services and internet search engine services into the remit of the new online content scheme; and
- Establishes a power for the eSafety Commissioner to request or require internet service providers to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct for time-limited periods in crisis situations.

Appendix 6:

Consumer Vulnerability: Expectations for the telecommunications industry

In May 2022, the ACMA published this document, which 'sets out a statement of expectations for the telecommunications industry to improve outcomes for consumer in vulnerable circumstances who may experience barriers to accessing and maintaining telecommunications products and services'.

The ACMA reminds telcos of the TCP Code and that it includes a range of obligations built upon a key commitment by telcos to assist and protect disadvantaged and vulnerable consumers, with specific rules about:

- dealing with disadvantaged and vulnerable consumers
- responsible selling
- credit and debt management
- financial hardship
- identifying and meeting consumer needs
- allowing for advocates and authorised representatives.

It also includes other helpful obligations that are not specific to the telecommunications industry.

The ACMA says 'This statement of expectations aims to contribute to the development of appropriate industry responses by providing guidance to assist industry in identifying vulnerability and setting out how we expect telcos to support consumers in vulnerable circumstances'.

The second (of four) expectations from the ACMA is 'Be proactive in identifying and responding to consumers in vulnerable circumstances' and the Statement specifically includes domestic and family violence as a factor that may contribute to vulnerability.

There are five priority areas for telcos listed, each including a key outcome and expectations:

1. Culture and Practices
2. Selling and Contracting
3. Customer Service
4. Financial Hardship
5. Credit/debt management and disconnection.

Under the first priority they suggest that telcos consult the Telco Together Foundation DFV Action Plan Framework and Training Framework and the Communications Alliance Guideline G660:2018. They also suggest telcos develop a DFV plan that addresses the needs of staff and customers who may be impacted by DFV. ***See industryimpacthub.org/dfv-action-framework/ for further information about the DFV Action Framework.***

Appendix 6:

Telecommunications Service Provider (Customer Identity Authentication) Determination

In April 2022 the ACMA introduced the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022, which came into effect on 30 June 2022.

The objectives being to:

a) reduce the harm caused to customers when access to their personal information, business information or telecommunications service is targeted by unauthorised persons or entities; and

(b require carriage service providers to follow effective identity authentication processes to protect the security of high-risk customer interactions.

This Service Provider Determination (SPD) places requirements on telcos to further authenticate customers in situations of high-risk customer interaction.

The determination lists examples of a high-risk customer transaction. These include everyday transactions which will now trigger an authorisation request, including a change of address, a transfer of title or a SIM swap. This request must be responded to before a high-risk transaction can be completed.

Authentication processes can create a situation of danger for end users who may be DFV victim-survivors. For this reason, in cases where a telco suspects a customer may be in a vulnerable circumstance (which includes being a victim of DFV) the SPD enables telcos to action different authentication processes (listed in Section 11 'Identify authentication requirements for people in vulnerable circumstances).

Appendix 6:

Telecommunications Consumer Protections (TCP) Code C628:2019

June 2022: The current version of the TCP Code, *C628:2019 Incorporating Variation no. 1/2022*, commenced on 17 June 2022.

The full code available here: *C628:2019 Incorporating Variation no. 1/2022*

The TCP Code is a code of conduct for the Telecommunications Industry in Australia. It provides community safeguards in the areas of sales, service and contracts, billing, credit and debt management and changing suppliers. It also sets out a framework of code compliance and monitoring. It applies to all Carriage Service Providers in Australia, and is enforceable by the ACMA.

The current version of the TCP Code, *C628:2019 Incorporating Variation no. 1/2022*, commenced on 17 June 2022. It updates and replaces C628:2019, with minor variations included to reflect updated ACCC guidance material referenced in Chapter 3, Disadvantaged and Vulnerable Consumers, and updated ASIC-ACCC guidance referenced in Chapter 6, Debt Collection.

Update, March 2024. In February 2024, the ACMA introduced a new Telecommunications (Financial Hardship) Industry Standard 2024, to commence from 29 March 2024. The Standard replaces financial hardship-related obligations in the TCP Code.

Updates to reflect the new Standard are being drafted in the context of the full code review and revision currently underway. For more information: commsalliance.com.au/hot-topics/TCP-Code-Review-2024

Review Communications Alliance website for further updates: commsalliance.com.au/Documents/all/codes/c628

Appendix 6:

National Plan to End Violence Against Women and Children 2022 – 2032 (National Plan).

In October 2022 the Australian, state and territory governments released the National Plan to End Violence against Women and Children 2022–2032 (National Plan). The Plan says:

The National Plan commits to 10 years of sustained action, effort and partnership across sectors and levels of government towards our vision of ending violence against women and children in one generation. It outlines what needs to happen to achieve our vision. This includes building the workforce, growing the evidence base and strengthening data collection systems, while delivering holistic, coordinated and integrated person-centred responses. To achieve this, we must listen to and be guided by victim-survivors and people with lived experience.

The National Plan puts in place a national policy framework to guide the work of governments, policy makers, businesses and workplaces, specialist organisations and family, domestic and sexual violence organisations and workers in addressing, preventing and responding to gender-based violence in Australia. The National Plan will be implemented through two 5-year Action Plans. These will detail specific Commonwealth, state and territory government actions and investment to implement the objectives across each of the four domains: prevention, early intervention, response, and recovery and healing.

Since then: The Albanese Labor Government has released the following supporting documents:

- First Action Plan 2023 – 2027
- First Action Plan 2023 – 2027 Activities Addendum
- Aboriginal and Torres Strait Islander Action Plan
- Outcomes Framework 2023 - 2032
- Theory of Change 2022 - 2032

Appendix 6:

G660:2023 Assisting consumers affected by domestic and family violence

In May 2023 Communications Alliance published this Guideline.
It replaced the Guideline: Assisting Customers Experiencing Domestic and Family Violence Guideline: G660:2018.

In April 2024 it was updated to cover the new requirements in the Financial Hardship Standard.

The Guideline says:

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.

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.

Key changes include:

- a restructure of the Guideline to better support its practical implementation, with a focus on plain-English information, guidance and advice appropriate to the audience (i.e. retail Carriage Service Provider (RSP) management and staff in different operational roles).

This includes:

- Clear information about how DFV may present for telecommunications consumers, including case studies to illustrate both possible presentations and (in later chapters) effective RSP assistance,
- Information (and links) to assist RSPs in understanding and managing DFV matters within the context and constraints of other telecommunications industry legal and regulatory obligations,
- 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:
  - support people affected by DFV, and
  - educate, train, and support staff.

Appendix 6:

- Expanded coverage to include:
  - the full range of telecommunications consumers, products, and services, including small business customers and fixed services,
  - updated information about the different ways that DFV may present.

    This includes more explicitly recognising that DFV can occur in any relationship (from intimate partnerships, immediate and extended family groups, communal and extended kinship connections, to carer and guardianship arrangements, including abuse of older people) and may include different 'abuse types', including (but not limited to) physical violence, emotional abuse, coercive control, economic abuse, technology-facilitated abuse and cultural and religious abuse.
- Updated figures, links and references.

C540:2023 Local Number Portability

C540:2023 (pdf 618kb)

June 2023: The Local Number Portability (LNP) Code was updated.

This Code sets out inter-Carrier/CSP operational procedures for the implementation of Local Number Portability processes. The Code sets minimum acceptable practices (including Standard Hours of Operation, activation targets and timeframes) which do not unnecessarily limit industry's ability to improve on the minimum level. Service metrics for Cat A and Cat C Ports, along with updated arrangements to Quarantine Disconnected Ported Telephone Numbers are part of the improvements included in the 2023 version of the Code.

Related material

Eligible Party Identification Codes List

Appendix 6:

Number Management – Use of Numbers by Customers

C566:2023 (pdf 508kb)

June 2023 This Code was published. This replaces both the:

- C566:2005 Rights of Use of Numbers Industry Code and
- C554:2004 Rights of Use of Premium Rate Service Numbers Industry Code.

This Code sets out arrangements relating to:

a) CSPs either Holding, or wanting to Hold, Numbers for use by them in connection with the supply of a Listed Carriage Service to a Customer; and

b) Carriers in their role of supplying Listed Carriage Services using Numbers.

The Code objectives also include clarifying a CSPs obligations in providing Rights of Use (ROU) when a Number is Issued; and enables ROU Holders to understand how they can use a Number Issued to them and what is and is not permitted.

This update provides better information to Retail Service Providers (RSPs) on how to manage ROU issues where the end user is affected by DFV and is not the customer with the ROU for the number(s) they use.

Now, it is clear that 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 the Use of Numbers Code.

This means processes can be in place to:

- **Terminate the right** to the perpetrator customer to use the number(s);
- **Disassociate the number(s)** from the perpetrator customer account; and
- **Transfer the number** to the affected person's **new clean slate account**.

Under the new C556 Number Management – Use of Numbers by Customers Industry Code, RSPs may:

- clause 4.3.3 – make a Service subject to terms and conditions as outlined in a Standard Form of Agreement (SFOA). A breach of the SFOA may result in the disconnection of the Service, with the Customer losing the ROU of the associated Number.
- clause 4.7.2 – move 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.
- clause 4.7.3 – where they are holding churned or ported number(s) in quarantine following disconnection, issue the number(s) to an affected person who is the former customer or authenticated end user.

Appendix 6:

RSPs should review and, if necessary, modify their 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 (the ROU holder).

RSPs should also review their number allocation systems and processes to allow former customers and end users affected by DFV to be (re)issued with a number(s) that is in quarantine where they have previously had a connection to that number(s).

Important note: 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.

Handling of Life Threatening and Unwelcome Communications Code

C525:2023(pdf 801kb)

June 2023. This Code was **revised** to:

- Add additional clarity to the definition of Pattern of Unwelcome Communications and Unwelcome Communications;
- Include a new clause to clarify information sharing when identifying a pattern of Unwelcome Communications from an offender who has moved Suppliers;
- Reduce the time required before sending a second warning letter;
- Consider circumstances for domestic and family violence situations.

The Code provides standard procedures for the cooperative handling (including call tracing) by carriers, carriage service providers and the national relay service provider of communications across networks that are life threatening or connected with a pattern of unwelcome communications. The Code also outlines when carriers, carriage service providers and the national relay service provider can deal with unwelcome call complaints relating to non real-time communications such as SMS, MMS and email.

Two Industry Guidance notes also exist to complement the Code. The first is a Customers Process Industry Guidance Note IGN010 and the second sets out the agreed thresholds for complaints to Helplines.

Appendix 6:

eSafety Industry Codes

June 2023: eSafety registered the following Codes:

- Social Media Services Online Safety Code
- App Distribution Services Online Safety Code
- Hosting Services Online Safety Code
- Internet Carriage Services Online Safety Code
- Equipment Safety Safety Code
- Internet Search Engine Online Safety Code

Sept 2023: eSafety registered the following Code:

- Consolidated Industry Codes of Practice for the Online Industry (Head Terms)

Telecommunications (Financial Hardship) Industry Standard 2024

The Standard

29 March 2024: This Standard came into force on this date.

These rules have been developed by the ACMA in response to a direction from the Minister for Communications, the Hon Michelle Rowland MP, to make an enforceable industry standard that will improve safeguards f or telco customers experiencing financial difficulties.

The new Telecommunications (Financial Hardship) Industry Standard 2024 requires telcos to establish and promote clearly accessible written financial hardship policies. Telcos must do more to proactively identify customers experiencing financial hardship and prioritise keeping them connected to services.

The definition of financial hardship explicitly names DFV as a potential indicator of financial hardship. Additionally, there are rules around the management of customers affected by DFV who are experiencing financial hardship.

Appendix 6:

Laws, documents, orders that may be of interest that are not specific to the Telco Industry

National Domestic Violence Order Scheme

From 25 November 2017 All Domestic Violence Orders (DVOs) issued in an Australian state or territory are automatically recognised and enforceable in all Australian states and territories. Under the National Domestic Violence Order Scheme, individuals protected by a domestic violence order issued before 25 November 2017 may apply to any local court in Australia to have it recognised.

The federal, state and territory governments agreed to introduce the National Domestic Violence Order Scheme through the Council of Australian Governments. The scheme represents a significant step towards further protecting and empowering families as they build new lives, safe and free from violence.

The Department of Home Affairs - external site has policy responsibility for the scheme.

Family Law Amendment (Family Violence and Other Measures) Act 2018

On 1 September 2018 *The Family Law Amendment (Family Violence and Other Measures) Act 2018* commenced.

The Act enhances the capacity of the justice system to provide effective outcomes for vulnerable Australians who are experiencing family violence. It amends the *Family Law Act 1975* to improve the family law system's response to family violence, and the intersection of the federal family law and state and territory family violence and child protection systems.

The Act implements recommendations of the Family Law Council's 2015 and 2016 reports on *Families with Complex Needs and the Intersection of the Family Law and Child Protection Systems*, and other expert reports.

Visit the Parliament of Australia - external site website for more information.

Appendix 6:

Debt Collection Guideline for collectors & creditors

In April 2021 ACCC and ASIC jointly produced this guideline which aims to assist creditors, collectors and debtors understand their rights and obligations, and ensure that debt collection activity is undertaken in a way that is consistent with consumer protection laws.

Coercive control

In November 2022, the New South Wales Government's Bill, the Crimes Legislation Amendment (Coercive Control) Bill 2022, was passed by parliament.

The passing of this bill means that **New South Wales is the first Australian state to criminalise coercive control**. The new legislation makes it an offence for a current or former intimate partner to carry out repeated abusive behaviours with the intention of controlling or coercing the victim.

Appendix 6: