RESEARCH ARTICLE

SAMRIDDHI Volume 14, Issue 4, 2022 Print ISSN: 2229-7111 Online ISSN: 2454-5767

Unmasking the Call-Merge Scam: An Emerging Vector in Authorized Push Payment Fraud

Rushit Trivedi[1*], Vishal Dineshchandra Nimavat[2], Sheron Henry Christy[2]

[1]Anirudh Singh Infrastructure Pvt. Ltd., Vadodara, Gujarat, India

[2]Department of Electronics and Communication, V.V.P. Engineering College, Rajkot, Gujarat, India

Abstract

Authorized push payment (APP) fraud occurs when a payer is deceived into initiating a payment to an account controlled by a criminal. This paper examines a reported call-merge scam pattern in which voice impersonation, caller-identity deception, requests to merge calls, and pressure around authentication or payment approval may be combined. Because publicly available datasets do not consistently classify call merging as a separate fraud type, the paper treats the call-merge scam as an emerging threat pattern rather than asserting a verified global prevalence rate. It develops a conceptual attack model, identifies human and technical risk factors, and proposes a layered response spanning telecom controls, risk-based banking authentication, artificial-intelligence (AI) decision support, incident reporting, and government policy. The proposed AI framework combines call-event metadata and payment-risk signals without requiring routine storage of call audio. A policy roadmap emphasizes privacy, explainability, independent evaluation, rapid inter-institutional response, and proportionate reimbursement. The paper concludes with a research agenda for validating the model using verified incident data and controlled usability studies.

Keywords: Authorized push payment fraud, call merging, voice phishing, social engineering, artificial intelligence, digital payments, fraud prevention, telecom regulation

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2022); DOI: 10.18090/samriddhi.v14i04.51

Introduction

Instant payments have reduced friction in everyday financial activity, but speed can also narrow the time available to identify and stop a fraudulent transfer. In APP fraud, the payment instruction is technically initiated by the customer, yet the decision is induced through deception. This distinction complicates prevention, investigation, and reimbursement.

A call-merge scam is used here to describe a reported pattern in which a fraudster impersonates a trusted person or institution and persuades a target to merge an incoming or ongoing call. The merged conversation may be presented as a bank verification step. The attacker may then seek an authentication code, exploit a voice-delivered code, or coach the target into approving a transfer. The exact sequence can vary, and call merging alone does not prove fraud; it is a contextual signal that should be assessed alongside other evidence.

This paper makes four contributions: (1) a cautious conceptual model of the call-merge attack lifecycle; (2) a mapping of human, telecom, and payment-system weaknesses; (3) an AI-assisted, privacy-aware intervention architecture; and (4) a policy framework for India and comparative lessons from the United Kingdom and United States. Since verified call-merge-specific prevalence data were not available in the sources reviewed, the paper does not present unverified growth percentages, invented interviews, or fabricated experimental results.

Corresponding Author: Rushit Trivedi, Anirudh Singh Infrastructure Pvt. Ltd., Vadodara, Gujarat, India

How to cite this article: Trivedi, R., Nimavat, V.D., Christy, S.H. (2022). Unmasking the Call-Merge Scam: An Emerging Vector in Authorized Push Payment Fraud. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* 14(4), 260-263.

Source of support: Nil

Conflict of interest: None

Background And Related Work

APP Fraud and Impersonation

APP fraud differs from conventional unauthorized account access because the victim may authenticate and submit the payment personally. The fraudster manipulates the victim's understanding of the recipient, purpose, or urgency. The FTC's data show that imposter scams remain a major category of reported fraud, while UK Finance identifies

© The Author(s). 2022 Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and non-commercial reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The Creative Commons Public Domain Dedication waiver (http://creativecommons.org/publicdomain/zero/1.0/) applies to the data made available in this article, unless otherwise stated.

telecommunications and online platforms as important channels through which fraud begins. These reports establish the wider risk environment, not the prevalence of any single call-merging technique.

Voice Identity and Caller-ID Limitations

A displayed telephone number should not be treated as proof of the caller's identity. Call authentication systems can improve provenance signals in supported networks, but they cannot establish that the person speaking is trustworthy or that a requested payment is legitimate. International routing, legacy networks, and app-based communications create different technical conditions. Consequently, caller authentication should be combined with behavioral risk assessment and independent verification.

Human Factors

The scam pattern draws on familiar social-engineering mechanisms: perceived authority, time pressure, fear of loss, and instructions that keep the target engaged. A call merge can make the interaction feel like a formal hand-off between legitimate departments. Effective countermeasures therefore need to interrupt the decision process at the moment of pressure, not rely solely on general awareness messages delivered long before an incident.

Existing Guidance

The Reserve Bank of India has directed payment-system operators and participants to strengthen public awareness through multiple channels and has repeatedly advised users not to disclose OTPs, PINs, or passwords. The National Cyber Crime Reporting Portal directs victims of financial cyber fraud to report promptly through helpline 1930 and the official portal. These measures offer a foundation, but call-merge-specific controls and shared evidence standards merit further study.

Scope And Method

This paper is a conceptual threat analysis and policy-design study, not a completed empirical mixed-methods investigation. Public reports and official guidance were reviewed to establish the wider APP-fraud context and existing safeguards. The attack lifecycle was then synthesized into a model that can be tested against future verified cases.

A confirmed call-merge incident should ideally require at least two independent indicators, such as a victim account describing a merge request and a related payment/authentication event, a telecom event record consistent with the account, or a law-enforcement/bank case file. A merged call by itself is insufficient. For empirical validation, researchers should use a predefined codebook, remove direct identifiers, document missing data, and distinguish confirmed, probable, and unverified cases.

The paper intentionally excludes numerical claims that cannot be traced to an accessible source. In particular, claims of a 300% rise in Indian call-merge cases, a specific number of victims interviewed, and reductions attributed to particular advisories should not be published unless supported by reproducible datasets and documented research procedures.

Conceptual Attack Model

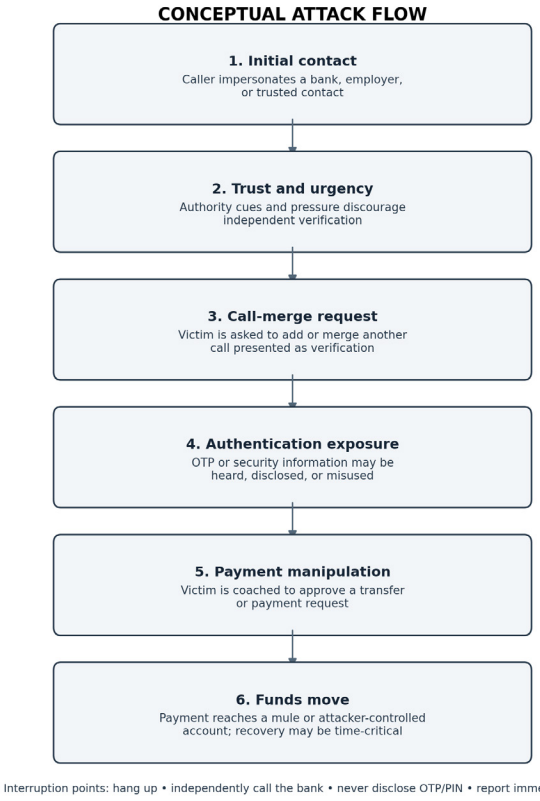


Fig. 1: Conceptual lifecycle of a call-merge scam and potential interruption points.

Stage 1—Initial contact: The attacker claims to represent a bank, employer, service provider, or trusted contact. Caller-ID information may be spoofed or otherwise misleading.
Stage 2—Trust and urgency: The caller introduces an account problem, suspicious transaction, job opportunity, or urgent administrative task. The target is encouraged to remain on the call and avoid checking independently.
Stage 3—Call-merge request: The target is asked to merge another call, supposedly involving a verification team or automated banking system. The feature itself is legitimate; the deceptive instruction is the risk.
Stage 4—Authentication exposure: The attacker attempts to obtain or overhear an OTP, induce the target to read it aloud, or misuse information disclosed during the conversation. Not every call-merge incident involves an OTP, and the model should not assume a specific technical interception mechanism without evidence.
Stage 5—Payment manipulation: The caller frames a payment as a refund, account-protection step, verification transfer, or other legitimate action. The target may approve

Table 1

Stakeholder	*Recommended measure*	*Implementation approach*	*Success indicators*
RBI / payment regulators	Risk-based payment confirmation for high-risk transfers	Define proportionate triggers; require clear warnings and independent confirmation for anomalous payments	Fraud loss rate; intervention rate; false-positive rate
DoT / telecom regulator / operators	Standardized warning when a suspicious call pattern coincides with financial-risk indicators	Pilot user-facing alerts; do not treat call merging alone as proof of fraud	Warning comprehension; scam conversion rate
Banks and UPI participants	Recipient and purpose confirmation; step-up checks for unusual new-payee transfers	Use transaction context, device signals, and customer-configurable safeguards	Time to block; confirmed APP losses; customer friction
I4C / law enforcement / banks	Rapid, structured incident exchange	Common incident fields, secure escalation, and preservation of evidence with access controls	Time from report to bank action; funds frozen/recovered
Government of India	National multilingual anti-vishing programme	Short scenario-based messages in regional languages through banks, telecoms, schools, and community networks	Awareness retention; reporting latency; reach by region
Legislators / regulators	Transparent liability and reimbursement standards	Assess shared responsibility across payment, telecom, and online platforms; define fair exceptions and dispute review	Claims resolution time; reimbursement consistency
AI governance and data-protection authorities	Privacy and algorithmic accountability requirements	Data minimization, impact assessments, audit logs, human review, retention limits	Audit compliance; subgroup performance; privacy complaints
Research institutions	Independent evaluation and open aggregate reporting	Pre-register pilots; publish anonymized statistics and negative results	Reproducibility; dataset quality; independent validation

a payment request or transfer funds to an attacker-controlled or mule account.

Stage 6—Movement and recovery: Funds may move rapidly through multiple accounts. Early reporting to the bank and relevant national reporting channels can improve the chance of intervention, although recovery is not guaranteed.

Proposed AI-Assisted Defence Architecture

Risk Signals and Decision Support

The proposed system is a risk-scoring aid, not an autonomous accusation engine. With appropriate consent, legal authority, and data minimization, telecom and payment providers could evaluate signals such as an unusual sequence of call merging, a new payee, a first-time high-value transfer, recent account recovery, unusual device/session behavior, repeated failed authentication, or a payment inconsistent with the customer's history. No single signal should automatically label a customer or caller as fraudulent.

Multi-Layer Decision Flow

A practical workflow has four steps: (1) generate a risk score from available event metadata; (2) apply a policy threshold that considers transaction amount and customer context; (3) introduce friction proportionate to risk, such as a plain-language warning, a cooling-off period, or confirmation through a separately verified channel; and (4) record the reason for the intervention and allow rapid human review. High-risk payments may require an out-of-band confirmation initiated through the bank's official app or a number independently obtained by the customer.

Privacy-Preserving AI

Routine recording or semantic monitoring of every personal call would raise substantial privacy, consent, and surveillance concerns. A safer initial design uses minimal event metadata and payment-side signals, with audio analysis restricted to lawful, clearly disclosed, narrowly scoped pilots. Models should be tested across languages, accents, age groups, disability-related speech patterns, and network conditions. False positives can lock out legitimate customers; false negatives can create a misleading sense of security.

Model Governance and Evaluation

An AI deployment should document its intended use, data sources, retention period, performance by subgroup, security controls, appeal process, and incident response. The NIST AI Risk Management Framework offers a useful voluntary structure for governing AI risks. Evaluation should report precision, recall, false-positive rate, time-to-intervention, customer abandonment, complaint rate, and confirmed loss prevented. Results should be independently audited before any nationwide mandate.

Policy Recommendations

The following recommendations are proposed policy options, not statements of existing legal requirements.



They build on RBI awareness guidance, India's cyber-fraud reporting channel, and comparative APP reimbursement experience in the UK [3]–[6].

Practical Prevention And Response

For users: Do not disclose an OTP, PIN, password, or UPI PIN to a caller. Do not merge a call because a stranger claims it is required for bank verification. End the conversation and contact the institution using the number printed on the card, its official app, or its official website. Read the transaction details and recipient name before approving any payment.

For banks and payment providers: Make warnings specific to the transaction, explain why a payment has been flagged, provide a simple cancel option, and maintain a 24-hour fraud-reporting route. Where legally and technically feasible, prioritize rapid recall, beneficiary-account review, and evidence preservation after a report.

For victims in India: Contact the bank immediately and report suspected financial cyber fraud through helpline 1930 and the National Cyber Crime Reporting Portal. Preserve transaction IDs, timestamps, phone numbers, messages, and screenshots. Reporting quickly may help intervention, but does not guarantee reimbursement or recovery.

Research Agenda And Limitations

The central limitation is the absence of a standardized public dataset that isolates call-merge scams from the wider categories of vishing, impersonation, and APP fraud. Public statistics are not directly comparable across countries because definitions, reporting coverage, payment rails, and reimbursement rules differ.

Future work should: (1) establish a common taxonomy for confirmed and suspected call-merge incidents; (2) evaluate whether call-state metadata adds predictive value beyond payment-risk signals; (3) conduct user studies comparing warnings and independent-callback prompts; (4) test AI performance across language and demographic groups; and (5) compare intervention and reimbursement outcomes across jurisdictions. Any claim of effectiveness should be based on measured outcomes rather than assumed benefits.

Conclusion

Call-merge scams illustrate how an ordinary communication feature can be incorporated into a wider social-engineering attack. The key risk is not the merge function in isolation, but the combination of impersonation, urgency, authentication exposure, and a payment decision made under deception. A defensible response should therefore combine user education with risk-based payment controls, telecom context, rapid reporting, and accountable AI-assisted decision support. Governments can help by standardizing incident data, improving cross-sector escalation, clarifying reimbursement expectations, and requiring transparent evaluation of new controls. The next research priority is to validate the proposed model using documented incidents rather than relying on unverified prevalence claims.

Acknowledgment

The authors are thankful to Department of Electronics & Communication, V.V.P. Engineering College, Rajkot, Gujarat, India.

References

[1] Anderson, R., Clayton, R., & Moore, T. (2012). *The economics of information security*. Annual Review of Economics, 4(1), 333-356.

[2] BIS. (2018). *Retail payments: recent developments, trends and analysis*. Bank for International Settlements, Committee on Payments and Market Infrastructures.

[3] European Banking Authority (EBA). (2017). *Opinion of the European Banking Authority on the transition from the Payment Services Directive (PSD1) to the revised Payment Services Directive (PSD2)*. EBA/Op/2017/14.

[4] Federal Trade Commission (FTC). (2017). *Consumer Sentinel Network Data Book for 2017*. Federal Trade Commission Office of Technology Research and Investigation.

[5] Gartner. (2018). *Market Guide for Online Fraud Detection*. Gartner Research Report G00350702.

[6] KPMG. (2018). *Global Banking Fraud Survey: Shifting paradigms in financial crime*. KPMG International Cooperative.

[7] Reserve Bank of India (RBI). (2017). *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18.

[8] Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

[9] UK Finance. (2018). *Fraud - The Facts 2018: The Definitive Overview of Payment Industry Fraud*. UK Finance Annual Report.

[10] Whitcomb, C. (2016). *Social Engineering: The Art of Human Hacking*. Wiley / John Wiley & Sons.