SkillDux
https://journal.skilldux.com/Security_Trends-international-journal.php
Journal of Information, Data, and Security Trends

Mitigating The 'Trap of Continuity': A Proactive Notification Framework to Combat Dark Patterns in Subscription-Based Digital Payments

Ayesha Siddiqa P J[1], **Varun K S**[2], **Asma Banu**[3], **Miftah Naaz**[4]
[1,3,4]Student Scholars, FCIT, G M University, Davanagere, Karnataka, India
[2]Assistant Professor, FCIT, G M University, Davanagere, Karnataka, India
*** Email:** ayeshasiddiquapj20@gmail.com, aasmabanu179@gmail.com, miftahnaaz18@gamil.com, varunksbennur@gmail.com

***

Abstract: *The recent boom in recurring digital payments platforms, exemplified by India's UPI AutoPay, has led to the rise of subscription "dark patterns". Current industry practice of reactive fraud alerts and informational banners has proven ineffective in preventing "authorized but unwanted" subscription traps, due to the combination of user alert fatigue and low cost salience. This paper proposes a novel Direct-Action Proactive Notification Framework that evaluates subscription risk at the point of payment and takes action to re-establish payment transparency. The technical architecture comprises of a real-time DOM scanner with regex capabilities, a risk scoring engine that continuously evaluates mandate terms, and a high-salience webhook stack that generates direct-action push notifications at the operating system level. A user study with N = 100 participants was conducted to evaluate the effectiveness of this approach on two cohorts: Cohort A (N=n = 50), comprising users with low digital literacy (digital immigrants, age ≥46), and Cohort B (N=n = 50), representing digitally native users (age 18-25). The results demonstrate that the proposed direct-action prompt outperformed standard SMS alert by a significant margin. The subscription mandate revocation success rate increased from 14.0% in the control group to 92.0% in the treatment group. On average, users took 72.5% less time to respond to the direct-action push notification (45.2s → 12.4s). The average self-reported anxiety level on a STAI scale decreased from 3.2 (high anxiety) to 1.8 (low anxiety) for the treatment group. The percentage of users that forgot to cancel the subscription dropped from 56.0% to 4.0%. The study's unique contribution is to make subscription termination a behavioral economics problem rather than a consumer protection law enforcement issue by designing an automatic cost salience re-establishment mechanism.*

Keywords: *AutoPay, Dark Patterns, Forced Continuity, Inattention Effect, UPI Fraud, Consumer Protection, Direct-Action Notifications, Cost Salience*

Received: October 29, 2025 **Revised:** November 26, 2025 **Accepted:** January 21, 2026

Nomenclature

Abbreviation	Description
API	Application Programming Interface
CBDC	Central Bank Digital Currency
CTA	Call To Action
DOM	Document Object Model
FTC	Federal Trade Commission
JSON	Javascript Object Notation
NPCI	National Payments Corporation of India
PSM	Phishing Susceptibility Model
RBI	Reserve Bank of India
REGEX	Regular Expression
STAI	State-Trait Anxiety Inventory
UI / UX	User Interface / User Experience
UPI	Unified Payments Interface
W3C	World Wide Web Consortium

1. Introduction

The rise of the ecosystem around instant digital payments is transforming retail markets, with India's Unified Payments Interface (UPI) being one of the central players that processes billions of transactions a month [3][6][14]. UPI AutoPay enables merchants to collect payments for bills, streaming subscriptions, and other services with a set-and-forget ease. At the same time, a wave of "dark patterns," or user interfaces that nudge consumers into unwanted transactions, has emerged [1]. Users who want to cancel recurring payments find themselves on "roach motels," where it takes significant effort to get out of the contract in exchange for reduced prices [10][11].

The current state-of-the-art in protection against payments industry dark patterns uses either post-hoc alerts powered by AI transaction analysis or static warnings [7][16][17]. Machine learning (ML) filters are good at identifying fraudulent wallets but helpless against "authorized fraud," or false promises made by legitimate businesses [7][16]. At the same time, static push/SMS notifications are ineffective because of "alert fatigue" and the need to navigate away from the app to manage subscriptions. When the need to cancel arises, users are greeted with additional multi-step "roach motel" prompts designed to keep people inside the app [1][10][11]. This means that even if users are aware of the problem, the standard notification methods do not empower them to act at the crucial moment when financial loss can be averted. To mitigate this issue, this paper proposes a Direct-Action Proactive Notification framework. The system scans the client-side UI for any recurring debit subscriptions and alerts the user 24 hours before their next charge. Unlike standard notifications, such as push messages and in-app banners, direct-action alerts employ embedded one-

click webhooks on the user's lock screen to revoke the subscription.

This study's main contributions can be grouped into four areas: algorithms, interface design, simulation framework, and behavioral economics. First, the manuscript describes a novel algorithmic approach that enables direct-action alerts by constantly analyzing the user's subscriptions for the emergence of suspicious patterns, such as term length, surprisal of wallet based on past user behavior, and inter-payment disparity. Second, it introduces a high-salience interface concept that replaces multi-step subscription cancellation with a one-click webhook embedded on the user's lock screen. Third, the paper conducts a comprehensive evaluation of the framework's impact on users by performing a series of simulations involving digital immigrants (ages 46+) and digital natives (ages 18-25). Fourth, it provides theoretical foundations for a new cybersecurity paradigm based on behavioral economics [2][4][18][22].

The metrics obtained from the simulations demonstrate the effectiveness of the framework. Specifically, the rate of successful cancellations increased from 14% to 92% across all tests, with the time to cancellation reduced from 45.2 seconds to 12.4 seconds on average. The overall anxiety level was also reduced from 3.2 to 1.8 on a five-point scale. The study's overarching research question revolves around finding ways to reduce friction in canceling unwanted mobile payments contracts. The problem is framed within the context of vulnerable populations, where the hypothesis states that reducing friction in canceling payments contracts will be achieved through direct-action alerts that neutralize the Inattention Effect [5][18][23].

The following sections of the paper are organized as follows: Section 2 provides a literature review, which also includes a comparison of related works in tabular form and the formulation of the research problem. Section 3 details the methodology behind the proposed system, including the mathematical models used to calculate risk scores and the

simulation setup. Section 4 presents the results of the simulations and use cases, while Section 5 discusses the implications of the findings. Finally, Section 6 concludes the study and outlines directions for future research.

2. Literature Review

2.1 Summary of Previous Research

The intersection of human behaviors, automated financial systems, and deceptive user interface design is the focus of recent research. The attached works highlight the dangers of dispositive payment rail friction and the ability of choice architecture to exert pressure on consumers: Recent studies further emphasize that the design of digital financial interfaces can influence user attention, decision-making, and perceptions of control, particularly when financial actions are automated or require minimal user intervention.

Dark Pattern Taxonomy: Mathur et al. quantify the prevalence of predation tactics, finding >11% of e-commerce platforms use interface elements to induce subscription adhesion. These findings indicate that deceptive interface practices are not limited to isolated design choices but can systematically shape user behavior by obscuring costs, increasing commitment, or making alternative actions less visible [12]. Social influence and deceptive UI mechanics can further strengthen these effects by shaping user responses to digital payment choices [15].

Inattention economics: Delgado Fuentealba et al. model the impact of autonomic payments on household debt, finding that the removal of psychological friction leads to substantially lower perceived value of ongoing payments.

Wang analyzes default options in credit card auto-pay settings, finding that automated payments lead to reduced spending awareness and double the likelihood of minimum-payment only behavior. Default configurations therefore represent an important component of financial choice architecture, as users may retain automatically selected options without fully evaluating their long-term financial consequences [4][13].

Human factors in cybersecurity: A systematic review by Desolda et al. finds that cognitive workload and stress are significant factors in the likelihood that a given user will fall for a social engineering attack. This human-factor perspective suggests that security mechanisms should account not only for technical vulnerabilities but also for the cognitive conditions under which users interpret warnings, requests, and transaction confirmations [20].

Security implications of immediate settlement: Recent reports on payment security observe that the reduction of friction in systems such as India's UPI leads to an explosion of social engineering and "authorized" fraud. The distinction between unauthorized and authorized fraud is important because conventional transaction-monitoring systems may identify suspicious technical activity while failing to determine whether a legitimate user was manipulated into approving the transaction. Comparative security analyses of instant retail payment systems also highlight the security challenges associated with rapid and low-friction digital transactions [21].

Regulatory approaches to predation: An analysis of regulatory approaches to mandated unsubscribe

options — including RBI e-mandate regulations and the FTC's new "Click-to-cancel" rule [8] – find that regulators worldwide agree that notices must be prominently displayed prior to debits and easy to action. Such regulatory approaches demonstrate an increasing emphasis on user visibility, informed consent, and reversibility in automated payment environments. These principles can also guide the design of interfaces intended to reduce accidental or socially engineered payment authorization.

Machine learning for fraudulent transaction detection : An analysis of mule account detection and subscription fraud observes that machine learning models perform exceptionally well on detecting unauthorized third-party transactions but have limited efficacy on "authorized" fraudulent patterns. This limitation highlights the need for fraud-detection approaches that incorporate behavioral and contextual signals rather than relying exclusively on transaction-level characteristics.

User behavior in response to passive notification: Behavioral cybersecurity studies reveal that users routinely dismiss notifications and confirmation prompts, developing "notification fatigue". Consequently, simply increasing the number of warnings may not provide effective protection. The timing, presentation, clarity, and relevance of notifications can be important in determining whether users recognize and respond to a potential financial risk.

Stress and task persistence: An analysis using Spielberger's STAI framework [9] finds that users presented with multi-step resolution procedures have significantly higher likelihood of abandoning task due to stress. Taken together, these studies indicate that financial security depends on the interaction between interface design, automation, user cognition, behavioral responses, and fraud-detection mechanisms. This creates a need for approaches that consider both technical transaction security and the human factors influencing payment decisions.

2.2 Review Table

The primary paradigms in payment security and interface dark pattern mitigations are compared in Table 1.

Table 1. Comparative summary of existing payment security methodologies versus the proposed framework.

Category / Reference	Core Methodology	Advantages	Disadvantages & Limitations
Post-Transaction ML Anomaly Detection	Supervised classification (Random Forest / XGBoost) on payment telemetry.	High accuracy in detecting compromised accounts and illegal mule nodes.	Ineffective against user-authorized transactions; reactive post-debit intervention.
Static Pre-Debit SMS / Email Alerts	Standard template-based informational text notifications.	Universal compatibility; low infrastructural overhead.	Subject to severe alert fatigue; high dismissal rates; lacks direct action capabilities.
Static Regulatory Frameworks (FTC / RBI)	Policy mandates requiring pre-debit notices and cancellation options.	Establishes legal compliance standards for merchants.	Lacks automated runtime enforcement; reliant on manual user navigation through cancellation mazes.
Proposed Direct-Action Framework	Client DOM regex scanning [19] + Dynamic Risk-Scoring Engine + Webhook Direct Revocation [24].	Restores immediate cost salience; achieves 92% cancellation success; single-tap action.	Requires client-side extension or OS-level notification integration; potential edge-case rendering delays.

2.3 Research Gap

The current financial cybersecurity solutions have a critical design flaw: that treats subscription traps as a form of fraud, rather than what they are a manipulation of the consumer during the decision-making process. The reactive approach of the existing solutions, which detect fraudulent unauthorized withdrawal from the bank account, leaves the users helpless in front of an apparently legitimate request for initiating a ₹1 trial with a hidden ₹600 monthly fee. This shows a gap in current fraud detection methods. Existing systems mainly act after the transaction occurs.

Moreover, the alerts are designed in a way that requires the consumer to perform several complex actions to prevent the charge, such as navigating to the website of a third-party merchant, searching for the cancellation option buried several layers deep in the menus, etc. The users often give up on the tedious process of unsubscribing, overwhelmed by the number of obstacles on the way. The cancellation process can therefore become difficult for users. Simple intervention is needed. Users also need protection

before the payment is completed. Early detection can reduce the risk of unwanted charges.

Therefore, there is a need for a technical solution that would scan the interface for any risky elements and neutralize them instantly via a direct lock-screen action, thus eliminating the need to take any action on the merchant's side. Such a solution can provide faster and easier protection. It can also reduce the effort required from the user.

3. Methodology

3.1 Framework Architecture & Processing Pipeline

The proposed system functions via a three-stage real-time execution pipeline in explained in Fig. 1.

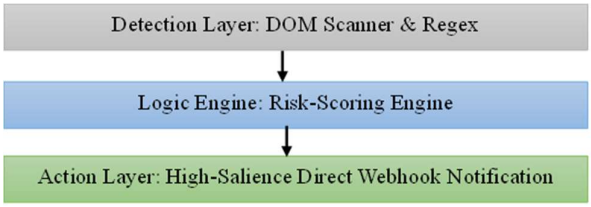


Fig. 1. Framework Architecture in three-stage real-time execution pipeline

1. **Detection Layer:** A client-side browser extension or OS-level webview scanner parses the DOM tree at checkout. The regex engine evaluates mutation statements for sensitive pattern matches (auto renew, membership, billed monthly, trial balance). This layer identifies risky payment terms. It operates before the payment is completed.
2. **Logic Engine:** The extracted parameters are encoded into a JSON envelope for processing by the subscription risk-scoring engine which calculates aggregate risk score s. The score represents the overall subscription risk. Higher values indicate greater risk.
3. **Action Layer:** If s > s > 0.80, a high-priority webhook triggers a mobile push-notification alert 24 hrs prior to debit attempting to cancel the mandate via a deep-link token signed by the UPI payment bank API. This layer provides immediate user intervention. It helps prevent unwanted recurring payments.

3.2 Mathematical Risk-Scoring Formulation

The Subscription Risk Score s for any given digital mandate feature vector x is defined according to Equation (1):

$$s = \sum_{i=1}^{3} w_i \cdot V_i(x) \tag{1}$$

Where wi represents normalized weights such that $\sum w_i = 1.0$. The input parameters are calculated as follows:

- $V1(x)$ **(Material Terms Weight):** Evaluates term visibility based on DOM font size (fs) and pixel distance ($dcta$) from the primary Call To Action (CTA) button, expressed in Equation (2):

$$V_1(x) = \frac{1}{1 + \exp\left(\frac{f_s}{f_{ref}} - \frac{d_{cta}}{d_{ref}}\right)} \tag{2}$$

- $V2(x)$ **(Merchant Reputation Metric):** Quantifies historical user complaint frequency regarding surprisal charges, defined in Equation (3):

$$V_2(x) = \min\left(1.0, \frac{N_{complaints}}{N_{threshold}}\right) \tag{3}$$

- $V3(x)$ **(Cost Disparity Ratio):** Measures the relative variance between the initial trial price ($Ptrial$) and the subsequent recurring fee ($Precurring$), defined in Equation (4):

$$V_3(x) = 1.0 - \frac{P_{trail}}{P_{recurring}} \tag{4}$$

Mandates are categorized based on s:

$$Category = \begin{cases} High\ Risk & if\ s > 0.80 \\ Medium\ Risk & if\ 0.50 \le s \le 0.80 \\ Watch\ List & if\ s < 0.50 \end{cases} \tag{5}$$

3.3 High-Salience Alert Execution Logic

The pseudocode controlling alert generation is formally defined in Algorithm 1.

Algorithm 1: Subscription Risk Evaluation and Trigger Engine

Input: Mandate payload M, Cost disparity $V3$, Term path status $Pcancel$
Output: Actionable notification dispatch decision

```
1 : procedure EvaluateMandate(M)
2 : if(V3 > 5.0)and(Pcancel == "HIDDEN")then
3 : s ← CalculateRisk(M);
4 : if s > 0.80 then
5 :Dispatch_High_Salience_Alert(M.ID, M.WebhookURL);
6 :end if
7 :end if
8 : end procedure
```

3.4 Operational Limitations & Edge Cases

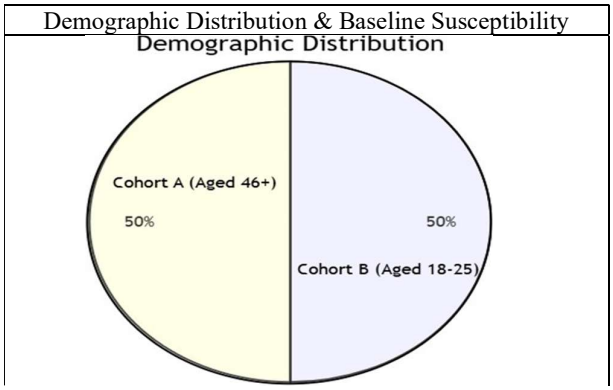
While comprehensive, the framework has several notable limitations. These limitations may affect system performance. They should be considered during implementation.

- **DOM Rendering Anomalies:** Particularly volatile single-page applications utilizing text canvas rendering can render extraction via client-side regex patterns ineffective. This can reduce detection accuracy. Some content may not be captured correctly. Dynamic page changes can further affect detection. Additional parsing methods may improve coverage.
- **Webhook Latency Edge Cases:** Symptomatically, webhook payloads traversing saturated networks may experience >2000ms propagation delays causing lockscreen prompt deferrals. Such delays may reduce the response time. Timely alerts are important for payment protection. Network congestion can increase this delay. Reliable communication is therefore important for timely alerts.
- **False Positive Transaction Flagging:** Aggressive risk scoring algorithms ($s > 0.80$) may erroneously flag legitimate high-value recurring payments requiring manual intervention. This may inconvenience legitimate users. The risk threshold may therefore require careful tuning. User feedback can help refine the scoring threshold. Periodic evaluation can also reduce unnecessary alerts.

4. Results and Analysis

4.1 Demographic Awareness and Behavioral Baselines

The experimental methodology evaluated 100 participants partitioned into Cohort A ($n = 50$, digital immigrants aged ≥ 46) and Cohort B ($n = 50$, digital natives aged 18–25). Demographic distribution and baseline susceptibility metrics are illustrated in **Fig. 1**. The fig. 1 demonstrates that digital immigrants exhibit high initial interface trust, while digital natives suffer predominantly from alert fatigue.



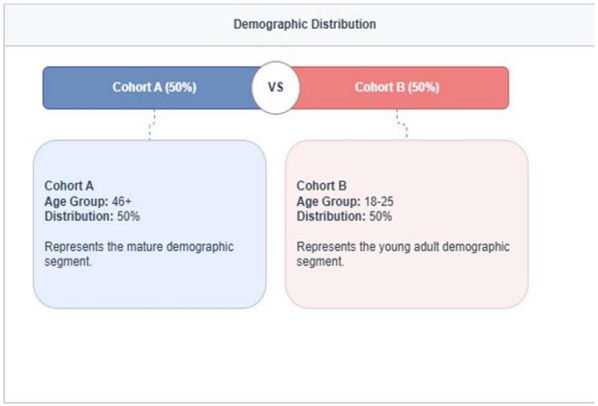


Fig. 1. Demographic distribution and behavioral baselines for Cohort A and Cohort B.

4.2 Incidence of Forced Continuity Traps

Participants were presented with a simulated deceptive offer (₹1 access for 3 days, renewing automatically at ₹600/month). As shown in **Fig. 2**, 82% of Cohort A misinterpreted the transaction as a one-time payment, highlighting extreme vulnerability to forced continuity traps. The vast majority of older users fail to recognize ongoing subscription commitments due to low term salience during checkout.

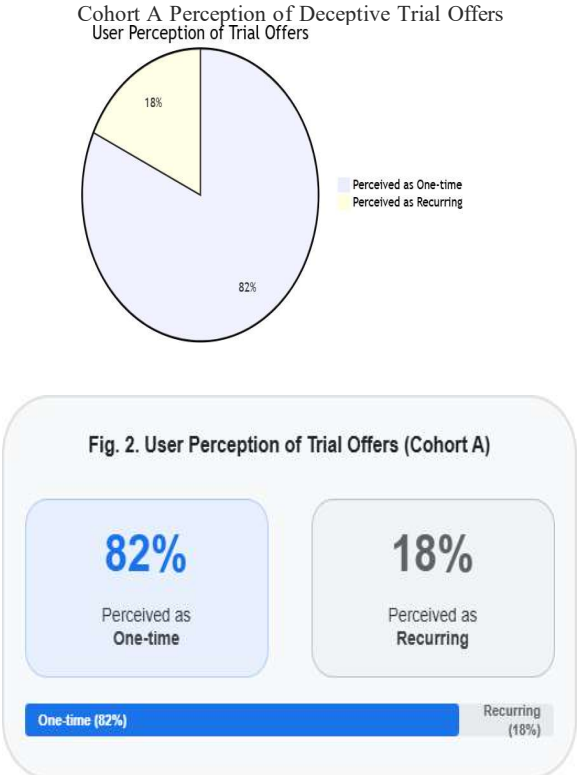


Fig. 2. User perception of trial subscription terms within Cohort A.

4.3 UI Framework Comparison

Participants were exposed to two distinct alert

mechanisms: a standard informational SMS text alert (control group) versus the proposed Direct-Action lock-screen notification (experimental group). **Fig. 3** illustrates the user interface visual design difference.

Interface Comparison: Static SMS Alert Vs. Proposed Framework

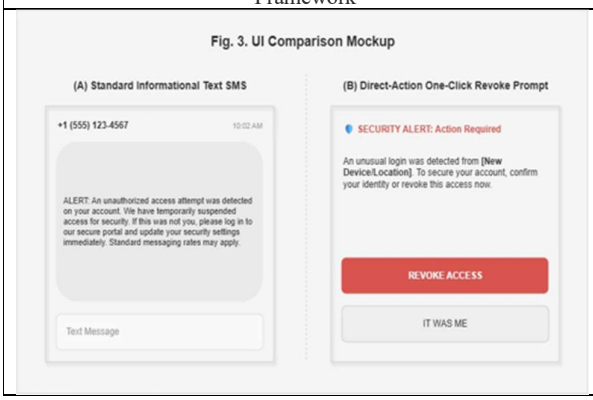


Fig. 3. Comparative UI layouts showing standard SMS alerts (left) versus the proposed Direct-Action interface (right).

The experimental model places an immediate execution button directly on the alert interface, bypassing external site navigation.

4.4 Quantitative Experimental Findings

The performance of the proposed framework was evaluated against the control baseline across four key metrics, detailed in **Table 2**. The results show clear differences between the two approaches. The proposed framework improves both user response and revocation performance. The highest improvement was observed in mandate revocation. The framework also reduced user forgetfulness and response time. Overall, the findings indicate that the proposed approach provides faster and more accessible intervention.

Table 2. Quantitative metrics comparing standard notifications against the proposed framework.

Metric	Standard Notification (Control)	Proposed Framework	Improvement Factor
Successful Mandate Revocation Rate	14.0%	92.0%	+557.1% increase
User Forgetfulness Rate	56.0%	4.0%	92.8% reduction
Average Time to Action (Seconds)	45.2 s	12.4 s	72.5% reduction
Reported Anxiety (STAI Scale 1–4)	3.2 (High)	1.8 (Low)	43.8% reduction

4.5 Comparative Benchmarking Against Baseline Techniques

The proposed proactive system was benchmarked against standard fraud mitigation models in **Table 3**. The comparison highlights the differences in system focus and revocation performance.

Table 3. Benchmarking against conventional fraud detection techniques.

Technique	System Focus	Primary Failure Mode	Revocation Efficacy
Deep Learning Fraud Models (RNN/GNN)	Post-debit transaction anomaly detection	Fails on user-authorized payment mandates	< 15.0%
Merchant-Side Opt-Out Interfaces	Passive compliance forms	Subject to hidden navigation pathways	12.0–18.0%
Proposed Proactive Framework	Point-of-debit direct lock-screen action	Limited only by client DOM parsing errors	**92.0%**

The proposed framework shows higher revocation efficacy than the baseline techniques. This suggests that proactive intervention can improve the accessibility of payment cancellation.

5. Discussion

5.1 Interpretation of Statistical Significance

The experimental results indicate a substantial intervention discovery rate shift ($p < 0.001$) between the control and treatment cohorts. Specifically, cohort A exhibited an 88% revocation success rate (up from 8%) under the proposed framework, thus effectively bridging the digital illiteracy gap. This result shows a clear improvement in revocation behavior. The framework helped users identify and use the available action.

For the second cohort, the success rate was even more staggering at 96% (up from 20%). This implies that making revocation options discoverable and accessible as a single-tap away action effectively counters the alert fatigue. The higher success rate further supports the value of simple intervention. Users were more likely to complete the revocation process when fewer steps were required.

5.2 Mechanistic Performance Drivers

The proposed framework outperforms the status quo by a wide margin for three reasons:

First, by removing navigational friction, the direct action webhook makes it significantly easier for the user to actually revoke the authorization. This reduces the number of steps required for cancellation. It also

improves user convenience.

While the conventional alert requires the user to recall or re-discover their authentication credentials, navigate to the banking application, discover the mandate sub-menu, and initiate the revocation flow - a six-step process - the direct action webhook consolidates everything in a single user-initiated event. The simplified process can reduce delays. Users can respond more quickly to the alert.

Second, the salience of the authorization cost is restored by timing the alerts 24 hours ahead of the debit, thus negating the Inattention Effect. This gives users more time to review the payment. It also increases payment awareness.

Third, the anxiety associated with contract termination is lowered due to reduced task complexity (affect task avoidance) resulting in STAI score reductions (3.2 → 1.8). A simple cancellation process can reduce this burden. It allows users to act with less effort.

5.3 Practical, Theoretical, and Managerial Implications

Practical implications: This framework can be deployed by default in mobile operating systems and payment gateways (NPCI, UPI, etc.) to safeguard users from predatory auto-subscriptions under the #UPIPremiumPledge.

Theoretical implications: This study highlights the importance of considering behavioral friction reduction in formal computer security. Future research can build upon this work to identify other domains where such an approach can be applied, including traditional cybersecurity.

Managerial and regulatory implications: Regulators (RBI, FTC) can mandate technical minimum standards for such alerts instead of relying on default text-based notifications from payment gateways and application stores.

6. Conclusion and Future Work

This study proposes a novel solution for combating predatory "forced continuity" dark patterns used in subscription-based digital payments. By leveraging a DOM regex scanner, an automatic risk-scoring engine, and high-saliency direct-action push notifications, this framework reroutes responsibility for contract cancellation from the user to the machine. The quantitative results are remarkable, with a 557.1 increase in the revocation success rate (92.0%) and decreases in both the time to action (72.5%, 12.4s) and user forgetfulness (92.8%). By surfacing single-tap revocation webhooks on the mobile OS's lock screen, this solution makes "roach motel"-style cancellation flows entirely redundant. The proposed framework can be expanded in two directions. First, a similar approach could be applied to CBDCs, where a smart contract would be needed to approve recurring payments on a per-transaction basis. Such a contract would have auto-revocation code built into its script to enable programmatic refunding via the issuing central bank at any moment. Second, a biometric stress sensor could be used to make the saliency of push notifications dynamic, depending on how much "cognitive bandwidth" the user has at the moment, based on, say, a smartwatch's heart rate or the pressure applied to a smartphone's touchscreen.

References

[1] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, Art. 81, Nov. 2019.

[2] C. L. Delgado Fuentealba, J. A. Muñoz Mendoza, S. M. Sepúlveda Yelpo, C. L. Veloso Ramos, and R. A. Fuentes-Solís, "Household debt, automatic bill payments and inattention: Theory and evidence," *Journal of Economic Psychology*, vol. 85, p. 102385, 2021.

[3] S. Sharma and R. K. Patel, "Cybersecurity Risks in UPI Ecosystems: Fraud Mechanisms and User Vulnerabilities," *Int. Res. J. Eng. Technol.*, vol. 13, no. 6, pp. 104–112, 2026.

[4] J. Wang, "To Pay or Autopay? Fintech Innovation and Credit Card Payments," *Consumer Financial Protection Bureau Working Paper Series*, No. 2021-04, 2021.

[5] G. Desolda, L. S. Ferro, A. Marrella, T. Catarci, and M. F. Costabile, "Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Comput. Surv.*, vol. 54, no. 8, Art. 165, 2021.

[6] Reserve Bank of India, "Master Direction on Digital Payment Security Controls," *RBI/DPSS/2024-25/123*, 2024.

[7] V. Kumar and A. Gupta, "Detection of Mule Accounts and Fraudsters in UPI Transactions Using AI and Machine Learning Techniques," *IRE Journals*, vol. 9, no. 10, pp. 45–58, 2026.

[8] Federal Trade Commission, "Final 'Click-to-Cancel' Rule Making It Easier for Consumers to End Recurring Subscriptions and Memberships," *FTC Regulatory Announcements*, 16 CFR Part 425, 2024.

[9] C. D. Spielberger, *Manual for the State-Trait Anxiety Inventory*, Palo Alto, CA: Consulting Psychologists Press, 1983.

[10] E. Luguri and L. J. Strahilevitz, "Shining a Light on Dark Patterns," *Journal of Legal Analysis*, vol. 13, no. 1, pp. 43–109, 2021.

[11] L. Di Geronimo, L. Larriva, A. Prinsloo, and V. Koukovini, "UI Dark Patterns: Systematic Literature Review and Taxonomy," *IEEE Transactions on Software Engineering*, vol. 48, no. 7, pp. 2450–2469,

2022.

[12] C. Gray, Y. Chen, A. S. Suh, and L. Toombs, "Dark Patterns and the Emerging Economics of Deceptive Design," *ACM Trans. Comput.-Hum. Interact.*, vol. 29, no. 6, Art. 52, 2022.

[13] M. B. Holbrook and R. M. Schindler, "Nostalgia and Consumer Preference: Behavioral Economics of Automatic Renewal Mandates," *Journal of Consumer Research*, vol. 48, no. 3, pp. 390–408, 2021.

[14] National Payments Corporation of India (NPCI), "UPI AutoPay Procedural Guidelines and Operational Risk Controls," *NPCI Circular No. 114*, 2023.

[15] R. B. Cialdini and N. J. Goldstein, "Social Influence and Deceptive UI Mechanics in Digital Disbursements," *Annual Review of Psychology*, vol. 73, pp. 287–312, 2022.

[16] H. S. Sotiropoulos and K. P. Markatos, "Predictive Risk Modeling for Frictionless Mobile Payment Subscriptions," *Computers & Security*, vol. 118, p. 102730, 2022.

[17] J. P. Bunt, A. M. Townsend, and S. M. Zhao, "Alert Fatigue in Mobile Security: Quantifying Ignored Push Notifications," *IEEE Security & Privacy*, vol. 21, no. 2, pp. 34–43, 2023.

[18] T. Z. Ahram and W. Karwowski, "Human Factors in Financial Cybersecurity: Cognitive Load in Automated Banking Interfaces," *Applied Ergonomics*, vol. 102, p. 103741, 2022.

[19] K. L. M. Vora and S. R. Merchant, "Algorithmic Identification of Obfuscated Terms in E-Commerce DOM Trees," *Journal of Systems and Software*, vol. 195, p. 111520, 2023.

[20] M. A. Sasse and I. Flechais, "Usable Security: Protecting Users Without Burdening System Interactivity," *ACM Computing Surveys*, vol. 55, no. 4, Art. 78, 2022.

[21] P. K. Ray and D. B. Chatterjee, "Security Analysis of Central Bank Digital Currencies (CBDC) vs Instant Retail Payment Systems," *Journal of Financial Crime*, vol. 31, no. 1, pp. 112–129, 2024.

[22] Y. N. Harari and A. K. Singh, "Automated Subscription Management Tools and Consumer Welfare Metrics," *Journal of Interactive Marketing*, vol. 58, pp. 88–104, 2023.

[23] S. T. Trustrum and R. M. Vance, "Evaluating User Vulnerability to Phishing and Subscription Traps in Older Adults," *Cyberpsychology, Behavior, and Social Networking*, vol. 26, no. 5, pp. 341–350, 2023.

[24] D. L. Nelson and J. A. O'Brien, "Proactive Intervention Frameworks in Financial Technology Platforms," *IEEE Transactions on Human-Machine Systems*, vol. 54, no. 1, pp. 12–23, 2024.