KPMG

Dark patterns under scrutiny

A board imperative for digital conduct, customer trust and regulatory compliance

Board Leadership Center (India)

KPMG. Make the Difference.

A. Regulatory developments in India

With increasing regulatory and consumer focus on fair digital practices, financial institutions and consumer markets are expected to ensure that customer-facing digital journeys are free from deceptive design practices commonly referred to as ‘dark patterns’.

1. **Central Consumer Protection Authority (CCPA) -** CCPA Guidelines for prevention and regulation of dark patterns, 2023 prohibit the use of deceptive digital design practices across platforms, advertisers, and sellers[1]
2. **IRDAI -** IRDAI has directed insurers operating digital platforms to comply with the CCPA dark pattern guidelines and conduct self-assessments, with remediation plans required for any identified non-compliance[2]
3. **RBI -** The Reserve Bank of India (RBI), through the responsible business conduct (second amendment) directions, 2026, has directed banks and their sales partners to ensure that user interfaces do not deploy dark patterns, effective 1 January 2027[3].

This development reflects a broader regulatory trend towards strengthening consumer protection and addressing digital conduct risks across banking, lending, insurance and payment ecosystems. Rising media attention, growing consumer complaints and regulatory interventions indicate that dark patterns are becoming a key area of supervisory focus, with implications extending beyond compliance to customer trust, reputation, and franchise value.

B. Dark patterns under global regulatory scrutiny

Globally, regulators are increasingly treating dark patterns as a consumer protection, competition, and digital conduct concern. Authorities across the US, EU, UK and Australia are actively investigating and penalising practices such as misleading consent mechanisms, hidden charges, difficult cancellation journeys, false urgency messaging and manipulative nudges. Few notable enforcement actions include:

1. **Large digital gaming platform (US):** The US Federal Trade Commission (FTC) secured a USD 520 million settlement, including USD 245 million in consumer refunds, alleging the use of dark patterns that led consumers into unintended purchases and made cancellation processes difficult[4]
2. **Major e-commerce platform (EU):** European regulators have scrutinised complex subscription and cancellation journeys resulting in regulatory action and changes to customer journeys across Europe[5]
3. **Large technology[6] and digital platforms[7]:** Regulators in the EU and UK have increasingly examined consent flows, privacy choices, cookie banners, and interface design that may steer users towards preferred outcomes, reflecting a broader move towards regulating manipulative digital design practices.

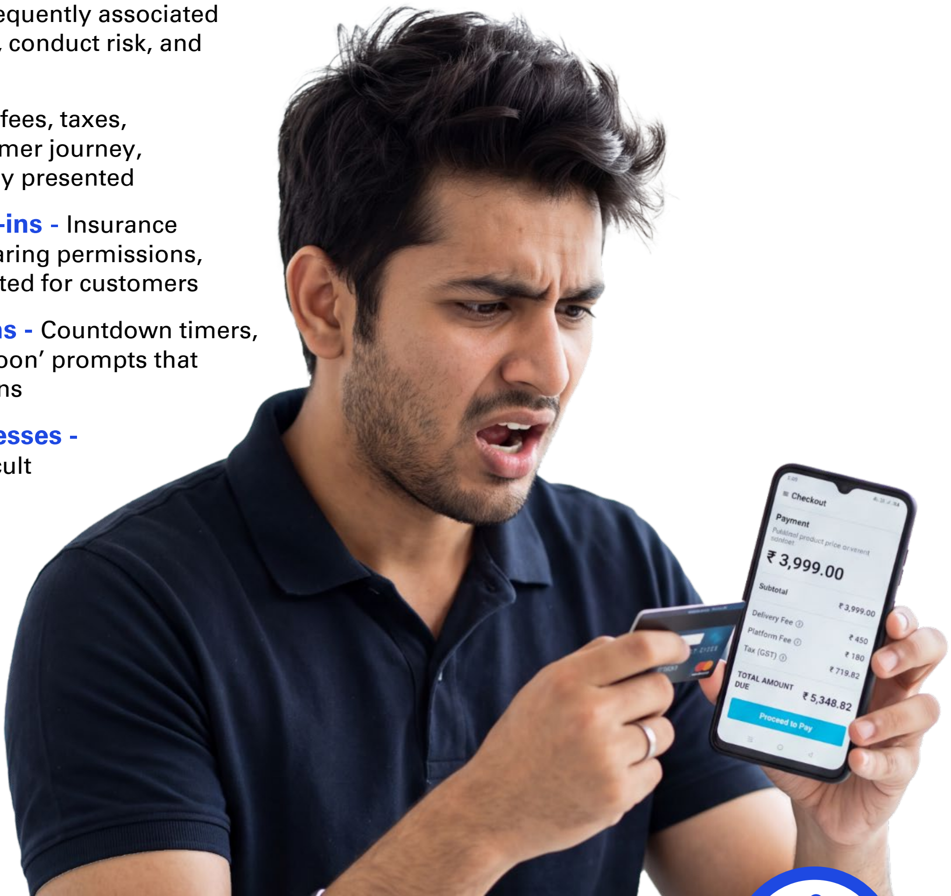
Collectively, these actions signal a broader regulatory expectation that digital experiences should be transparent, fair, and designed in the best interests of consumers rather than optimised solely for commercial outcomes.

1. The Guidelines for Prevention and Regulation of Dark Patterns, 2023, Central Consumer Protection Authority (CCPA), November 2023
2. IRDAI asks insurers to curb ‘dark patterns’, seeks compliance report in 15 days, Economic Times, April 2026
3. Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Second Amendment Directions, 2026, RBI, May 2025
4. Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges, FTC, December 2022
5. Amazon Agrees to Drop Prime Cancellation ‘Dark Patterns’ in Europe, TechCrunch, July 2022
6. EDPB adopts Art. 65 dispute resolution binding decisions regarding Facebook, Instagram and WhatsApp”, CNIL, January 2023
7. French SA: Cookies and advertisements inserted between emails: GOOGLE fined 325 000 000 EUR by the CNIL”, EDPB, September 2025

C. Typical pitfalls across financial institutions and consumer markets

The following practices are among the most commonly observed across banking, insurance, payments, e-commerce, telecom, travel, and subscription-based businesses, and are frequently associated with regulatory scrutiny, customer complaints, conduct risk, and reputational damage:

1. **Hidden fees and drip pricing-** Charges, fees, taxes, or add-on costs disclosed late in the customer journey, resulting in a higher final price than initially presented
2. **Pre-selected products and default opt-ins -** Insurance covers, warranties, subscriptions, data-sharing permissions, or marketing consents automatically selected for customers
3. **Misleading urgency and scarcity claims -** Countdown timers, limited-stock messages, or 'offer ending soon' prompts that pressure customers to make quick decisions
4. **Complex opt-out or cancellation processes -** Easy sign-up processes coupled with difficult cancellation, account closure, subscription termination, or consent withdrawal mechanisms
5. **Biased interface design and consent mechanisms -** Visual emphasis on preferred options, hidden alternatives, confusing wording, or consent flows that influence customer decisions without clear transparency.



D. Leveraging AI and technology for dark pattern detection and monitoring

As organisations prepare for heightened regulatory scrutiny, AI and technology-enabled tools are increasingly being used to help identify and monitor potential dark patterns across websites, mobile applications, and digital customer journeys. Potential dark patterns can be identified through multiple technology-enabled techniques:

1. **Website crawling and screenshot analysis -** Reviews digital journeys and user interfaces to detect potential dark patterns such as false urgency, confirm shaming, interface interference, drip pricing, and disguised advertising
2. **Repository scanning -** Analyses source code to identify embedded dark patterns, including pre-selected options, hidden consent mechanisms, subscription traps, and interface biases
3. **API and payload analysis -** Examines backend flows to identify hidden charges, pricing changes, auto-renewals, recurring billing arrangements, and biased recommendation logic
4. **Customer journey analytics -** Uses behavioural data to identify friction points, unusual customer drop-offs, abandoned cancellation attempts, and other indicators that may signal potentially manipulative design practices
5. **Complaint and feedback monitoring -** Leverages AI to analyse customer complaints, grievance data, call centre interactions, app reviews, and social media feedback to identify recurring themes associated with dark-pattern risks
6. **Continuous monitoring and change detection -** Tracks changes to digital journeys, user interfaces, and customer-facing processes to identify newly introduced risks and support ongoing compliance monitoring
7. **Risk dashboards and governance reporting -** Aggregates findings across channels and platforms to provide management and boards with visibility into emerging digital conduct risks, remediation efforts, and risk trends.

As regulatory expectations continue to evolve, organisations may increasingly need to demonstrate not only compliance with applicable requirements but also the existence of effective monitoring mechanisms capable of identifying, assessing, and remediating potential dark-pattern risks on an ongoing basis.

E. Growing concern for Institutions on dark patterns

Dark patterns should not be viewed solely as a design, marketing, or compliance issue. At their core, they raise questions about institutional culture, customer fairness, conduct risk, and the alignment between commercial objectives and long-term stakeholder trust. For boards, dark patterns present risks across multiple dimensions:

- **Regulatory risk:** Increased likelihood of regulatory investigations, enforcement actions, penalties, and remediation requirements
- **Conduct and consumer protection risk:** Potential harm to customers arising from decisions that are not fully informed or freely made
- **Reputational risk:** Negative media coverage and public scrutiny can erode trust and damage brand equity
- **Strategic risk:** Short-term commercial gains achieved through aggressive digital practices may undermine long-term customer relationships and franchise value
- **Third-party risk:** Organisations may be held accountable for customer experiences delivered through intermediaries, partners, distributors, aggregators, and digital platforms.

As regulators increasingly focus on outcomes rather than intent, Boards may need greater visibility into how digital journeys are designed, governed, monitored, and challenged across the enterprise.

F. Questions the board should ask

1. Does the organisation have a clear framework for digital conduct and customer fairness, and how does management assess compliance with it?
2. How does management obtain assurance that digital journeys, sales practices, and customer interfaces do not create unintended consumer harm or regulatory exposure?
3. What governance mechanisms exist to challenge digital design decisions where commercial objectives may conflict with customer interests?
4. How are customer complaints, behavioral insights, and customer feedback used to identify potential dark-pattern risks?
5. What management information is reported to the board on digital conduct risks, including complaints, consent practices, cancellation journeys, and customer outcomes?
6. How are emerging regulatory expectations on dark patterns incorporated into product approvals, digital transformation initiatives, and change programs?
7. To what extent are third-party distributors, sales partners, aggregators, and digital platforms subject to equivalent standards, oversight, and accountability?
8. What independent reviews or assurance activities have been conducted over digital customer journeys, and what were the key findings and remediation actions?
9. How is management leveraging technology, AI, and ongoing monitoring to identify, assess, and remediate digital conduct risks?
10. Could any of our customer journeys, while technically compliant, be perceived by regulators, customers, or the media as unfair, misleading, or inconsistent with our customer-centric values?

KPMG in India contacts:

Ritesh Tiwari
Partner
Board Leadership Center
E: riteshtiwari@Kpmg.com

Suveer Khanna
Partner
Risk and Integrity Advisory
E: skhanna@kpmg.com

Mustafa Surka
Partner
Risk and Integrity Advisory
E: mustafasurka@Kpmg.com

Abhishek Jhunjhunwala
Associate Partner
Risk & Integrity Advisory
E: abhishekjhunjhunwala@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai-400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.