

From: Tanya Farrell
To: [REDACTED]
Subject: FW: More RE: Follow up on questions raised by ACMA 20/06 [SEC=OFFICIAL]
Date: Wednesday, 3 July 2024 1:31:07 PM
Attachments: image007.png
image003.png
image004.png
image005.png
image006.png
DFV telco initiatives summary JULY 2024.pdf
image007.png
image008.png
image009.png
image010.png

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



Sent: Wednesday, July 3, 2024 1:13 PM
To: Samantha Yorke <Samantha.Yorke@acma.gov.au>; [REDACTED] Adam Suckling <Adam.Suckling@acma.gov.au>; Cathy Rainsford <Cathy.Rainsford@acma.gov.au>; Tanya Farrell <Tanya.Farrell@acma.gov.au>
Cc: Nerida O'Loughlin <Nerida.O'Loughlin@acma.gov.au>; [REDACTED]
Subject: RE: More RE: Follow up on questions raised by ACMA 20/06 [SEC=OFFICIAL]

CAUTION: This email is from an external sender. Do NOT click on links or open attachments unless you recognise the sender and KNOW the content is safe. If you are in doubt, please contact the Corporate Service Desk.

Dear all,

Further to [REDACTED] email below, please find attached the promised summary information about all the work in the telco space to address the harm from domestic and family violence (current and planned – by CA, ITF and others).

Also included is an analysis of proposed TCP Code obligations to mandate specific actions and responses to protect and support consumers affected by DFV, presented against recommendations about what should be mandatory in this area. Reiterating that further adjustments are expected as the Code drafting progresses to clarify drafting and address any identified gaps – I genuinely believe that there is no disagreement about the intent and desired consumer outcome in this complicated space. There is certainly a desire and willingness from our (CA and its members) end to work collaboratively and constructively together.



In the spirit of reconciliation the Communications Alliance acknowledges the Traditional Custodians of country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

From: [REDACTED]
Sent: Thursday, June 27, 2024 11:44 AM
To: Samantha Yorke <Samantha.Yorke@acma.gov.au>; Adam Suckling <Adam.Suckling@acma.gov.au>; Cathy Rainsford <Cathy.Rainsford@acma.gov.au>; Tanya Farrell <Tanya.Farrell@acma.gov.au>
Cc: Nerida O'Loughlin <Nerida.O'Loughlin@acma.gov.au>; [REDACTED]
Subject: More RE: Follow up on questions raised by ACMA 20/06

CAUTION: This email is from an external sender. Do NOT click on links or open attachments unless you recognise the sender and KNOW the content is safe. If you are in doubt, please contact the Corporate Service Desk.

Apologies – attached is the position paper that I intended to attach to my original message.

I [REDACTED]



I acknowledge the Traditional Custodians of the lands on which I work and reside, the Gadigal People of the Eora Nation, and I pay my respects to their Elders, past, present, and emerging.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

From: John Stanton
Sent: Thursday, June 27, 2024 4:57 AM

To: Samantha Yorke <Samantha.Yorke@acma.gov.au>; adam.suckling@acma.gov.au; Cathy Rainsford <Cathy.Rainsford@acma.gov.au>; Tanya Farrell <Tanya.Farrell@acma.gov.au>
Cc: Merida.O'Loughlin@acma.gov.au; [REDACTED]
Subject: TCP: Follow up on questions raised by ACMA 20/06
Importance: High

Dear all,

Thank you again for your time on Thursday to discuss the draft TCP Code.

We would like to follow up on a few items discussed, not least because we realised that some of the lengthy discussions on these issues took place when both Cath and Tanya were working in different areas of the ACMA and may not, therefore, have reviewed the relevant position papers and comment logs.

For ease of reading, we have included this information in a Word document.

Also included are links to the referred position papers and comment logs.

We again repeat our offer to meet to discuss any parts of drafting that are unclear, etc.

Best regards

I [REDACTED]



I acknowledge the Traditional Custodians of the lands on which I work and reside, the Gadigal People of the Eora Nation, and I pay my respects to their Elders, past, present, and emerging.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

NOTICE: This email message is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorised review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message.

Addressing the harms of domestic and family violence – Telco initiatives, commitments and plans

There is a plethora of work being undertaken – and new initiatives underway – to address the harms associated with DFV, across government, industry in general and at a telco-specific level. These efforts are ongoing and iterative – recognising that collaborative and ongoing engagement will receive the best results for consumers in this sensitive and complicated space.

Actions and resources already developed are considered 'live' and are regularly updated. These are supported by a number of other initiatives and lines of work already underway, and work being developed or planned. This includes:

- new proposed obligations in the TCP Code to mandate specific actions and responses to protect and support consumers affected by DFV. Note that this is an iterative drafting process, and further adjustments are expected as the Code drafting progresses to clarify drafting and address any identified gaps.
- educational initiatives (such as information for DFV frontline services to assist them understand options for their 'clients' (those affected by DFV)), and work to identify efficiencies and initiatives to support action by the sector as a whole.

Challenges include:

1) working out the best framework to ensure understanding and engagement of the issues at the appropriate levels within organisations, in an efficient and effective manner, without unnecessary duplication of effort and respecting the limited resources of all parties, but particularly the experts on the frontline.

2) how to frame action in a way that enables the issues are appropriately considered and addressed by individual businesses, while:

- allowing flexibility in support, which is critical for the safe, trauma-informed, and DFV-affected-person-lead management of issues in this complicated area, and
- facilitating the open dialogue necessary for continual improvement. That is, an approach that provides spaces for business to openly and honestly discuss best practice support, as well as the challenges and concerns in assisting those affected by DFV without fear of penalty.

At a national level, the Domestic, Family & Sexual Violence Commissioner is looking to facilitate and coordinate cross-industry collaboration to accelerate implementation of the *National Plan to End Violence Against Women and Children 2022-2032*, as part of their work to address and end violence against women and children. As an early step, a roundtable was held on 24 June 2024. It included banks, energy providers, and telcos amongst others (with CA, Telstra, Optus and TPG Telecom all involved).

In the telco space, considerable time and effort has been (and continues to be) put into understanding the impact of DFV on consumers and their telecommunications needs, to drive improvements in how telcos can better interact with, and support customers affected by DFV. This includes a substantial body of work through Communications Alliance and also through the Telco Together Foundation.

Table 1 below provides an overview of telco-specific activity; a summary of industry's delivered actions, commitments, plans and initiatives in this important area.

Table 2 provides detailed information about the proposed mandatory DFV-related protections in the revised TCP Code, presented to show how the approach taken reflects stakeholder feedback on the provisions that should be mandatory (centred around ACCAN's policy position paper, which reflects/matches feedback directly to CA during the Guideline development, from experts in the field, including eSafety, WESNET, 1800RESPECT, Woman's Legal Service Victoria, Economic Abuse Reference Group, Thriving Communities Australia, Katherine Women's Legal Service, DV Service Management, Relationships Australia, and the Australian National University's Centre for Social Research & Methods).

Table 1: Overview of telco-specific commitments, plans and initiatives

Key: CA – Communications Alliance. TTF – Telco Together Foundation. Both organisations are funded by the telco industry.
TFA – technology-facilitated abuse.

Instrument or initiative	What it achieves	Comment
<p><u>G660 Assisting Consumers Affected by Domestic and Family Violence Industry Guideline</u> (CA)</p> <p>Originally published 2018. Substantially updated and expanded in 2023 after an iterative drafting process with considerable consultation and discussion with key stakeholders (Regulators, government agencies, DFV specialist groups, more general consumer groups, First Nations specialist groups, ANU researchers and telcos) over a 12-month period.</p> <p>Living document. Continually updated with more examples, guidelines, updated references, to provide more clarity, etc.</p> <p>Three updates already since publication one year ago (most recent, March 2024).</p>	<p>Publicly available detailed information and BP guidance, tailored for the telco industry, to help CSPs develop tailored and appropriate DFV training, policies and procedures for their business model, size and situation. Includes:</p> <ul style="list-style-type: none"> - illustrations of the numerous ways that DFV might present in the telco space (including case studies) - clear information to highlight and explain how issues are affected by different regulatory instruments (this is not just a TCP Code issue) and explain how potential conflicts can be managed - details about options to assist a DFV-affected person safely and appropriately. 	<p>In developing G660, it became clear that there were some elements that could usefully be made mandatory, to ensure that telcos considered DFV issues appropriately. (our view + that of experts in the field)</p> <p>CA committed to uplifting to the TCP Code all these key elements. Table 2 details how this has been achieved in the current draft TCP Code. (noting that this is an iterative drafting process, and further adjustments are expected to address any gaps or clarify drafting).</p> <p>And committed to, or re-iterated CA's commitment to, amending other instruments to permit particular action when DFV was identified, to ensure CSPs were able to take appropriate action to assist victim-survivors without being in breach of other regulation (e.g. amendments to C525, C566, TCP Code).</p>
<p><u>C525 Handling of Life Threatening and Unwelcome Communications Industry Code</u> (CA)</p> <p>Last revised in 2023 to specifically consider circumstances for DFV situations.</p>	<p>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.</p> <p>C525 also outlines when C/CSPs and the national relay service provider can deal with</p>	<p>Changes to C525 were made to consider circumstances for domestic and family violence situations. This included a reduction in timings for warning letters and service suspension, new templates for warning letters, and consent requirements for sharing information within warning letters.</p>

Instrument or initiative	What it achieves	Comment
	unwelcome call complaints relating to non-real-time communications such as SMS, MMS and email.	
<p><u>C566 Number Management – Use of Numbers by Customers Industry Code</u> (CA)</p> <p>Last revised 2023, including to support arrangements for those affected by DFV.</p>	<p>Covers the arrangements under which CSPs may issue, assign, transfer or surrender numbers. Includes obligations to manage and port numbers and rights of use and rules around a customer's right of use (ROU) of that number.</p>	<p>Changes to C566 were made in 2023 to permit separation of a DFV-affected person's number from the abuser's account (where the abuser is the customer and is otherwise the rights of use (ROU) holder).</p> <p>(Guidance on implementing ROU changes is included in G660.)</p>
<p>TCP Code – revised draft 2024 (CA)</p> <p>Draft Code and full details of iterative review and revision process, available here.</p>	<p>Specific requirements for DFV uplifted from the CA guideline, per recommendations from the experts from DFV support services, consumer groups and regulators.</p> <p>Clauses are spread throughout the Code (as the Code is structured by customer journey). For ease of reference, a summary table is provided below, with issues presented against the ACCAN DFV Policy Position (which was consistent with feedback from other stakeholders)</p>	<p>See table 2, below.</p> <p><i>Note that Code drafting follows an iterative drafting process, and further adjustments are expected to address any gaps or clarify drafting.</i></p> <p>(with proposed revision process designed to facilitate more regular updates of Code, as required)</p>
<p>1800 Respect call record suppression (CA)</p>	<p>Records of calls to this helpline are already, or soon will be (before the end of the year), suppressed from the majority of billing records. This is designed to reduce likelihood of perpetrators being alerted of their victim's call for assistance.</p>	<p>Issues around formalising and/or expanding this initiative are being explored with DITRDCA (and through them, DSS).</p>
<p>Quarterly DFV Roundtables (TTF)</p> <p>Living action. Members Telstra, Optus, TPG Telecom, Vocus Group, Aussie Broadband, More Telecom, and Uniti Group discuss and decide upon DFV initiatives to implement across industry.</p>	<p>Objective: To identify areas of collective action within the industry that will have greatest impact on reducing instances and supporting victims of DFV across Australia.</p>	<p>TTF has taken a <u>staged approach</u> to its collaborative work with members to address DFV, recognizing that the subject is complex and requires 'ground-blocks' to be in place. The work incorporates sustained learning and continuous improvement.</p>

Instrument or initiative	What it achieves	Comment
<p><u>DFV Action Framework</u> (TTF) Living document. Started in 2020 and delivered in 2022, the Action Framework was developed in collaboration with TTF members and in consultation with: CA, Our Watch, eSafety, ACCAN, the ACMA, TIO, MensLine, Wesnet, Federal AGD, the DSS and others.</p> <p>The Framework consists of four DFV Action Plan options:</p> <ol style="list-style-type: none"> 1) <u>Adapt</u> 2) <u>Embed</u> 3) <u>Tailor</u> 4) <u>Influence</u> <p>Telcos complete the DFV Action Plan best suited (at that time) to their DFV strategy and learning. Signed off by the telco CEO, TTF assesses the telco DFV Action Plan Report and publishes a summarised version on the IIH website, as a public report.</p> <p>Each Action Plan option has minimum criteria telcos need to fulfill when developing their Plan.</p> <p>Telcos also provide a written Annual Update (eg an increase in the number of staff DFV-trained), also signed off by the telco CEO, assessed by TTF and made public.</p>	<p>The Telco Industry DFV Action Framework is a practical guide for telcos of any size or type to understand how they can better support domestic and family violence victims and survivors, and within their means, reduce instances of DFV across Australia.</p> <p>Following the process outlined in the Framework, telcos produce and implement a DFV Action Plan. Telcos are able to cycle through the four Action Plan options over time, to suit their DFV learning, progress and strategy. The Action Plan content is designed for continuous improvement.</p> <p>Telstra, Optus, Vocus Group, TPG Telecom, More Telecom, Tangerine, Vodafone, iiNet, Lebara, Internode, felix, Dodo, iPrimus and Aussie Broadband now have DFV Action Plans in place. <u>Their public reports can be seen here.</u> Six more telco Action Plans are under development.</p> <p>The Framework supports a best practice, continuous improvement, structured, integrated approach to effectively responding to DFV, referencing information and resources across government and industry, including from the ACMA, TIO, ACCAN, CA and others.</p>	<p>The TTF DFV Action Framework is available to telcos who are non-members, in recognition of the importance of the subject to society and helping CSPs of all sizes better support those affected by DFV.</p>
<p><u>The DFV Pledge</u> (TTF) Living document. Developed in 2022.</p>	<p>Signed by telco CEOs, the Telecommunications Industry DFV Pledge specifies four commitments:</p> <ol style="list-style-type: none"> a. Applying our organisational resources to support DFV customer and employee victims and survivors and, within our means, work to reduce instances of DFV in society. 	

Instrument or initiative	What it achieves	Comment
	<ul style="list-style-type: none"> b. Producing a Domestic and Family Violence Action Plan, within two years of the date of signing the pledge, using the DFV Action Plan Framework to inform our approach. c. Continuing to learn and revise our approach, mindful of the continually-changing nature of technology facilitated abuse (TFA). d. Collaborating with other signatories, through Telco Together Foundation, to share challenges and solutions and further build best practice". 	
<p><u>DFV and TFA Insights and Best Practice Forum (TTF)</u> Living action. Started in 2022 as 2 separate series, a quarterly <u>DFV Insights Series</u> for all DFV Pledgers, and a quarterly <u>Best Practice DFV and Technology Facilitated Abuse (TFA) Forum</u>, were combined in 2024 to open both up to more telcos and to include all DFV Pledgers.</p>	<p>The objectives of the (now combined) DFV and TFA Insights and Best Practice Forum are:</p> <ul style="list-style-type: none"> a. To increase the ability of participants to improve their DFV and TFA prevention or response by Learning from subject matter experts, change-makers and one another b. b. To discuss and explore challenges others have experienced, learning from each other and finding solutions. c. To lift the standard of DFV prevention/response across the industry d. To improve consistency in messaging across the industry. e. To avoid repetition and duplication of telco exploration and/or action 	<p>Presentations to date have been by industry, frontline support organisations, those with lived experience and DFV experts, on:</p> <ul style="list-style-type: none"> • <i>Golden Rules of DFV Response</i> • <i>TFA Red Flags and What To Do About Them</i> • <i>Vicarious Trauma</i> • <i>DFV Lived Experience</i> • <i>Adapt DFV Action Plan Support</i> • <i>Supporting Employees in the Workplace</i>
<p><u>TFA Lunch and Learn (2023)</u> (TTF) (one-off event, with 90+ participants)</p>	<p>Aim: to engage with a broad range of telco employees in support of increasing awareness of TFA, its impacts, and steps to prevent it (both for industry and for victim-survivors)</p>	<p>The event included presentations from:</p> <ul style="list-style-type: none"> • eSafety • Wesnet

Instrument or initiative	What it achieves	Comment
<u>DFV Support Register</u> (TTF) – under development	<p>Currently, there is no central database of the support options provided by telcos. The intention is for the DFV Support Register to include as many mainstream telcos as possible. Its objectives are to assist both frontline agencies (DFV support and law enforcement) and victim-survivors to understand what assistance and support is available.</p> <p>It is also designed to increase the visibility of the work telcos are doing to support DFV victim-survivors and encourage more telcos to take up the DFV Pledge and develop Action Plans.</p>	A draft has been circulated to frontline agencies, and their feedback is currently being incorporated into the next iteration. Technical challenges are also being considered at the moment. The next steps will be to pilot the Register in an active working environment with frontline agencies, identifying and addressing improvement opportunities.
<u>TFA Consumer Awareness Campaign</u> (TTF) – under development	<p>The draft campaign objectives are:</p> <ol style="list-style-type: none"> To increase consumer awareness of what abusive use of telco products and services looks like, especially in the context of coercive control by a current or former intimate partner. To increase awareness of personal responsibility for attitudes and behaviours. To aid telco frontline employees when supporting consumers experiencing tech abuse. To direct consumers to resources, further information and support. 	Being developed in conjunction with eSafety. Tabled for discussion with members at the next TTF DFV Roundtable in early July.
<u>Technology Facilitated Abuse (TFA) Forum</u> (TTF) – under consideration	<p>Primary objectives of this proposed forum are:</p> <ol style="list-style-type: none"> To create a mechanism for TFA action from telecommunications stakeholders across the industry. To harness and optimise existing and new technology resources from interlinked players, working collaboratively. 	

Instrument or initiative	What it achieves	Comment
	<p>c. To boost the work of eSafety and Our Watch.</p> <p>The National Plan recognises TFA and a telecommunications industry-led approach as essential to contributing to ending violence to women and children, but there is currently no plan for taking this from aspiration to fact.</p>	
<p>Telco industry roadmap</p> <p>including operational-level telco DFV Forum (CA, TTF and others TBA)</p> <p>Discussions are underway about how to improve collaboration and coordination of telco actions around managing DFV issues.</p> <p>CA and TTF have committed to a closer relationship to support this work.</p> <p>Wesnet has also expressed interest in being involved.</p>	<p>Efficiencies of scale and continual learning opportunities, allowing:</p> <ul style="list-style-type: none"> - further understanding of how to address issues, in a 'safe' environment - education - identifying gaps 	<p>Concepts being explored include:</p> <ul style="list-style-type: none"> - developing a telco industry DFV roadmap – to look at collaboration opportunities in this sector, and how they fit with work across the wider business and community, in connection with the work proposed by the DFSV Commissioner - collaboration on educational initiatives (e.g. for front line DFV assistance services or for consumers). - running an operational-level forum for sharing experiences, problems, challenges and solutions, similar to the Scam and Fraud Alliance and the good work being done by the NASC for support of people impacted by scams via their Communications and Awareness 'fusion cell'.

Table 2: Proposed mandatory DFV-related protections in the revised TCP Code (presented against each point in ACCAN's position paper)

The proposed new TCP Code has been substantially reviewed and revised, including in relation to vulnerable customers, with DFV specifically highlighted. (Note: This supports and complements the TTF DFV Action Framework.)

It requires that CSPs:

- have policies, processes and training in relation to DFV, as is appropriate to each CSP and each role within it,
- conduct general awareness training on DFV for all staff.
- ensure appropriate protection from disconnection for DFV-affected customers/end-users, including clear requirements about the information that can be requested from DFV-affected consumers and its retention.

A summary of DFV-related TCP clauses and related is presented below.

ACCAN Policy Position	How it is addressed in the revised TCP Code Proposed Drafting	
	Overview	Drafting
TRAINING		
<p>Mandate that CSPs work with a reputable training provider with DFV expertise annually to ensure they have the most up-to-date information on DFV issues.</p> <p>Require that CSP staff conduct regular specialist DFV training to ensure they are appropriately trained to assess consumer vulnerability and respond to consumers experiencing or at risk of DFV.</p> <p>Require that CSP staff undergo specific training to ensure that they prioritise the safety of consumers experiencing or at risk of DFV, and that this training</p>	<p>A new chapter has been included with a focus on organisation culture and governance, to foster a top-down and bottom-up approach to inclusive, fair and reasonable outcomes for customers: Chapter 2 sets out obligations in relation to organisational culture and governance. It obliges CSPs to provide company-wide training on DFV as well as more specific training for customer facing staff. This training must be completed on induction and as an annual refresher.</p> <p>The customer-facing training must include: a requirement to understand the legal and regulatory obligations as they relate to their role; common forms of DFV; include information to help staff understand DFV at a high level and how to safely respond to DFV in their role and manage DFV associated issues. It must also educate staff on vicarious trauma.</p>	<p>Chapter 2 Organisational Culture and Governance</p> <p>Organisational culture</p> <p>3.1.1 A CSP must have processes to support an organisational culture of compliance with the Code. [3.3.1]</p> <p>3.1.2 A senior executive for the CSP must oversee the implementation and operation of policies, supporting material, training, and resources to support compliance with this Code. [new]</p> <p>Staff training: company-wide</p> <p>3.2.2 To support a culture of compliance with this Code, CSPs must provide company-wide staff training on the Code, including awareness of: [3.3.3]</p> <p>...</p> <p>(c) DFV; [new]</p> <p>...</p> <p>2.2.3 Company-wide staff training must occur: [new]</p> <p>(a) at induction; and</p> <p>(b) as an annual refresher.</p> <p>Staff training: customer facing staff</p>

ACCAN Policy Position	How it is addressed in the revised TCP Code Proposed Drafting	
	Overview	Drafting
be developed in cooperation with a reputable training provider with DFV expertise.	<p>The Code includes guidance to work with a reputable training provider with DFV expertise.</p> <p>There is also an obligation to review the effectiveness of training.</p>	<p>3.2.4. Company-wide training must be supplemented by appropriately tailored training to suit their specific roles and responsibilities for relevant customer facing staff and their managers on compliance with this Code. This includes training on: (</p> <p>...</p> <p>(d) DFV; and [new] Note: this includes (if relevant) all customer facing staff, specialist DFV staff and staff working in areas likely to deal with DFV-related issues (e.g. sales, credit management, debt management, collections, financial hardship, fraud, privacy and escalated complaints management) [new]</p> <p>3.2.5. Customer facing staff training must occur: [new]</p> <p>(a) at induction to a role; and</p> <p>(b) as an annual refresher.</p> <p>Chapter 4 – Supporting the Consumer</p> <p>Domestic and Family violence – customer facing staff training</p> <p>4.2.9. When developing appropriately tailored DFV training for relevant customer facing staff and their managers, a CSP must: [new]</p> <p>(a) ensure staff understand the specific legal and regulatory obligations relevant to their role as they relate to DFV; [new]</p> <p>(b) educate staff on common forms of DFV associated with a telecommunications good or service; [new]</p> <p>(c) include information to help staff: [new]</p> <p>(i) understand (at a high level) the nature and impact of DFV; [new]</p> <p>(ii) recognise and safely respond to DFV as it is likely to present to them, in their role; and [new]</p> <p>(iii) manage and safely respond to DFV-associated issues; [new]</p> <p>(d) ensure staff are familiar with all relevant policies and support materials; and [new]</p> <p>(e) educate staff on vicarious trauma. [new]</p> <p><i>Staff training</i></p> <p><i>Working with a reputable training provider with DFV expertise to develop and review DFV staff training will allow training material to reflect both current best practice on DFV-specific issues and a CSP's company-specific needs (e.g. to support a CSP's</i></p>

ACCAN Policy Position		How it is addressed in the revised TCP Code Proposed Drafting
	Overview	Drafting
		<p>policy and supporting materials). A list of DFV training providers is found in G660 Assisting Consumers Affected by Domestic and Family Violence Industry Guideline, Appendix 3: Training resources for RSPs.</p> <p>Monitoring 3.2.8. A CSP must have processes to review the effectiveness of training associated with TCP Code compliance and make relevant changes as required. [new]</p>
REPORTING		
Stated position	Overview	Drafting
Require that CSPs report to the ACMA on their performance concerning the support they provide to consumers experiencing or at risk of DFV.	<p>Strengthened and new reporting provisions are included in chpt 10.</p> <p>The ACMA has the powers under s521 to request information on CPS' processes /compliance etc. It can and does request information.</p> <p>Having enforceable provisions in the TCP Code supports a more comprehensive solution than direct regulation, as it ensures that ALL CSP's are audited on TCP Code compliance annually. This includes auditing on specific identified issues each year, as identified by CommCom in conjunction with stakeholders including the ACMA and ACCAN.</p> <p>Where the auditor (CommCom) identifies issues, it can work with the CSP to correct them (in set timeframes). Where there is serious non-compliance, or the CSP fails to address more minor issues in the timeframes directed by CommCom, CommCom escalates to the ACMA for action.</p> <p>This work complements and supports the ACMA's more targeted auditing and enforcement regime.</p>	<p>Reporting is required to CommCom as per updated Compliance Assessment Report.</p> <p>Specific process metrics/reporting are proposed in relation to vulnerable consumers and DFV, including in relation to training, support, DFV specifically, policies, governance, monitoring (see section 10.2)</p> <p>CommCom already reports /escalates to the ACMA on TCP Compliance issues. These arrangements are clearer in the redrafted chpt 10.</p>

ACCAN Policy Position	How it is addressed in the revised TCP Code Proposed Drafting	
	Overview	Drafting
POLICIES, SYSTEMS and PROCEDURES and REGULATORY APPROACH		
<p>Direct regulation should require CSPs to have policies, systems, and procedures in place that:</p> <ul style="list-style-type: none"> • Remove requirements for consumers to provide proof to CSPs when experiencing or at risk of DFV. • Avoid the need for consumers to repeatedly disclose experience of DFV. • Require that CSPs have easily accessible information for consumers experiencing or at risk of DFV. • Effectively support authorised representatives (ARs) to assist consumers experiencing or at risk of DFV. • Require that CSPs identify and provide flexible and tailored assistance to consumers experiencing DFV. 	<p>This co-regulatory approach allows for a more comprehensive solution than the blunt mechanisms afforded through direct regulation, with a far more comprehensive check of compliance than the ACMA could achieve alone. Combined with the collaborative approach evident in the guideline development, it should lead to continual improvement and better consumer outcomes than we believe could be achieved through any other regulatory approach.</p> <p>See also comments on review, revision and auditing.</p> <p>The proposed revised Code includes obligations for a CSP to have policies and supporting materials and training on DFV that: emphasises safety, is trauma-informed, set out how the CSP will identify and support customers; aligns with other obligations. The policy must ensure that communication channels, support and escalation requirements are clear and accurate.</p> <p>The CSP must not require evidence as a pre-requisite for assistance. Where a CSP requires information it must only be to support compliance with other legal/reg obligations.</p> <p>The Customer Service chapter sets out obligations for CSPs with case management</p>	<p>Supporting consumers affected by domestic and family violence</p> <p>4.2.3. A CSP must have and implement policies and supporting materials on DFV. [new]</p> <p>4.2.4. A CSP's DFV policies, supporting materials, and training must: [new]</p> <p>(a) emphasise safety (of the affected consumer and CSP staff); [new]</p> <p><i>Note: It is never appropriate for a CSP to require that a consumer be required to involve their alleged perpetrator in any discussion. Such actions could put lives at risk.</i></p> <p>(b) be trauma-informed; [new]</p> <p>(c) include information on common forms of DFV associated with a telecommunications good or service; [new]</p> <p>(d) clearly set out how the CSP will identify and support consumers affected by DFV; [new]</p> <p>(e) ensure that a CSP's obligations, communication channels, support and escalation requirements (external and internal) are clear and accurate; and [new]</p> <p>(f) align with and appropriately reference mandatory consumer obligations under other instruments (e.g. the Financial Hardship Standard). [new]</p> <p>4.2.5. A CSP must not require evidence of DFV as a pre-requisite for general assistance and support under the CSP's DFV policy. [new]</p> <p>4.2.6. A CSP may require specific information to support particular actions under their DFV policy, to support compliance with other legal or regulatory obligations. [new]</p> <p><i>Note: For example, this may include a statutory declaration or letter from a support service to establish their circumstances, or information to establish that the requesting party is the end-user of a service, when undertaking a rights of use change for a service or investigating fraud.</i></p> <p>4.2.7. Where further information is requested under cl 4.2.6, a CSP must only request and retain the minimum amount of information to meet their legal or regulatory obligations. [new]</p> <p><i>Note: CSPs should request and retain 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 the request.</i></p> <p>4.2.8. A CSP must publish on its website a list of one or more external DFV support services. [new]</p> <p>Developing a response to DFV</p>

ACCAN Policy Position	How it is addressed in the revised TCP Code Proposed Drafting	
	Overview	Drafting
<ul style="list-style-type: none"> Require that CSPs provide appropriate assistance to consumers at risk of DFV e.g. safety planning, assisting the victim-survivor in setting up new accounts, splitting up joint accounts, securing their information, even if the violence may have temporarily stopped. 	<p>processes to ensure they have been designed to prioritise customer outcomes, with specific guidance that DFV customers may need to avoid the need to repeat details of their situation.</p>	<p><i>It is important that DFV policies, supporting materials and training is company-specific to ensure a safe and comprehensive DFV response, as it facilitates a response that fits the organisation's size, structure, and way of operating. Additionally, policies, supporting materials and training should make it clear that a flexible response to assisting consumers affected by DFV is necessary; there is not a 'one-size-fits-all' solution, the safe and appropriate response can vary depending on the consumer's circumstances. For detailed guidance for CSPs on how to manage DFV and how to develop comprehensive, company-specific DFV policies, supporting materials and training, see Industry Guideline G660: Assisting Consumers Affected by Domestic and Family Violence</i></p> <p>Customer Service</p> <p>7.1.5 Where a CSP has a case management process, it must ensure the process has been designed to prioritise customer outcomes. [new]</p> <p><i>Note: prioritising outcomes will depend on the issues being managed. For example, case management for customers affected by DFV would be different to that for a customer with a technical issue. It may include processes to avoid or minimise the need for a customer to constantly repeat details of their situation or problem and consider the compromise between repetition of the issue and wait time.</i></p>
CREDIT MANAGEMENT PROCESSES		
<p>Direct regulation should require CSPs to have policies, systems, and procedures in place that:</p> <ul style="list-style-type: none"> Provide for the review of whether expenditure attached to an account can be ascribed to economic abuse or has been exacerbated by DFV, and where this is the case, limit, flag or quarantine the account and provide tailored relief to the consumer as appropriate. 	<p>Any Financial Hardship obligations now sit within the FH Standard.</p> <p>However, the proposed TCP Code does include obligations to protect DFV customers from disconnection. It also includes obligations relating to circumstances where a failure to pay a debt was a result of DFV.</p> <p>Information about (and the definition of) Authorised Representative and Advocates has been updated/made clearer. And there are obligations included to ensure appropriate support for consumers and their AR or advocate (including vulnerable consumers, such as those affected by DFV) It is unclear what the ACCAN proposes in terms of strengthening authority,</p>	<p>Protecting consumers affected by DFV from disconnection</p> <p>9.1.4. Once a CSP becomes aware a consumer is affected by DFV, it must make best efforts to protect the affected person's telecommunications service(s) from disconnection by the CSP. [new]</p> <p><i>Note: 'Protecting from disconnection' does not mean that a service cannot be disconnected or that it must be maintained in perpetuity. Rather, it means that the CSPs has protections in place to shield a DFV-affected customer or end-user from unwanted disconnection while their matter is being actively managed by the CSP, noting that some DFV-affected end-users, may wish to have their service disconnected (including for safety reasons).</i></p> <p>9.1.5. A CSP must have processes in place to ensure the telecommunications service(s) of a DFV-affected end user is not disconnected or ported while the CSP is managing a rights of use dispute. [new]</p> <p>Protecting a DFV-affected person's service from disconnection</p>

ACCAN Policy Position	How it is addressed in the revised TCP Code Proposed Drafting	
	Overview	Drafting
<ul style="list-style-type: none"> Require CSPs to undergo a rigorous review process prior to disconnecting a consumer experiencing or at risk of DFV. Strengthen the authority of ARs when interacting with CSPs on behalf of consumers experiencing or at risk of DFV. 	<p>without putting the consumer at risk of scam or fraud.</p> <p>More information on appropriate support is provided in the DFV Guideline and in the Authorised Rep and Advocate Industry Guidance (IGN 017) (in review pending TCP Code changes)</p>	<p><i>Exemptions to right of use rules are available to allow for the separation and transfer of the end-user's number where that end-user is affected by DFV. Under the C566 Number Management – Use of Numbers by Customers Industry Code, processes must be in place to terminate the right to the customer's use of the number where they are a perpetrator of DFV, disassociate the number(s) from the perpetrator's account, and transfer the number to the DFV-affected person. See C566 Number Management – Use of Numbers by Customers Industry Code and G660 Assisting Consumers Affected by Domestic and Family Violence Industry Guideline, for details.</i></p> <p>Disputed defaults, consumers affected by DFV</p> <p>9.6.3. Where a debt has been default listed and the customer's circumstances indicate DFV may be present, a CSP should consider the effect of DFV on the associated debt. Where it is identified by the CSP that the failure to pay was through no fault of the customer due to DFV: [new]</p> <p>(a) the default should be considered as listed in error; and [new]</p> <p>(b) the CSP must use reasonable endeavours to inform the credit reporting body within 1 working day.</p> <p><i>Disputed defaults and DFV</i></p> <p><i>For detailed guidance for CSPs on how to manage disputed defaults and DFV see Industry Guideline G660: Assisting Consumers Affected by Domestic and Family Violence. Additionally, Clause 16 of the Principles of Reciprocity and Data Exchange (PRDE, the credit reporting data exchange rules) contains exemptions for cases of DFV or elder abuse.</i></p>
Severability of Accounts		

ACCAN Policy Position	How it is addressed in the revised TCP Code Proposed Drafting	
	Overview	Drafting
<ul style="list-style-type: none"> Require CSPs to draft contracts going forward that allow for the severability of accounts, which enable DFV victim-survivors to sever their number from the perpetrator's account (and vice versa).¹⁴ 	<p>Exceptions to rights of use rules are available to allow for the separation and transfer of the end-users number under C566 Number Management – Use of Numbers by Customers Industry Code.</p> <p>The proposed TCP Code strengthens these obligations by ensuring a CSP has processes to ensure DFV-affected end users are not disconnected while a CSP is managing a rights of use dispute.</p>	<p>Protecting consumers affected by DFV from disconnection</p> <p>9.1.4. Once a CSP becomes aware a consumer is affected by DFV, it must make best efforts to protect the affected person's telecommunications service(s) from disconnection by the CSP. [new]</p> <p><i>Note: 'Protecting from disconnection' does not mean that a service cannot be disconnected or that it must be maintained in perpetuity. Rather, it means that the CSPs has protections in place to shield a DFV-affected customer or end-user from unwanted disconnection while their matter is being actively managed by the CSP, noting that some DFV-affected end-users, may wish to have their service disconnected (including for safety reasons).</i></p> <p>9.1.5. A CSP must have processes in place to ensure the telecommunications service(s) of a DFV-affected end user is not disconnected or ported while the CSP is managing a rights of use dispute. [new]</p> <p>Protecting a DFV-affected person's service from disconnection</p> <p><i>Exemptions to right of use rules are available to allow for the separation and transfer of the end-user's number where that end-user is affected by DFV. Under the C566 Number Management – Use of Numbers by Customers Industry Code, processes must be in place to terminate the right to the customer's use of the number where they are a perpetrator of DFV, disassociate the number(s) from the perpetrator's account, and transfer the number to the DFV-affected person. See C566 Number Management – Use of Numbers by Customers Industry Code and G660 Assisting Consumers Affected by Domestic and Family Violence Industry Guideline, for details.</i></p>