
FINANCIAL FRAUD DETECTION IN DIGITAL PAYMENT ECOSYSTEMS

Dr. V. Sangeetha

Associate Professor

Department of Computer Science with Data Analytics

Dr. N.G.P. Arts and Science College

Coimbatore, Tamil Nadu, India

Abstract

Digital payment ecosystems have transformed the way individuals, merchants, banks, fintech firms, and public agencies transfer value. Mobile wallets, instant account-to-account transfers, payment cards, QR-based transactions, payment gateways, and embedded finance services improve convenience and market access, but they also create a broad and rapidly changing environment for financial fraud. Fraudsters exploit stolen credentials, social engineering, malware, synthetic identities, account takeover, device manipulation, mule networks, and weaknesses in merchant or platform controls. The resulting losses affect consumers, payment providers, merchants, and confidence in digital financial services.

This review-based study examines financial fraud detection in digital payment ecosystems through a risk-management, data-analytics, and consumer-protection perspective. It considers fraud typologies, transaction-data characteristics, detection methods, operational controls, and governance requirements. The paper synthesizes evidence from fraud analytics research, payment-security guidance, financial crime literature, and digital-risk management frameworks to identify how suspicious behaviour can be detected without undermining legitimate user experience or data privacy. The analysis indicates that effective fraud detection depends on layered controls rather than on a single model or authentication mechanism. Real-time risk scoring, behavioural analytics, device intelligence, network analysis, anomaly detection, supervised machine learning, rule-based controls, and human investigation each perform different functions. Sustainable fraud prevention also requires transparent escalation procedures, customer education, privacy-aware data governance, continuous model monitoring, and collaboration among payment participants. A balanced approach can reduce fraudulent activity while preserving trust, inclusion, and reliability in digital payment ecosystems.

Keywords: Financial fraud; Digital payments; Fraud detection; Payment security; Machine learning; Behavioural analytics; Account takeover; Transaction monitoring; Cyber resilience; Consumer protection

1. INTRODUCTION

Digital payments now operate through interconnected networks of banks, payment system operators, card schemes, mobile applications, merchants, payment aggregators, telecommunications providers, cloud services, and identity systems. These connections enable users to make payments across physical and digital channels with limited delay. At the same time, they increase the number of points at which a transaction can be misdirected, impersonated, manipulated, or otherwise abused. Fraud detection has therefore become a core operational requirement for institutions that provide or support payment services.

Financial fraud in digital payments does not refer to one isolated offence. It includes unauthorized transfers, account takeover, card-not-present fraud, merchant fraud, application

fraud, QR-code substitution, phishing-led payment scams, refund abuse, mule-account activity, and forms of identity misuse. Some incidents are driven by technical compromise, while others depend primarily on deception and coercion. In practice, fraud schemes often combine both: a victim may be persuaded to share a one-time password, click a malicious link, install remote-access software, or approve a payment that appears legitimate.

The speed of digital payments creates a difficult control problem. Payment providers must approve a large volume of legitimate transactions quickly, while recognising the small proportion that carries material fraud risk. Excessively strict controls may block genuine users, disrupt essential purchases, and reduce financial inclusion. Weak controls can permit fraud, damage customer confidence,

increase dispute-management costs, and expose institutions to regulatory and reputational risk. The challenge is to make risk decisions that are timely, explainable, and proportionate to the transaction context.

Fraud detection is therefore best understood as a socio-technical process. It combines secure product design, identity and authentication controls, transaction monitoring, data quality, alert investigation, customer support, incident response, and institutional accountability. This paper analyses these connected dimensions and outlines practical directions for strengthening fraud detection in digital payment ecosystems.

2. LITERATURE REVIEW

The fraud-detection literature shows a transition from static rule-based monitoring toward data-driven and adaptive methods. Earlier systems commonly relied on simple rules, such as value thresholds, blocked merchant categories, or repeated failed attempts. These controls remain useful because they are transparent and easy to implement, but they may fail when criminals alter transaction amounts, devices, locations, or timing patterns. More recent research therefore examines statistical methods, anomaly detection, supervised learning, sequence analysis, graph-based methods, and hybrid systems that combine expert rules with learned models.

A central theme in the literature is the difficulty of learning from highly imbalanced data. Fraudulent transactions are generally much less frequent than legitimate transactions, and labels may arrive only after a complaint, chargeback, investigation, or recovery process. Fraud patterns can also change rapidly as criminals adapt to new security measures. Researchers consequently emphasise evaluation methods that consider precision, recall, false-positive cost, detection delay, calibration, and operational workload rather than using overall classification accuracy alone.

2.1 DIGITAL PAYMENTS AND FRAUD RISK

Digital payment channels generate multiple data signals that can be useful for fraud assessment. Examples include transaction amount, time, currency, beneficiary, merchant category, account age, device identifier,

application version, IP address, geographic context, authentication result, payment history, and the relationship between counterparties. No single field can reliably establish fraud. Instead, risk often appears through unusual combinations of signals, such as a new device used immediately after credential changes, a rapid sequence of transfers to new beneficiaries, or behaviour that differs materially from a customer's previous activity. Account takeover is a major concern because a compromised account can appear to belong to a legitimate customer. Attackers may obtain credentials through phishing, password reuse, malware, SIM-swap activity, social engineering, or data breaches. Strong authentication reduces some of this risk, but it does not remove it when the user has been deceived or when the device itself is compromised. Detection systems therefore need to assess changes in behaviour, device trust, beneficiary novelty, and session anomalies in addition to checking whether an authentication challenge was completed.

Merchant and platform risks also require attention. Fraud may originate through fake merchant onboarding, collusive refund activity, manipulated payment requests, chargeback abuse, synthetic transactions, or exploitation of weak application programming interfaces. Payment aggregators and marketplaces can be particularly exposed because they connect many buyers and sellers and may have varying levels of visibility over fulfilment, delivery, or customer identity. Monitoring must include both payer-side and payee-side activity so that fraud is not treated only as a consumer-authentication problem.

The fraud landscape is further shaped by user awareness and accessibility. Digital payments should remain usable for new users, elderly customers, small merchants, and people with limited digital literacy. Security messages that are unclear, overly technical, or displayed too late may not prevent deception. Effective controls must therefore be supported by simple warnings, accessible dispute channels, responsible interface design, and timely communication with customers when risk is detected.

2.2 FRAUD DETECTION APPROACHES

Rule-based detection remains an important first line of defence. Rules can flag

transactions that exceed risk thresholds, involve sanctioned or previously reported accounts, occur after unusual login events, or show repeated failed authentication attempts. They support quick policy changes during known attack campaigns and can be reviewed by compliance, fraud, and operations teams. However, rules can become brittle when criminal behaviour changes or when large rule sets create conflicting alerts.

Supervised machine-learning models use labelled examples of past legitimate and fraudulent activity to estimate the probability that a new event is suspicious. Logistic regression, decision trees, random forests, gradient boosting, neural networks, and related models can identify complex interactions among transaction features. Their performance depends on reliable labels, representative training data, thoughtful feature engineering, and controls for bias or leakage. A model that performs well in retrospective testing may still fail in live operation if payment behaviour or attack patterns change.

Anomaly detection is useful where confirmed fraud labels are limited or delayed. These methods establish a baseline of normal behaviour and identify deviations, such as atypical transaction velocity, unexpected device changes, unusual beneficiary networks, or rapid movement of funds. Anomaly scores should not automatically be treated as proof of fraud. They are most useful when combined with contextual checks, business rules, and human review, because legitimate customers may also display unusual behaviour during travel, emergencies, seasonal purchases, or changes in income.

Network and graph analytics extend the analysis beyond individual transactions. They can examine links among accounts, devices, merchants, phone numbers, beneficiaries, and transaction flows to identify clusters, mule-account patterns, or coordinated activity. Real-time streaming systems are increasingly important because many payment decisions must be made within seconds. This requires controls that are scalable, auditable, resilient, and able to deliver clear reasons for intervention to operations teams and customers.

3. OBJECT OF STUDY

The primary object of this study is to examine how financial fraud can be detected, assessed, and prevented within digital payment ecosystems. The study focuses on the relationship between payment-channel design, user behaviour, transaction data, fraud typologies, risk-scoring methods, and governance arrangements. It treats fraud detection as a continuous process that begins before a payment is initiated and continues through monitoring, investigation, customer redress, and learning from confirmed incidents.

The paper considers common digital-payment environments, including cards, mobile wallets, instant transfers, QR-based payments, payment gateways, online merchant platforms, and account-to-account payment services. It examines how fraud risk can arise at onboarding, login, payment initiation, authentication, beneficiary addition, merchant settlement, refund processing, and post-transaction dispute stages. This broad view is necessary because fraud can move across channels and exploit control gaps between institutions.

A further objective is to identify the mechanisms through which a suspicious event becomes a financial loss. These mechanisms include compromised credentials, deceptive communications, weak identity verification, device compromise, delayed detection, ineffective alerts, poor customer support, and gaps in coordination among payment participants. The study also considers the operational consequences of false positives, including unnecessary declines, friction, delayed access to funds, and erosion of user trust.

Finally, the study evaluates layered fraud-management strategies involving risk-based authentication, behavioural analysis, secure system architecture, model governance, human oversight, consumer education, and incident response. The purpose is not only to describe fraud techniques but to clarify practical measures that support payment security, financial inclusion, privacy, and confidence in digital financial services.

3.1 FRAUD TYPOLOGIES AND ATTACK SURFACE

This subsection examines the principal forms of fraud and control weaknesses that can affect digital payment transactions.

- Assessment of phishing, impersonation, social engineering, malware, and remote-access scams that target customer credentials or approval behaviour.
- Analysis of account takeover, credential stuffing, SIM-swap risks, device compromise, and session hijacking.
- Examination of card-not-present fraud, QR-code manipulation, payment-link abuse, fake merchant activity, and refund or chargeback abuse.
- Evaluation of mule accounts, beneficiary networks, rapid fund movement, and coordinated transaction patterns.
- Study of onboarding vulnerabilities, synthetic identity risk, weak know-your-customer checks, and document manipulation.
- Consideration of third-party, cloud, application programming interface, and merchant-integration risks within connected payment ecosystems.

3.2 DETECTION AND RISK ASSESSMENT DIMENSIONS

This subsection evaluates the data and decision dimensions that support effective fraud detection.

- Transaction amount, velocity, timing, channel, merchant, beneficiary, and geographic context.
- Customer behaviour, account history, login pattern, device profile, session activity, and authentication outcome.
- Network relationships among accounts, devices, recipients, merchants, phone numbers, and transaction pathways.
- Risk scores, rules, alerts, confidence levels, review priorities, and possible customer-impact outcomes.
- False positives, missed fraud, decision latency, operational workload, recovery potential, and dispute-management cost.
- Data quality, label delay, model drift, privacy restrictions, explainability, fairness, and audit requirements.

3.3 GOVERNANCE, PRIVACY AND RESILIENCE

This subsection considers institutional measures that reduce fraud risk while protecting legitimate users and payment-system integrity.

- Risk-based authentication, secure credential management, device binding, transaction confirmation, and session protection.
- Clear governance for fraud rules, model approval, monitoring, escalation, exception handling, and periodic validation.
- Privacy-aware data minimisation, access controls, retention policies, secure sharing, and lawful use of personal data.
- Continuous monitoring of payment flows, threat intelligence, incident reporting, and coordinated response among relevant entities.
- Customer education, accessible warnings, rapid support channels, dispute resolution, and timely communication after suspected fraud.
- Business continuity, cyber-resilience testing, staff training, vendor oversight, and post-incident review to strengthen future controls.

4. RESEARCH METHODOLOGY

The present study adopts a review-based, descriptive, analytical, and comparative methodology to examine financial fraud detection in digital payment ecosystems. The methodology brings together concepts from financial crime prevention, payment security, machine learning, information systems, consumer protection, and cyber-resilience. It is designed to identify how fraud signals are generated, how they are interpreted, and how detection decisions affect both security outcomes and legitimate customer activity.

The study is based on secondary evidence from peer-reviewed research articles, institutional reports, payment-security guidance, financial-crime publications, standards, and policy documents. The material is interpreted through a thematic framework that considers fraud types, data signals, detection approaches, operational controls, governance, privacy, and resilience. Comparative analysis is used to distinguish the strengths and limitations of rule-based, statistical, machine-learning, behavioural, and network-oriented approaches.

4.1 RESEARCH DESIGN

The research follows a descriptive and comparative design to synthesise evidence on

fraud risk and detection practices in digital payment environments.

Component	Description
Research Type	Review-based, descriptive, analytical, comparative
Approach	Financial fraud risk, payment security, and data-analytics analysis
Data Source	Research articles, standards, reports, policy documents, and industry guidance
Analysis Method	Thematic synthesis and comparative assessment of detection approaches
Focus Area	Digital payments, fraud typologies, transaction monitoring, governance, and resilience

4.2 SOURCES AND ANALYTICAL CATEGORIES

The study considers the following evidence categories for evaluation:

- Research on financial fraud, credit-card fraud, account takeover, social engineering, and digital-payment risk.
- Transaction-monitoring, anomaly-detection, supervised-learning, sequence-analysis, and graph-analytics studies.
- Payment-security standards, cyber-resilience guidance, authentication frameworks, and digital identity publications.
- Consumer-protection, anti-money-laundering, data-governance, and operational-resilience documents.
- Each evidence source is analysed based on:
- Fraud type, attack pathway, affected payment channel, and relevant threat actor behaviour.
- Available data signals, feature quality, label availability, and timing of detection decisions.
- Detection performance, explainability, false-positive impact, investigation workload, and recovery potential.
- Governance, privacy, customer-protection, security-control, and incident-response implications.

5. DATA ANALYSIS

The data analysis synthesises evidence on how digital payment fraud can be detected through linked behavioural, transactional, technical, and network signals. A typical sequence begins when a payment event is initiated; the platform evaluates the account, device, payment context, authentication result,

beneficiary, and historical behaviour; the system assigns a risk score or applies control rules; and the transaction is approved, declined, delayed, or escalated for review. The quality of this process depends on whether signals are timely, accurate, and interpreted in a way that reflects both customer risk and operational consequences.

Behavioural deviations are particularly important in real-time payment settings. A transaction may be suspicious when it occurs from a new device, follows multiple failed login attempts, is directed to a newly added beneficiary, or forms part of an unusually rapid sequence of transfers. However, deviations are not always fraudulent. A legitimate user may change phones, travel, make an emergency payment, or receive a first-time salary or business payment. Detection systems must therefore use contextual evidence and avoid treating any individual signal as conclusive.

Supervised models can improve prioritisation when historical fraud labels are available. They can identify combinations of features that have been associated with confirmed fraud, but their results must be monitored for drift, imbalance, and changing attacker tactics. A model must also be evaluated against business costs. A system that prevents some fraudulent transfers but blocks large numbers of legitimate low-income users, small merchants, or time-sensitive payments may create unacceptable harms. Thresholds should therefore be calibrated using risk appetite, operational capacity, and customer-impact analysis.

Network analysis provides an additional layer of insight. It can reveal connections that are

not visible when each transaction is assessed alone, including multiple accounts using the same device, clusters of recipients linked to rapid pass-through behaviour, or merchant patterns that differ from normal settlement activity. These indicators can support investigation and proactive intervention, particularly where mule accounts or coordinated groups are involved. Network signals should be governed carefully because they can be sensitive, complex to explain, and affected by data-sharing restrictions.

The evidence also shows that fraud detection is strengthened when it is combined with secure engineering and customer-centred controls. Strong authentication, device and session protection, secure application development, clear payment confirmation, recipient verification, transaction limits, and immediate alerts can reduce the opportunity for fraud before an analytical model is required. When suspicious activity is detected, timely communication and an accessible support process can limit loss and improve customer confidence.

6. DISCUSSION

The findings indicate that financial fraud detection in digital payment ecosystems requires a layered and adaptive framework. No single control is sufficient because fraud may involve compromised credentials, manipulation of user consent, fraudulent merchants, mule networks, or weaknesses in third-party systems. Effective programmes combine prevention, detection, investigation, recovery, learning, and customer protection. The objective is not simply to identify transactions that look unusual, but to make proportionate decisions that reduce loss while supporting legitimate payment activity.

One important observation is that authentication should be treated as a risk-management process rather than as a one-time technical checkpoint. A successful password or one-time code does not always demonstrate that a user is acting voluntarily or that the session is safe. Risk-based checks, behavioural analysis, device trust, beneficiary novelty, and contextual prompts can add protection when a transaction presents elevated risk. At the same time, these controls should be designed to be understandable and accessible so that security

measures do not unfairly exclude or confuse users.

The discussion also highlights the value of human oversight. Automated systems can sort large volumes of activity and prioritise high-risk cases, but investigators are needed to interpret complex context, recognise emerging patterns, resolve customer disputes, and challenge flawed model outputs. Human review must be supported by clear case-management procedures, evidence retention, escalation pathways, and feedback loops that improve rules and models after confirmed incidents.

Privacy, fairness, and accountability are essential. Fraud detection frequently relies on data about behaviour, devices, locations, relationships, and past transactions. Institutions should collect and use this information lawfully, minimise unnecessary data, protect it from misuse, and ensure that automated decisions are auditable. Governance should include model validation, bias testing, access controls, vendor oversight, incident reporting, and customer redress. These measures help ensure that fraud prevention reinforces rather than weakens trust in the payment ecosystem.

Finally, resilient payment ecosystems require cooperation. Banks, fintech companies, payment operators, merchants, cybersecurity teams, regulators, law-enforcement agencies, and consumers each hold different information and responsibilities. Structured information sharing, common reporting standards, rapid response arrangements, and fraud-awareness campaigns can improve collective capacity to identify and disrupt emerging schemes. Such cooperation must be designed with safeguards for confidentiality, competition, and personal-data protection.

7. CONCLUSION

This study concludes that financial fraud detection is a foundational requirement for secure and trusted digital payment ecosystems. The expansion of mobile, card-based, instant, and platform-mediated payments offers significant benefits, but it also creates opportunities for account takeover, deception, identity misuse, merchant abuse, mule-account activity, and other forms of financial crime. Fraud risk must therefore be managed across the full payment lifecycle, from onboarding

and authentication to transaction monitoring, dispute handling, and recovery.

The analysis shows that effective detection depends on a combination of rule-based controls, real-time risk scoring, behavioural analytics, machine learning, anomaly detection, network analysis, secure system design, and informed human review. These tools should be evaluated not only by technical accuracy but also by false-positive impact, decision speed, explainability, customer experience, privacy, and fairness. Continuous monitoring is necessary because fraud patterns, payment channels, and attacker methods change over time.

8. REFERENCES

1. Abdallah, A., Maarof, M. A., and Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, 90-113. <https://doi.org/10.1016/j.jnca.2016.04.007>
2. Akoglu, L., Tong, H., and Koutra, D. (2015). Graph based anomaly detection and description: A survey. *Data Mining and Knowledge Discovery*, 29, 626-688. <https://doi.org/10.1007/s10618-014-0365-y>
3. Baesens, B., Van Vlasselaer, V., and Verbeke, W. (2015). *Fraud Analytics: Using Descriptive, Predictive, and Social Network Techniques*. Wiley.
4. Bank for International Settlements. (2016). *Guidance on Cyber Resilience for Financial Market Infrastructures*. Committee on Payments and Market Infrastructures and IOSCO.
5. Bhattacharyya, S., Jha, S., Tharakunnel, K., and Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3), 602-613. <https://doi.org/10.1016/j.dss.2010.08.008>
6. Bolton, R. J., and Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235-255. <https://doi.org/10.1214/ss/1042727940>
7. Carcillo, F., Dal Pozzolo, A., Le Borgne, Y.-A., Caelen, O., Mazzer, Y., and Bontempi, G. (2018). SCARFF: A scalable framework for streaming credit card fraud detection with Spark. *Information Fusion*, 41, 182-194. <https://doi.org/10.1016/j.inffus.2017.09.005>
8. Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), Article 15. <https://doi.org/10.1145/1541880.1541882>
9. European Banking Authority. (2019). *Guidelines on ICT and Security Risk Management*. EBA.
10. Financial Action Task Force. (2021). *Opportunities and Challenges of New Technologies for AML/CFT*. FATF/OECD.
11. Financial Action Task Force. (2021). *Guidance on Digital Identity*. FATF/OECD.
12. Ghosh, S., and Reilly, D. L. (1994). Credit card fraud detection with a neural-network. *Proceedings of the 27th Hawaii International Conference on System Sciences*, 621-630.
13. Hand, D. J. (2010). Fraud detection: A statistical challenge. In C. C. Aggarwal (Ed.), *Data Mining and Knowledge Discovery Handbook* (2nd ed.). Springer.
14. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., and Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234-245. <https://doi.org/10.1016/j.eswa.2018.01.037>
15. Kou, Y., Lu, C.-T., Sirwongwattana, S., and Huang, Y.-P. (2004). Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing and Control*, 749-754. <https://doi.org/10.1109/ICNSC.2004.1297040>
16. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., and Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559-569. <https://doi.org/10.1016/j.dss.2010.08.006>

A sustainable response requires governance and resilience as well as technology. Payment providers should strengthen authentication, secure applications and interfaces, monitor emerging threats, support rapid customer reporting, test response processes, and maintain transparent accountability for automated decisions. By combining data-driven detection with consumer protection, privacy-aware governance, and coordinated action among payment participants, digital payment ecosystems can reduce fraud while remaining accessible, reliable, and inclusive.

17. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST.
18. National Institute of Standards and Technology. (2020). Zero Trust Architecture. NIST Special Publication 800-207. <https://doi.org/10.6028/NIST.SP.800-207>
19. OECD. (2022). OECD Recommendation on Digital Security Risk Management. Organisation for Economic Co-operation and Development.
20. Phua, C., Lee, V., Smith, K., and Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review*, 34, 1-14. <https://doi.org/10.1007/s10462-009-9121-9>
21. Randhawa, K., Loo, C. K., Seera, M., and Lim, C. P. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access*, 6, 14277-14284. <https://doi.org/10.1109/ACCESS.2018.2806420>
22. Reserve Bank of India. (2021). Reserve Bank of India (Digital Payment Security Controls) Directions, 2021. RBI.
23. Reserve Bank of India. (2025). Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025. RBI.
24. Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology.
25. Sorournejad, S., Zojaji, Z., Ebrahimi Atani, R., and Monadjemi, A. H. (2016). A survey of credit card fraud detection techniques: Data and technique oriented perspective. arXiv:1611.06439.
26. The International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. ISO.
27. United Nations Office on Drugs and Crime. (2021). Cyber-Enabled Fraud: A Review of the Threat Landscape. UNODC.
28. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., and Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 18, 30-55. <https://doi.org/10.1007/s10618-008-0116-z>
29. West, J., and Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers and Security*, 57, 47-66. <https://doi.org/10.1016/j.cose.2015.05.005>
30. World Bank. (2022). The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. World Bank. <https://doi.org/10.1596/978-1-4648-1897-4>