Central Consumer Protection Authority

Krishi Bhawan, New Delhi - 110001

Case No: YY-2/4/2025-CCPA

In the matter of: Use of dark patterns resulting in unfair trade practices, misleading advertisements, and violation of consumer rights by McAfee Software India Private Limited.

CORAM:

Smt. Nidhi Khare, Chief Commissioner

Shri Anupam Mishra, Commissioner

Appearances:

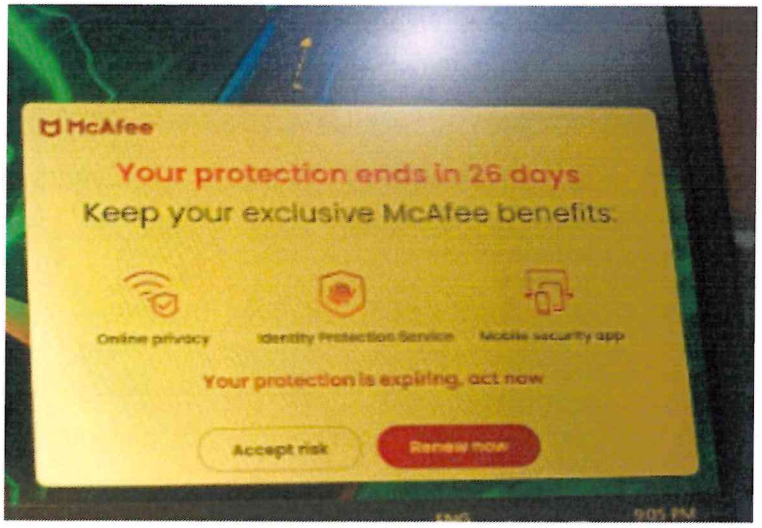
For McAfee Software India Private Limited:

1. Grace Quek, representative of the company
2. Nav Dhawan and Sanjana Srivastava, Advocates

Date: 20.05.2026

ORDER

1. CCPA has received a representation from Mr. Krishna Nigam, Advocate, Your Commercial Attorney, dated 01st September 2025 regarding the renewal notifications used by McAfee, alleging use of dark pattern practices that undermine consumer autonomy during subscription renewal. The representation was accompanied by a snapshot of the interface as supporting evidence which is reproduced below for ready reference:



2. In the representation, it was alleged that the instead of providing a fair and transparent choice such as *Cancel* or *Skip*, the notification restricts the consumer to only two choices:

A. Accept Risk

B. Renew Now

He further stated that this design is a manipulative dark pattern, specifically falling within the category of "Confirm Shaming" as defined under the CCPA guidelines. It forces consumers into renewing the service by equating non-renewal with irresponsibility or recklessness ("Accept Risk"), thereby depriving consumers of a neutral and informed choice. Such practices not only mislead the consumers but also amount to unfair trade practices, directly contravening consumer protection framework laid down by the Government of India.

3. Accordingly, in exercise of the powers under Sections 18 and 19 of the Consumer Protection Act, 2019 (hereinafter referred to as "the Act"), CCPA conducted a preliminary inquiry to examine whether the aforesaid practices violate the provisions of the Act especially violation of consumer rights, unfair trade practice, or misleading advertisement.

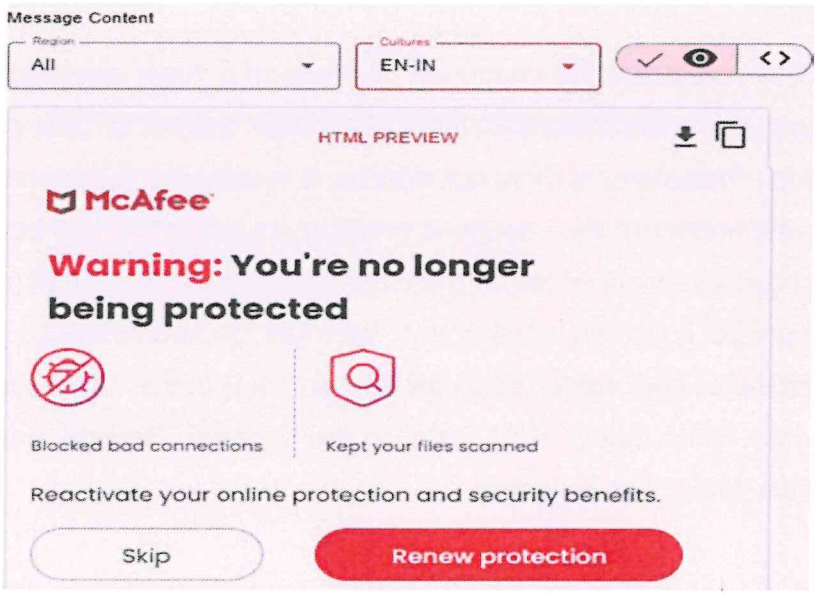
4. It is important to note that the impugned renewal interface was not confined to a singular or isolated transaction, but formed part of a standard interface design which might be deployed across the platform for all similarly placed consumers. The use of fear-based prompts such as "Accept Risk" coupled with the absence of a clear and neutral opt-out mechanism appears to have the effect of systematically influencing consumer choice and decision-making process. Such interface design appears to be capable of nudging consumers towards subscription renewal by creating an impression that refusal to renew would expose them to security vulnerabilities or unsafe digital conditions. CCPA further observed that the impugned interface was not a mere contractual arrangement between individual consumers and the opposite party, but a uniform digital design affecting class of consumers interacting with the renewal system of the platform.

5. Dark patterns incorporated within digital interfaces often operate in a psychological manner, due to which consumers may not individually recognise, report, or challenge such manipulative practices despite being adversely affected by them. Consequently, absence of individual complaints cannot be construed as absence of

consumer harm, particularly where the interface itself is designed to influence consumer behaviour through coercive or manipulative choice design.

6. In view of the above, the practice therefore appears to be possessed with the necessary element of commonality and widespread consumer impact so as to attract the jurisdiction of the CCPA under the Act for class action. Therefore, impugned renewal interface prima facie appears to be misleading, unfair trade practice and violation of consumer rights under the Act read with Guidelines for Prevention and Regulation of Dark Patterns, 2023.

7. Accordingly, a Show Cause Notice dated 4th December 2025 was issued to the opposite party, directing it to submit its response along with supporting documents. In response to the Notice the opposite party vide letter dated 19th December, 2025 submitted that the India renewal interface has been modified and a neutral or opt-out option, namely "Skip", has now been incorporated. The company also expressed its appreciation to the CCPA for bringing the concerns regarding the renewal interface to its attention.



8. The response submitted by the opposite party was examined by CCPA. It was observed that although the opposite party stated that the renewal interface had subsequently been modified and a neutral "Skip" option had been introduced, the response did not adequately address the issues raised in the Show Cause Notice including explanation for the design of the renewal interface, steps taken to ensure compliance with consumer protection laws. However, the response furnished by the

opposite party was substantially limited to the assertion that the interface had now been modified after receipt of the Notice.

9. CCPA further observed that the subsequent introduction of a neutral "Skip" option by the opposite party after issuance of notice establishes that the earlier interface lacked a fair and transparent opt-out mechanism. Such post-facto corrective action, though relevant for future compliance, does not extinguish liability arising from the earlier deployment of manipulative interface practices which might have already impacted consumers on a large scale and warranted closer examination regarding their impact on consumers during the relevant period.

10. Accordingly, upon consideration of the interface design, the representations conveyed therein, the scale of deployment, and the potential impact on consumer autonomy and informed decision-making, the CCPA was satisfied that a prima facie case was made out under Sections 2(28), 2(47), and 2(9) of the Consumer Protection Act, 2019 read with Clauses 3 and 4 of the Guidelines for Prevention and Regulation of Dark Patterns.

11. CCPA notes that the impugned interface may have operated systematically across the platform and potentially affected a large number of consumers prior to its modification. Therefore, CCPA considered it necessary to ascertain the scale, duration, and impact of the impugned practice, including the number of consumers who may have been influenced by the interface design and the extent to which such design impaired consumer choice and informed decision-making. Accordingly, in exercise of the powers conferred under Section 19(1) of the Act, the matter was thus referred vide letter dated 08.01.2026 to the Director General (Investigation) for conducting a detailed investigation.

12. The Director General (Investigation) in its investigation report dated 20th February, 2026 submitted the following:

i. Confirm Shaming: Base on the response McAfee admits that the prior renewal interface used "Accept Risk" messaging, a classic Confirm Shaming tactic by framing opt-out as risk acceptance to emotionally pressure users. Subsequently upon receipt of CCPA notice changes were made only on December 16, 2025 - post CCPA notice which indicates that McAfee has found violating design existed during the relevant period which amounts to indulgence

and non- compliance to dark pattern as per Clause 3 of the Dark Patterns Guidelines, 2023.

ii. Forced Action & Skip Option Rollout: McAfee confirms the renewal prompt lacked neutral opt-out options, forcing users to accept or dismiss by manipulative actions. Wherein the company made the correction post-notice by changing the "Accept Risk" option with a "Skip" option, this proves the interface coerced specific actions prior to the notice date. Evasion of "relevant time" does not negate the admitted prior Forced Action design, violating Clause 4 of the Dark Patterns Guidelines, 2023.

iii. McAfee states "Skip" or "No, thanks" was added on December 16, 2025, with evidence partially shared on December 18, but fails to confirm uniform rollout across all platforms/devices. Post-CCPA notice, timing of changes evidences absence of neutral options before mid-December 2025. "All updates live" claim lacks proof of prior compliance or full implementation details.

iv. Consumer Subscriptions Evidence: McAfee admits no documentary evidence exists proving subscriptions/renewals directly resulted from the challenged interface, failing to disprove harm. Absence of data supports presumptive misleading practices under the Consumer Protection Act, 2019, as dark patterns were designed to drive unintended renewals.

v. Consumer Complaints: McAfee claims no records exist of consumer complaints related to coercive renewal prompts or absent opt-out options in the past 12 months, despite acknowledging occasional inquiries about renewals and auto-renewals. This absence of documented complaints does not disprove the coercive nature of the interface, as dark patterns are designed to evade overt objections while subtly pressuring users into unintended actions.

vi. Systemic Interface Feature: McAfee confirms the "Accept Risk" messaging - a systemic renewal interface feature - was updated only after CCPA notice, replacing it with "No, thanks," "Skip," or removal from non-critical alerts, with all updates now live. This admission evidences the feature's widespread prior deployment across their systems, persisting until mid-December 2025. The reactive remediation and vague "monitoring" claim fail to verify pre-notice compliance and disprove ongoing systemic dark patterns before the mandated changes.

vii. Internal Compliance Processes: McAfee fails to disclose the "established policies" guiding internal operations and external marketing by not providing documentary evidence of specific checks, audits, or processes aligned. This

non-specific response evades substantive disclosure, implying inadequate prior oversight that allowed Confirm Shaming and Forced Action violations to persist until post-notice. Failure to produce verifiable compliance mechanisms evidences systemic non- compliance during the violation period as per Consumer Protection Act, 2019, or Dark Patterns Guidelines, 2023.

viii. Conclusion: In view of the findings recorded, it is conclusively established that M/S McAfee Software India Private Limited has violated multiple provisions of the Consumer Protection Act, 2019, as well as the Guidelines for Prevention and Regulation of Dark Patterns, 2023.

ix. McAfee's admitted use of "Accept Risk" messaging and absent neutral opt-out options in the renewal interface as these manipulative designs systematically deceived consumers into unintended renewals through coercive prompts and emotional pressure, exploiting vulnerabilities for commercial gain. This constitutes unfair trade practices under Section 2(47) of the Consumer Protection Act, 2019,

x. The McAfee interface amounts to misleading advertisements by concealing critical opt-out information and employing fear-based inducement, framing non-renewal as security "risk" which obscured material facts and induced decisions through false urgency, persisting systemically until post-CCPA notice remediation on December 16, 2025. These practice show non-compliance under Section 2(28) of the CP Act, 2019.

xi. McAfee's reactive changes, evidentiary evasions, absent compliance proofs, and failure to disprove harm directly violate Clause 3 (Confirm Shaming) and Clause 4 (Forced Action) of the Guidelines for Prevention and Regulation of Dark Patterns, 2023.

13. The report of the Director General (Investigation) was shared with the opposite party vide letter dated 16.03.2026 for their comments.

14. The opposite party vide dated 26.03.2026 furnished its comments on DG (Inv. Report) wherein it made the following submissions:-

i. Phrase “Accept Risk” used in the renewal interface merely reflected the ordinary consequence that protection under the cybersecurity subscription would lapse upon expiry of the subscription period. It was contended that the wording did not introduce any false, exaggerated, or misleading representation and that the product by its very nature is intended to safeguard users from

cyber-attack risks. The expression was therefore contextual in nature and could not be construed as an attempt to mislead or emotionally manipulate consumers. The opposite party further submitted that the impugned interface was shown only to existing users in a subscription renewal context, who were already familiar with the nature and functionality of the product, and therefore the interface neither misled consumers nor impaired their decision-making autonomy.

ii. With regard to the allegation of "Confirm Shaming", the opposite party submitted that the essential element of deceptive inducement under the Guidelines for Prevention and Regulation of Dark Patterns, 2023 was absent in the present case, as the wording merely communicated the consequence of expiry of cybersecurity protection and did not create any artificial fear or false urgency. The opposite party therefore denied that the interface amounted to "Confirm Shaming" within the meaning of Clause 3 of the Guidelines.

iii. In relation to the allegation of "Forced Action", the opposite party submitted that users were not compelled to renew their subscriptions in order to continue using the product during the subsisting subscription period. It was further submitted that users retained the ability to dismiss the interface and proceed further, including through the "X" button located at the top-right corner of the interface. The opposite party also submitted that no complaints relating to the renewal interface were received from consumers during the period between 01.01.2025 and 31.12.2025. On this basis, it was contended that the interface did not satisfy the threshold of compulsion, conditional access, or coercion necessary to constitute "Forced Action" under Clause 4 of the Guidelines.

iv. The opposite party further denied that the impugned interface amounted to an unfair trade practice under Section 2(47) of the Consumer Protection Act, 2019. It was submitted that the interface did not adopt any deceptive practice or unfair method for promoting subscription renewals, as consumers were neither misled regarding any material aspect of the service nor compelled to renew their subscriptions. According to the opposite party, the interface merely presented renewal-related information to existing subscribers and did not impair consumer choice or autonomy.

v. The opposite party also denied that the impugned interface constituted a misleading advertisement under Section 2(28) of the Act. It was submitted that the interface neither falsely described the service nor concealed any material information from consumers. According to the opposite party, users retained

the ability to decline renewal and continue further by dismissing the interface, and therefore the absence of a separately labelled "Skip" option did not amount to concealment of important information or misleading representation.

vi. Without prejudice to the aforesaid submissions, the opposite party stated that upon being apprised of the concerns raised by the CCPA, it undertook an immediate review of the interface and on 16.12.2025 modified the renewal interface by incorporating neutral opt-out options such as "No Thanks" and "Skip" and by removing the earlier phrasing from non-critical alerts. The opposite party submitted that the earlier wording identified in the investigation report has not been used thereafter and that the company has cooperated fully with the inquiry by furnishing information and documents sought by the Authority.

vii. The opposite party further relied upon the matter concerning InterGlobe Aviation Limited before the CCPA to contend that in a comparable proceeding involving allegations relating to dark patterns and confirm shaming, no monetary penalty had been imposed in view of prompt corrective measures undertaken by the company. The opposite party therefore submitted that no penalty ought to be imposed in the present case and, in the alternative, any penalty imposed should remain limited and proportionate considering that the impugned interface was operational only during a limited period, was shown only to existing users, and no consumer complaints had allegedly been received in relation thereto.

15. Thereafter, hearing was scheduled on 27.03.2026 during which Grace Quek, Nav Dhawan and Sanjana Srivastava, Advocates appeared on behalf of the opposite party and made the following submissions:

i. The impugned interface did not amount to "forced action" or "confirm shaming" under the Guidelines for Prevention and Regulation of Dark Patterns, 2023. It was contended that the consumer's ability to continue with the existing subscription without renewal was never blocked and that there existed no "roadblock" compelling the consumer to purchase the renewed subscription. The company argued that the option to decline renewal remained available through the "Accept Risk" button and additionally through an "X" icon placed at the top-right corner of the prompt window enabling closure of the interface. It was submitted that no undesired action was mandatorily required to be

undertaken by the consumer in order to proceed further and therefore the essential ingredients of "forced action" were not satisfied.

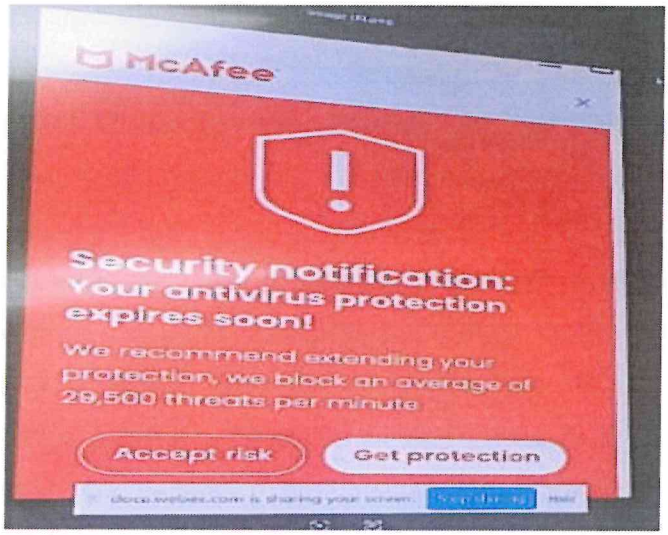
ii. They further submitted that the phrase "Accept Risk" merely reflected the natural consequence of expiry of antivirus protection and constituted a descriptive warning intended to notify consumers that their devices may become vulnerable to cyber threats after expiry of the subscription. It was argued that the wording used was factually accurate and did not amount to emotional manipulation or coercion. The company also submitted that users of antivirus software are generally technologically literate and familiar with standard interface conventions, including the placement of the "X" symbol for closure of windows and prompts.

iii. No complaints had been received by the company during the period from 01.01.2025 to 31.12.2025 alleging deception, forced renewal or manipulation arising out of the impugned interface. Reliance was also placed upon proceedings involving IndiGo concerning alleged confirm shaming in travel insurance prompts, wherein corrective modifications were undertaken and no directions under Sections 20 or 21 of the Consumer Protection Act, 2019 were ultimately issued. Drawing parity with the said matter, the company submitted that prompt corrective measures had already been undertaken in the present case as well and therefore no further action was warranted.

16. During the hearing, CCPA observed that the impugned interface through the use of expressions such as "Renew Now" and "Accept Risk" created a sense of fear and urgency regarding expiry of protection. The CCPA noted that such wording and interface design could manipulate consumers into selecting the option preferred by the opposite party instead of enabling a neutral and informed choice. CCPA further observed that the consumer's choice could have been presented in a simple and neutral manner through plain options such as "Yes" or "No", without employing emotionally loaded terminology.

17. Thereafter, CCPA specifically queried the opposite party regarding the absence of any visible "X" or close option in the screenshot annexed with the Notice. In response, the opposite party acknowledged that the close option was not visible in the particular screenshot under consideration, though it sought liberty to verify whether such option appeared upon hovering the cursor over the relevant area. The CCPA observed that even in the demonstrative examples subsequently shown by the

opposite party during the hearing, alleged "X" or close option appeared in a subdued grey colour, whereas the renewal-related options, including "Accept Risk", were displayed more prominently with a red background, thereby potentially steering or influencing consumer choice towards renewal. CCPA noted that such visual presentation could impair the consumer's ability to exercise a free and neutral choice.



18. CCPA noted that once the interface had already communicated that the consumer's protection would expire within a specified number of days, the repeated use of expressions such as "Accept Risk" unnecessarily amplified fear and pressure upon the consumer. CCPA also noted that reliance upon the technological literacy of users cannot justify interface designs which are capable of nudging or manipulating consumer decision-making through visual prominence, fear-based wording or asymmetrical presentation of options.

19. During the abovementioned hearing, CCPA directed the opposite party to furnish details regarding the number of existing users/subscription renewals.

20. Thereafter, vide submission dated 01.04.2026, opposite party submitted the following:-

i. A total of 3,55,133 subscription renewals were recorded during the period from January 2025 to December 2025, and that the said data substantially pertained to the period prior to the modification of the subscription renewal interface on 16.12.2025.

ii. The opposite party further submitted that no complaints had been received from consumers during the aforesaid period specifically concerning the wording or presentation of the "opt-out" option in the impugned interface.

21. It is important to note that Section 2(47) of the Consumer Protection Act, 2019 defines "unfair trade practice" as-

> *"(47) "unfair trade practice" means a trade practice which, for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice including any of the following practices, namely:..*
>
> *(f) makes a false or misleading representation concerning the need for, or the usefulness of, any goods or services"*

22. The abovementioned provision uses the expression "including", thereby making it clear that the categories listed therein are illustrative and not exhaustive in nature. Therefore, any unfair method or unfair or deceptive practice which has the effect of impairing consumer choice, influencing consumer decision-making through unfair means, or inducing consumers into unintended transactions would fall within the definition of "unfair trade practice" under the Act.

23. In the present case, the impugned renewal interface formed part of the opposite party's subscription renewal mechanism and was deployed for the purpose of promoting renewal and continued sale of its cybersecurity services. The use of fear-based terminology such as "Accept Risk", coupled with the visual prominence accorded to the "Renew Now" option and absence of a neutral and equally prominent opt-out mechanism during the relevant period, constituted a deceptive and manipulative trade practice.

24. CCPA further notes that Section 2(47) (f) specifically recognizes as an unfair trade practice any false or misleading representation concerning the need for, or usefulness of, any goods or services. In the present case, by framing the consumer's decision not to renew the subscription as "Accept Risk", the opposite party conveyed an express and implied representation that non-renewal of its antivirus subscription would necessarily expose the consumer's device to security threats, unsafe digital conditions or heightened cyber risks requiring immediate continuation of the service.

Such representation was not merely descriptive in nature but was designed to create fear and apprehension regarding the consequences of non-renewal.

25. CCPA observes that there is no material on record or guarantee from the opposite party that failure to renew its subscription service would necessarily result in compromise of the consumer's device or exposure to cyber threats. Equally, the opposite party cannot guarantee that usage of its antivirus software would completely eliminate all risks relating to viruses, malware or other cybersecurity vulnerabilities. The impugned expression therefore created an exaggerated and misleading impression regarding the usefulness and need of the opposite party's services by portraying non-renewal itself as acceptance of danger or insecurity. Such fear-based representation manipulated consumer perception concerning the necessity and usefulness of the service and thereby falls within Section 2(47) Act.

26. Section- 2 (28) of the Act defines "*misleading advertisement*". Definition is reproduced below for ready reference:-

> *(28) "misleading advertisement" in relation to any product or service, means an advertisement, which-*
>
> *i. falsely describes such product or service; or*
>
> *ii. gives a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; or*
>
> *iii. conveys an express or implied representation which, if made by the manufacturer or seller or service provider thereof, would constitute an unfair trade practice; or*
>
> *iv. deliberately conceals important information;*

27. As mentioned above, definition of "misleading advertisement" include any advertisement which conveys an express or implied representation that would constitute an unfair trade practice if made by the manufacturer, seller or service provider. The impugned renewal interface, although embedded within the subscription renewal flow of the digital platform, was promotional and commercial in character as it was specifically designed to encourage and induce consumers to renew and continue availing the services of the opposite party.

28. The interface conveyed express and implied representations that non-renewal of the subscription would amount to acceptance of security risks and exposure to unsafe digital conditions, while renewal of the subscription would necessarily safeguard the consumer from such risks. Such representations, conveyed through the

expression "Accept Risk" and the overall manipulative design design of the interface, distorted the consumer's perception regarding the necessity and effectiveness of the service and induced consumers. Since the said representations themselves constitute unfair trade practices within the meaning of Section 2(47) of the Act, the impugned interface also amounts to a misleading advertisement under Section 2(28)(iii) of the Consumer Protection Act, 2019.

29. The Consumer Protection (E-Commerce) Rules, 2020 have been framed under the Consumer Protection Act, 2019 with the objective of ensuring transparency, fairness and protection of consumer rights in digital and online marketplace. The said Rules impose statutory obligations upon e-commerce entities to refrain from adopting unfair trade practices and to ensure that consumer consent for purchase decisions is obtained through explicit, informed and affirmative action. CCPA notes that the impugned renewal interface was deployed through a digital platform operated by the opposite party and therefore attracts the obligations cast upon e-commerce entities under the Consumer Protection (E-Commerce) Rules, 2020.

30. Rule 4(3) of the said Rules provides that no e-commerce entity shall adopt any unfair trade practice, whether in the course of business on its platform or otherwise. The use of fear-based wording such as "Accept Risk", coupled with the absence of a neutral and equally prominent opt-out mechanism during the relevant period, influenced consumer decision-making through manipulative interface design and constitutes an unfair trade practice within the meaning of the aforesaid Rule read with Section 2(47) of the Consumer Protection Act, 2019.

31. CCPA also observes that Rule 4(9) of the Consumer Protection (E-Commerce) Rules, 2020 mandates that consent for purchase of goods or services must be obtained only through explicit and affirmative consumer action. The design of the impugned renewal interface, by presenting consumers with uneven and psychologically loaded choices such as "Renew Now" and "Accept Risk" instead of neutral alternatives, impaired free and informed consumer consent in relation to subscription renewal decisions. The visual prominence accorded to the renewal option, coupled with fear-inducing terminology, cannot be regarded as a fair mechanism for obtaining explicit and voluntary consumer consent as contemplated under the said Rules.

32. It is important to note that prior to issuance of the Guidelines for Prevention and Regulation of Dark Patterns, 2023, the Department of Consumer Affairs and CCPA undertook detailed consultations with e-commerce entities, digital platforms, industry associations, consumer organisations, legal experts and technology companies to ensure transparency, clarity and industry-wide awareness regarding prohibited manipulative interface practices.

33. CCPA conducted stakeholder consultations on the issue of dark patterns and manipulative online interfaces with participation from industry stakeholders, consumer organisations, technology platforms and legal experts. Thereafter, a dedicated Task Force comprising representatives from prominent companies across multiple sectors, industry associations, consumer organisations, legal experts and technology platforms was constituted for preparation of the Guidelines. The Guidelines were thereafter finalized after extensive deliberations, consideration of stakeholder suggestions and detailed discussions.

34. Issue of dark patterns has continuously remained under active consideration of the CCPA through sustained stakeholder engagement and industry consultations. On 28.05.2025, in a high-level stakeholder meeting convened by the Department of Consumer Affairs, concerns relating to deceptive online practices and manipulative digital interfaces were deliberated with representatives from major e-commerce entities, industry associations, consumer organisations and legal institutions. During the said meeting, all e-commerce entities were specifically directed to undertake self-audits for identification and removal of dark patterns from their platforms and to proactively ensure compliance with the Guidelines for Prevention and Regulation of Dark Patterns, 2023. In pursuance thereof, several major entities submitted compliance reports/self-declarations affirming that self-audits had been conducted and that necessary measures were being undertaken to keep their platforms free from dark patterns.

35. Subsequent to issuance of the Guidelines, continued stakeholder engagement and compliance initiatives were undertaken by CCPA. An advisory dated 05.06.2025 was issued which was widely covered by print & visual media, including social media requiring e-commerce platforms to conduct self-audits for identification of dark patterns on their platforms and to ensure compliance with consumer protection obligations.

36. Annexure 1 to the Guidelines for Prevention and Regulation of Dark Patterns, 2023 lists the specified dark patterns prohibited under the said Guidelines, one of which is "Confirm Shaming". The definition of "Confirm Shaming" is reproduced below for ready reference:-

> *(3) "Confirm shaming" means using a phrase, video, audio or any other means to create a sense of fear or shame or ridicule or guilt in the mind of the user so as to nudge the user to act in a certain way that results in the user purchasing a product or service from the platform or continuing a subscription of a service, primarily for the purpose of making commercial gains by subverting consumer choice.*

The impugned interface employed the expression "Accept Risk" as the only visible alternative to "Renew Now", thereby framing the consumer's decision not to renew the subscription as acceptance of danger, insecurity or irresponsible conduct. Such fear-based wording was specifically designed to psychologically pressure consumers into continuing the subscription and therefore squarely falls within the category of "Confirm Shaming" under the Guidelines.

37. Annexure 1 to the Guidelines for Prevention and Regulation of Dark Patterns, 2023 lists the specified dark patterns prohibited under the said Guidelines, one of which is "Interface Interference". The definition of "Interface Interference" is reproduced below for ready reference:-

> *"Interface interference" means a design element that manipulates the user interface in ways that (a) highlights certain specific information; and (b) obscures other relevant information relative to the other information; to misdirect a user from taking an action as desired.*

In the present case, the renewal-related option was displayed with significantly greater visual prominence, including coloured highlighting and prominent placement, whereas the alleged close or opt-out mechanism was either absent from the screenshot placed on record or displayed in a subdued and less visible manner. Such presentation of options had the effect of steering consumers towards renewal instead of facilitating a neutral and informed choice.

38. Annexure 1 to the Guidelines for Prevention and Regulation of Dark Patterns, 2023 lists the specified dark patterns prohibited under the said Guidelines, one of which is "Trick Question". The definition of "Trick Question" is reproduced below for ready reference:-

(11) "Trick Question" means the deliberate use of confusing or vague language like confusing wording, double negatives, or other similar tricks, in order to misguide or misdirect a user from taking desired action or leading consumer to take a specific response or action

In the present case, use of the expression "Accept Risk" in the context of declining subscription renewal amounts to a "Trick Question" within the meaning of Clause 11 of the Guidelines. Instead of presenting consumers with clear and neutral choices such as "Yes" or "No", the interface employed psychologically loaded and misleading terminology capable of confusing or misdirecting consumers regarding the actual consequence of their selection. The wording used by the opposite party distorted the consumer's understanding of the available choices and nudged consumers towards a commercially favourable outcome.

39. Annexure 1 to the Guidelines for Prevention and Regulation of Dark Patterns, 2023 lists the specified dark patterns prohibited under the said Guidelines, one of which is "Forced Action". The definition of "Forced Action" is reproduced below for ready reference:-

(4) "Forced action" mean forcing a user into taking an action that would require the user to buy any additional goods or subscribe or sign up for an unrelated service or share personal information in order to buy or subscribe to the product or service originally intended by the user.

Opposite party's interface design failed to provide consumers with a fair, neutral and equally accessible opt-out mechanism during the relevant period. Although the opposite party contended that consumers could dismiss the prompt through an "X" icon, the same was either not visible in the impugned screenshot or was displayed in a substantially less prominent manner compared to the renewal option. The interface thereby created pressure upon consumers to proceed towards subscription renewal through manipulative choice design and unequal presentation of options.

40. Accordingly, CCPA found that the impugned renewal interface deployed by the opposite party constituted multiple dark patterns prohibited under the Guidelines for Prevention and Regulation of Dark Patterns, 2023, including "Confirm Shaming", "Interface Interference", "Trick Question" and "Forced Action", resulting in unfair trade practices, misleading representations and impairment of consumer choice and informed decision-making.

41. The CCPA after carefully considering the written submissions, the submissions made by the opposite party during the hearings and the investigation report submitted by Director General (Investigation) finds that the opposite party has violated the following provisions of the Consumer Protection Act 2019:-

a. Section 2(28)- Misleading advertisement
b. Section 2(47)- Unfair Trade Practice
c. The Consumer Protection (E-Commerce) Rules, 2020
d. Guidelines for Prevention and Regulation of Dark Patterns, 2023

42. The CCPA is empowered under Section- 21 of the Consumer Protection Act, 2019 to issue directions to the advertiser of false or misleading advertisement to discontinue or modify the advertisement and if necessary, it may, by order, impose a penalty which may extend to ten lakh rupees and for every subsequent contravention may extend to fifty lakh rupees. Further, Section 21 (7) of the above Act prescribes that following may be regarded while determining the penalty against false or misleading advertisement:-

a) the population and the area impacted or affected by such offence;
b) the frequency and duration of such offence;
c) the vulnerability of the class of persons likely to be adversely affected by such offence.

43. It is important to note that CCPA has taken note of the fact that the opposite party subsequently modified the impugned interface during the pendency of the proceedings. However, such corrective action was undertaken only after issuance of notice and commencement of regulatory action and therefore cannot absolve the opposite party from liability for the violations already committed. The material available on record establishes that the impugned interface formed part of a systemic renewal design deployed across the platform and was capable of affecting a large number of consumers. The opposite party itself has admitted that more than 3,55,133 subscription renewals were recorded during the relevant period prior to modification of the interface. In such circumstances, mere post-facto modification of the interface cannot dilute the gravity of the violations established under the Consumer Protection Act, 2019 read with Consumer Protection (E-Commerce) Rules, 2020 and Guidelines for Prevention and Regulation of Dark Patterns, 2023.

44. Having regard to the scale of deployment of the impugned interface, the number of consumers potentially affected, the duration for which the practice remained operational and the nature of the interface design employed, CCPA is of the considered opinion that imposition of penalty is necessary in the interest of consumers and for securing compliance with the consumer protection framework governing digital platforms. Therefore, this is a fit case for imposition of penalty and issuance of necessary directions to prevent recurrence of such practices in future.

45. In view of the above, under Section- 20, 21 read with Section 10 of the Consumer Protection Act 2019, CCPA hereby issues the following directions:-

a) The opposite party shall ensure that no dark patterns are employed on its platform, website, application or any other digital interface.

b) The opposite party shall ensure strict compliance with the provisions of the Consumer Protection Act, 2019, the Rules and Regulations framed thereunder, and the Guidelines for Prevention and Regulation of Dark Patterns, 2023.
The opposite party shall ensure that no dark patterns are employed on its platform, application.

c) In light of the nature of the violations detailed in the foregoing paragraphs, it is necessary (as discussed in above paras) that the opposite party is directed to pay a penalty of ₹1,00,000.

d) Submit a compliance report of the directions (a) to (c) above within 15 days of receipt of the Order.

.....
(Nidhi Khare)
Chief Commissioner

.....
(Anupam Mishra)
Commissioner