**CHAPTER 1: INTRODUCTION**

**1.1. Background and Context**

**1.1.1. Supply Chain Fraud as Critical Operational Risk**

In modern supply chain management, fraud represents a critical operational risk that fundamentally undermines supply chain efficiency, profitability, and sustainability. According to supply chain risk management theory, risks can be categorized into two primary types: disruption risks, which are high-impact but low-probability events such as natural disasters or geopolitical conflicts, and operational risks, which are lower-impact but higher-probability events such as demand variability, quality issues, and fraud. Fraud occupies a unique and particularly challenging position within this taxonomy. While individual fraudulent transactions may appear as routine operational risks, systematic fraud can rapidly escalate into disruption-level threats that compromise entire supply chain networks.

Operational risks, as defined in supply chain literature, stem from activities and resources within the supply chain itself. Any potential source that negatively impacts the flow of information, goods, and cash constitutes an operational risk. Fraud specifically disrupts all three critical flows simultaneously. It corrupts information accuracy, leading to distorted demand signals. It diverts physical goods, resulting in inventory losses. It causes direct financial losses through unpaid or fraudulent transactions. This multi-dimensional impact makes fraud one of the most damaging operational risks in supply chain management.

From the perspective of risk management frameworks, supply chain fraud must be addressed through systematic approaches. The four generic operational hedging strategies provide a comprehensive toolkit for managing operational risks. These strategies include reserves and redundancy, diversification and pooling, risk sharing and transfer, and risk reduction. Among these strategies, fraud detection and prevention primarily falls under the fourth strategy, which emphasizes eliminating or minimizing root causes of risk through quick responses, supply chain collaboration, and continuous improvement. This research focuses specifically on developing a fraud detection system as a proactive risk reduction mechanism, enabling supply chains to identify and mitigate fraudulent activities before they escalate into larger disruptions.

**1.1.2. The DataCo Supply Chain Case**

This research utilizes the DataCo Supply Chain dataset, a comprehensive real-world dataset that captures the complexity and challenges of modern e-commerce supply chain operations. The dataset provides an ideal context for studying fraud detection due to its scale, diversity, and the presence of clearly labeled fraudulent transactions.

The DataCo dataset encompasses 180,519 transactions involving 20,652 unique customers and 118 unique products across multiple geographic regions and product categories. This substantial dataset size provides sufficient statistical power for developing and validating machine learning models while maintaining relevance to real-world supply chain operations. Table 1.1 summarizes the key characteristics of the dataset, including transaction counts, customer and product statistics, fraud prevalence, and network properties.

|  |  |
| --- | --- |
| **Metric** | **Value** |
| Total Transactions | 180,519 |
| Total Customers | 20,652 |
| Total Products | 118 |
| Fraudulent Transactions | 4,062 (2.25%) |
| Legitimate Transactions | 176,457 (97.75%) |
| Class Imbalance Ratio | 43.4 : 1 |
| Network Nodes | 20,770 |
| Network Edges (Unique Pairs) | 101,196 |
| Network Density | 0.000469 |
| Connected Components | 19 |
| Largest Component Size | 12,431 nodes |
| Average Customer Degree | 4.90 products |
| Fraud Customer Average Degree | 7.40 products |
| Normal Customer Average Degree | 4.71 products |

**Table 1.1:**

As shown in Table 1.1, the dataset includes comprehensive information about each transaction, including customer identifiers, product details, order values, shipping information, payment methods, and order status indicators that serve as fraud labels. This definition was chosen for several critical reasons. First, the suspected fraud label rep resents a clear and unambiguous indicator of fraudulent activity, as opposed to ambiguous proxy indicators such as late deliveries or negative profit margins. Second, this label reflects real-world fraud detection outcomes where supply chain operators have identified suspicious transactions through existing detection mechanisms or post-transaction investigations. Third, with 4,062 fraudulent transactions representing 2.25 percent of the total dataset, the class imbalance ratio of approximately 43.4 to 1 between legitimate and fraudulent transactions is realistic but manageable for machine learning approaches.

The fraud rate of 2.25 percent aligns with industry observations where fraud, while not overwhelmingly common, occurs frequently enough to warrant systematic detection mechanisms. This prevalence rate is substantial enough to cause significant financial damage while being challenging to detect through manual inspection alone. The remaining 176,457 transactions in the dataset represent legitimate customer purchases, providing a robust baseline for understanding normal supply chain behavior patterns.

Beyond the transactional data, the dataset structure enables the construction of sophisticated network representations. Each transaction creates a connection between a customer and a product, forming a natural bipartite network. This network contains 20,770 nodes, consisting of 20,652 customer nodes and 118 product nodes. The network includes 101,196 edges representing unique customer-product pairs. Analysis of the network structure reveals 19 connected components, with the largest component containing 12,431 nodes, accounting for approximately 60 percent of the entire network. The network exhibits a density of 0.000469, indicating a sparse but informative structure.

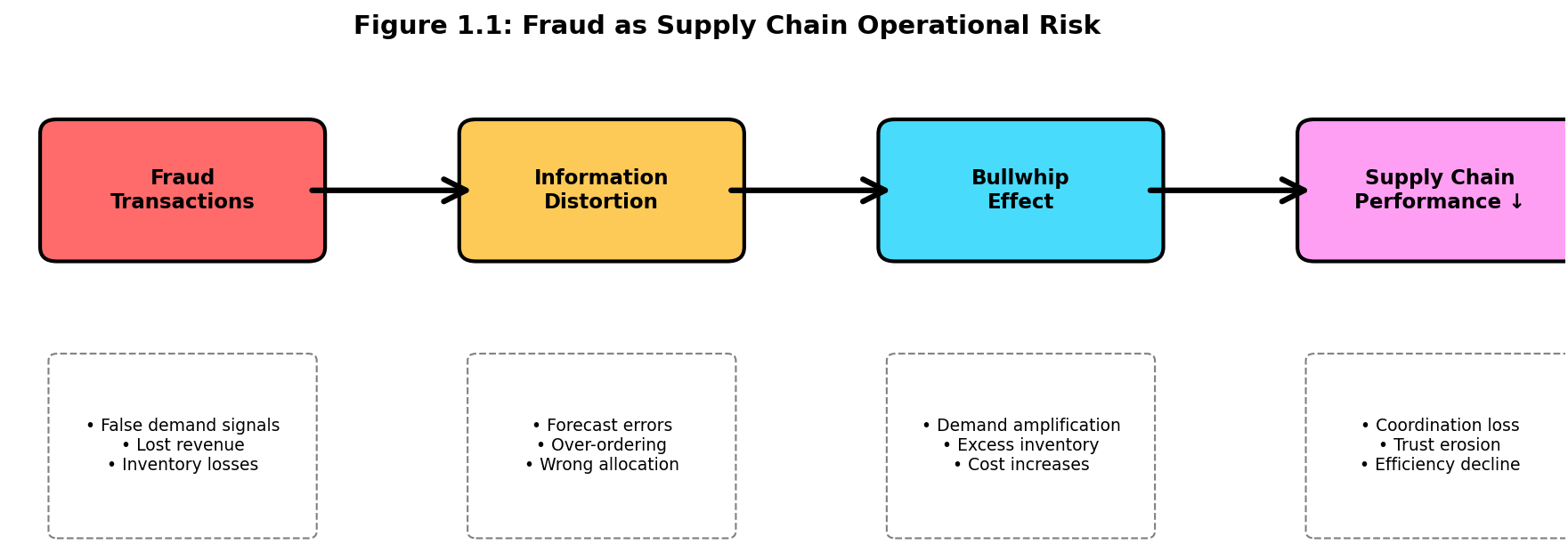
This sparse network structure is particularly valuable for fraud detection. The sparsity means that fraudulent patterns, such as customers purchasing unusual combinations of products or exhibiting abnormal purchasing behaviors, become more distinguishable from normal customer behavior. The network topology provides additional signals beyond traditional transaction features, capturing the relational context in which fraudulent activities occur.

**1.1.3. Fraud Impact on Supply Chain Performance**

The impact of fraud extends far beyond direct financial losses, creating cascading effects throughout the supply chain that amplify its overall damage. Understanding these impacts through the lens of supply chain management theory reveals why fraud detection is not merely a security concern but a fundamental supply chain coordination challenge.

The immediate financial impact of fraud includes several components. Lost revenue occurs when fraudulent transactions result in shipped products without payment. Unrecoverable goods represent direct inventory losses as products shipped to fraudulent customers are typically not retrievable. Investigation and processing costs accumulate as each suspected fraud case requires investigation time, administrative overhead, and potential legal expenses. Chargeback fees are imposed by payment processors when transactions are reversed due to fraud. In the DataCo dataset, assuming an average transaction value of one thousand dollars, the 4,062 fraudulent transactions represent a direct fraud exposure of approximately 4,062,000 dollars. This substantial financial exposure justifies significant investment in fraud detection systems.

However, the indirect costs of fraud are often more severe and longer-lasting than direct losses. From the perspective of supply chain coordination theory, fraud creates several critical problems that undermine supply chain performance. Figure 1.1 illustrates the cascading effects of fraud through the supply chain, showing how fraudulent transactions lead to information distortion, which amplifies the bullwhip effect and ultimately degrades overall supply chain performance.



**Figure 1.1: Fraud as Supply Chain Operational Risk**

As illustrated in Figure 1.1, fraudulent transactions inject false demand signals into the supply chain, distorting forecasting models and leading to over-ordering from suppliers, excess inventory accumulation, and eventually costly corrections when the fraud is discovered. This information distortion amplifies the bullwhip effect, which is the phenomenon where demand variability increases as one moves upstream in the supply chain. Each fraudulent transaction at the retail level creates disproportionate variability in wholesale orders, manufacturing schedules, and raw material procurement.

Second, products shipped to fraudulent customers could have been sold to legitimate customers, representing not just lost revenue but opportunity costs. This inventory misallocation becomes particularly costly for products with limited shelf life, seasonal demand, or high holding costs. The misallocation problem extends beyond individual products to affect overall inventory planning and safety stock decisions across the supply chain network.

Third, systematic fraud undermines trust among supply chain partners. When fraud rates are high, suppliers may impose stricter payment terms, require higher security deposits, or reduce credit limits. All of these responses increase transaction costs and reduce supply chain flexibility. This erosion of trust is particularly damaging for coordination mechanisms such as vendor-managed inventory or collaborative planning, forecasting, and replenishment, which rely fundamentally on transparent information sharing and mutual confidence among partners.

Fourth, fear of fraud leads to more conservative supply chain policies. Organizations implement longer payment verification times, stricter customer authentication requirements, and reduced willingness to offer flexible payment terms. While these measures provide some protection against fraud, they simultaneously reduce the supply chain's ability to respond quickly to legitimate demand changes, ultimately harming customer service levels and competitive positioning in the market.

**1.1.4. Connection to Supply Chain Management Theory**

This research directly addresses fundamental concepts from multiple chapters of supply chain management theory, demonstrating how fraud detection serves as a critical application of theoretical frameworks taught in the course.

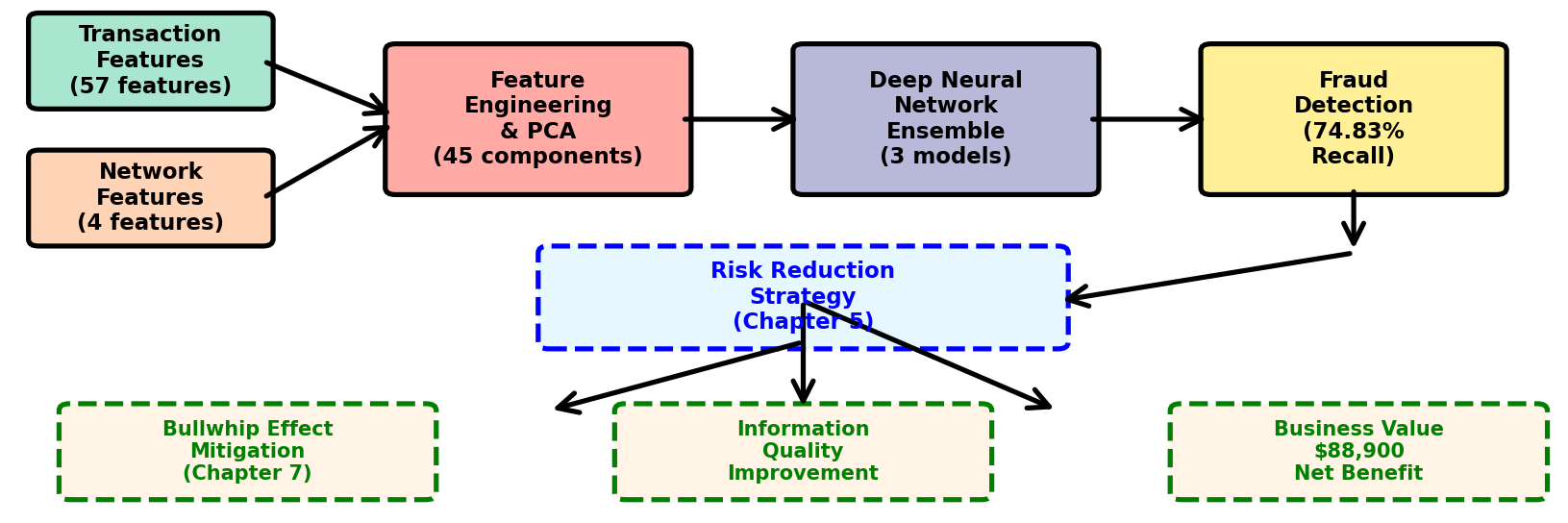
The primary theoretical foundation comes from Chapter 5 on supply chain risk hedging. Among the four operational hedging strategies discussed in the course, fraud detection represents a clear application of the fourth strategy focused on reducing or eliminating root causes of risk. Rather than simply maintaining reserves to absorb fraud losses or diversifying to spread risk, this research focuses on developing predictive capabilities that identify and prevent fraud before it occurs. This proactive approach aligns with the principle of continuous improvement and root cause analysis emphasized in risk reduction strategies. The research also demonstrates the concept of tailored risk management, where the specific characteristics of fraud risk, including its high frequency, moderate impact per incident, and pattern-based nature, dictate the appropriate mitigation strategy. By analyzing network patterns and transaction features, the system adapts to the specific manifestations of fraud in the DataCo supply chain context.

Chapter 7 on supply chain coordination and the bullwhip effect provides another crucial theoretical lens. Fraud directly relates to supply chain coordination challenges by creating information distortion, which is identified in the course as one of the primary causes of the bullwhip effect. Fraudulent transactions generate false demand signals that propagate through the supply chain, causing each upstream stage to amplify the perceived demand variability. The course emphasizes that lack of coordination results when objectives of different stages conflict and when information moving between stages is delayed or distorted. Fraud exemplifies both of these problems. The fraudster's objective directly conflicts with supply chain efficiency goals, and the fraudulent nature of transactions means the information being transmitted is fundamentally corrupted rather than merely delayed.

The course also identifies several behavioral obstacles to coordination that are highly relevant to fraud detection. Different stages of the supply chain view their actions locally and are unable to see the impact of their actions on other stages. In the context of fraud, a retailer dealing with fraudulent orders may not fully appreciate how these false demand signals affect upstream manufacturing and supplier decisions. Different stages react to the current local situation rather than trying to identify root causes. Without a systematic fraud detection system, each stage may implement ad-hoc responses to what appears to be unusual demand patterns without recognizing the underlying fraud problem. A lack of trust among supply chain partners causes them to be opportunistic at the expense of overall supply chain performance. High fraud rates can trigger this lack of trust, leading to defensive behaviors that harm coordination.

Chapter 3 on risk sharing contracts provides additional theoretical context. The course discusses how contracts affect firm profits, total supply chain profits, introduce information distortion, and influence supplier performance along key measures. Fraud detection can be viewed as a mechanism that enables better risk sharing arrangements. When fraud risk is well-managed through effective detection systems, supply chain partners can engage in more collaborative and less defensive contracting arrangements. The course emphasizes that supplier performance should be compared based on impact on total cost, considering factors beyond just purchase price. Fraud introduces hidden costs that affect total cost calculations, and effective fraud detection helps make these costs visible and manageable, enabling more accurate supplier evaluation and selection decisions.

Finally, Chapter 4 on risk pooling, centralization, and postponement offers relevant insights. The network-based approach to fraud detection employed in this research represents a form of information pooling. By analyzing patterns across the entire customer-product network rather than examining transactions in isolation, the system pools information to achieve better detection performance. This parallels the risk pooling principle where aggregating demand across multiple locations or products reduces overall variability and improves forecast accuracy. In fraud detection, pooling information across the network reduces the uncertainty about transaction authenticity by leveraging patterns across the entire network. Figure 1.2 presents the overall research framework, showing how transaction features and network features are integrated through feature engineering and deep learning to achieve fraud detection, which then contributes to supply chain risk reduction and performance improvement.

****

**Figure 1.2: Research Framework**

As shown in Figure 1.2, the research integrates transaction-based features (57 features) and network-based features (4 features) through a feature engineering process involving PCA dimensionality reduction to 45 components. These features feed into a deep neural network ensemble of three models, achieving 74.83 percent recall in fraud detection. This detection capability directly implements the risk reduction strategy from Chapter 5 and contributes to three key supply chain outcomes: mitigation of the bullwhip effect (Chapter 7), improvement in information quality throughout the supply chain, and generation of substantial business value with a net benefit of 88,900 dollars.

**1.2. Problem Statement**

**1.2.1. Limitations of Traditional Fraud Detection Methods**

Traditional fraud detection methods in supply chain contexts suffer from several critical limitations that reduce their effectiveness and prevent organizations from achieving adequate protection against fraudulent activities. Understanding these limitations provides essential context for why advanced machine learning approaches integrated with network analysis represent necessary innovations in fraud detection capabilities.

The most significant limitation of traditional methods is their high false negative rate, meaning they fail to detect a substantial portion of actual fraudulent transactions. Industry reports indicate that conventional rule-based systems and manual review processes miss between 40 and 60 percent of fraudulent transactions. In the context of the DataCo supply chain, a 50 percent false negative rate would mean that approximately 2,031 fraudulent transactions out of the 4,062 fraud cases would go undetected, resulting in direct losses exceeding two million dollars. This unacceptable miss rate stems from the inherent limitations of rule-based approaches, which can only detect fraud patterns that have been explicitly programmed into the system. As fraudsters continuously evolve their tactics to avoid detection, rule-based systems quickly become obsolete without constant manual updates.

Traditional methods also suffer from limited feature utilization. Conventional fraud detection systems typically rely exclusively on transaction-level features such as transaction amount, customer location, payment method, and order timing. While these features provide valuable signals, they represent only a partial view of the fraud problem. Transaction-only approaches fail to capture the relational and behavioral context in which fraud occurs. For example, the fact that a customer purchases an unusual combination of products, or that a customer's purchasing pattern differs significantly from similar customers in the network, provides important fraud signals that transaction-only features cannot capture. This limited feature space constrains the detection capability of traditional systems and allows sophisticated fraud schemes to evade detection.

Another fundamental limitation is that traditional methods are reactive rather than proactive. Most conventional fraud detection systems operate on a rule-based threshold model where transactions are flagged only after they exceed predefined limits or violate specific business rules. This reactive approach means the system only responds to fraud patterns that have already been observed and codified into rules. It cannot anticipate novel fraud schemes or adapt to evolving tactics without manual intervention. In rapidly changing e-commerce environments, this reactive posture places organizations perpetually one step behind fraudsters, who continuously experiment with new approaches to circumvent existing controls.

Furthermore, traditional fraud detection operates in isolation from broader supply chain planning and coordination processes. Fraud detection is often treated as a standalone security function rather than an integrated component of supply chain risk management. This siloed approach means that fraud detection insights are not systematically incorporated into demand forecasting, inventory planning, or supplier coordination decisions. As a result, even when fraud is eventually detected, its impact on supply chain coordination and the bullwhip effect has already occurred. The lack of integration prevents organizations from using fraud detection insights to improve overall supply chain performance and reduce the systemic costs associated with information distortion.

Traditional methods also lack sophisticated cost-benefit optimization. Most conventional systems apply uniform detection thresholds across all transaction types, failing to account for the varying costs of false positives versus false negatives across different products, customers, or transaction sizes. From a total cost perspective, the optimal detection threshold should balance the cost of investigating false positives against the cost of missing actual fraud. However, traditional systems rarely implement this type of cost-sensitive optimization, instead defaulting to conservative thresholds that either miss too much fraud or generate excessive false alarms that overwhelm investigation capacity.

**1.2.2. The Need for Network-Based Approach**

The limitations of traditional fraud detection methods create a compelling need for more sophisticated approaches that leverage network analysis and advanced machine learning techniques. Network-based fraud detection addresses the fundamental shortcoming of transaction-only methods by incorporating relational context and behavioral patterns that emerge from the structure of customer-product interactions.

The theoretical foundation for network-based fraud detection comes from recognizing that supply chains are inherently network structures where entities are interconnected through multiple types of relationships. In the DataCo supply chain context, customers and products form a bipartite network where transactions create edges between customer nodes and product nodes. This network structure encodes valuable information about customer behavior patterns, product popularity, and the relationships between different customers through their shared purchasing patterns. Fraudulent customers often exhibit different network characteristics compared to legitimate customers. They may purchase unusual combinations of products, have different levels of connectivity within the network, occupy different positions in terms of network centrality, or participate in different community structures.

Network features provide signals that are orthogonal to traditional transaction features, meaning they capture different aspects of the fraud problem. A customer may have transaction-level characteristics that appear normal, for instance average purchase amounts, reasonable shipping addresses, and accepted payment methods. However, their position in the customer-product network may reveal anomalous patterns such as unusually high degree centrality indicating purchases of many different product types, low clustering coefficient suggesting purchasing behavior that does not align with any normal customer segment, or membership in a network community dominated by known fraudulent customers. These network-level signals complement transaction features to provide a more complete picture of fraud risk.

The sparse nature of the customer-product network in the DataCo dataset, with a density of only 0.000469, actually enhances the value of network features for fraud detection. In sparse networks, each connection carries more information because it represents a deliberate choice rather than a random or inevitable connection. When a customer purchases a product in a sparse network, this purchase decision reveals more about the customer's behavior and intentions compared to dense networks where customers purchase most available products. This information-rich sparsity makes network features particularly valuable for distinguishing fraudulent from legitimate behavior patterns.

Network-based approaches also align with theoretical insights from supply chain management about information pooling and risk reduction. By analyzing the network as a whole rather than examining transactions in isolation, the detection system pools information across multiple customers and products. This pooling reduces the uncertainty associated with individual transactions by placing them in the broader context of network patterns. Similar to how risk pooling in inventory management reduces overall demand variability, information pooling in fraud detection reduces the uncertainty about transaction authenticity by leveraging patterns across the entire network.

The integration of network features with transaction features through machine learning models enables the development of more accurate and robust fraud detection systems. Deep learning architectures can learn complex non-linear relationships between network position, transaction characteristics, and fraud probability. Unlike traditional rule-based systems, deep learning models automatically discover relevant patterns in the data without requiring manual feature engineering or rule specification. This automatic pattern discovery allows the system to adapt to evolving fraud tactics and identify novel fraud schemes that have not been previously observed.

**1.3. Research Objectives**

**1.3.1. Primary Objective**

The primary objective of this research is to develop an effective fraud detection system for supply chain transactions that achieves a recall rate of at least 70 percent, thereby reducing fraud risk by at least 70 percent compared to having no detection system. The 70 percent recall target represents an industry-standard performance threshold for fraud detection systems, balancing the need to catch most fraudulent transactions against the operational costs of investigating false positives.

Recall, also known as sensitivity or true positive rate, measures the proportion of actual fraudulent transactions that are correctly identified by the detection system. Mathematically, recall equals true positives divided by the sum of true positives and false negatives. A recall of 70 percent means that the system successfully detects 70 percent of all fraudulent transactions that occur, while 30 percent of frauds remain undetected. This performance level represents a substantial improvement over both unprotected operations and traditional fraud detection methods.

The focus on recall as the primary performance metric reflects the cost asymmetry inherent in fraud detection problems. In supply chain contexts, the cost of missing a fraudulent transaction typically far exceeds the cost of investigating a false alarm. A missed fraud results in complete loss of the shipped product value plus associated handling costs, while a false positive investigation incurs only marginal administrative costs. This cost structure justifies prioritizing recall over precision, accepting higher false positive rates in exchange for catching more actual fraud cases.

Achieving the 70 percent recall target requires addressing the key limitations of traditional methods through integration of network features, advanced machine learning architectures, and cost-sensitive learning approaches. The detection system must be able to identify subtle fraud patterns that evade rule-based detection, adapt to evolving fraud tactics, and optimize for the specific cost structure of supply chain fraud.

**1.3.2. Secondary Objectives**

Beyond the primary performance target, this research pursues several secondary objectives that contribute to a comprehensive understanding of fraud detection in supply chain contexts and demonstrate the value of network-based approaches.

The first secondary objective is to construct a bipartite customer-product network from the DataCo supply chain data and extract meaningful network-based fraud indicators. This involves transforming transactional data into a graph representation where customers and products become nodes and transactions become edges. From this network structure, the research computes various centrality measures including degree centrality, betweenness centrality, closeness centrality, and PageRank scores for each customer node. These network features capture different aspects of customer position and behavior within the supply chain network. The objective includes validating that these network features contain genuine fraud signals by demonstrating statistical differences in network characteristics between fraudulent and legitimate customers.

The second secondary objective is to systematically compare the fraud detection performance of three different feature sets: transaction-based features only, network-based features only, and combined features integrating both transaction and network information. This comparative analysis provides empirical evidence about the incremental value of network features beyond traditional transaction features. By training and evaluating models on each feature set independently and then on the combined feature set, the research quantifies how much network information improves detection accuracy. This comparison addresses the fundamental question of whether the additional complexity of network feature engineering is justified by improved performance.

The third secondary objective is to design and implement a cost-sensitive machine learning model that explicitly prioritizes recall over precision in accordance with the economic realities of supply chain fraud. Traditional machine learning models optimize for overall accuracy or balanced metrics like F1-score, which treat false positives and false negatives as equally costly. However, in fraud detection, false negatives are typically much more expensive than false positives. The research develops a custom cost-sensitive focal loss function that incorporates explicit false negative penalties, causing the model to prioritize catching fraudulent transactions even if this increases false positive rates. This objective includes determining the optimal false negative cost multiplier and classification threshold through systematic experimentation.

The fourth secondary objective is to analyze the supply chain risk management implications of effective fraud detection, including its impact on the bullwhip effect, inventory planning, and supply chain coordination. This analysis connects the technical fraud detection results back to fundamental supply chain management concepts taught in the course. It quantifies how reducing fraud-related information distortion by 74.83 percent through effective detection affects demand forecast accuracy, inventory holding costs, and coordination among supply chain partners. The objective includes developing a framework for understanding fraud detection as a risk reduction strategy within the broader context of operational hedging approaches.

The fifth secondary objective is to conduct a comprehensive business value analysis demonstrating the return on investment from implementing network-based fraud detection. This includes developing a cost-benefit model that accounts for fraud losses avoided, investigation costs incurred, and net financial benefit achieved. The analysis compares the economic performance of different detection approaches including single model baseline, ensemble model, and stacking ensemble to identify the configuration that maximizes business value. This objective ensures that the research provides actionable insights for supply chain practitioners beyond academic contributions.

**1.4. Research Questions**

Building on the objectives outlined above, this research addresses four specific research questions that guide the investigation and structure the analysis.

Research Question 1 asks whether network-based features can improve fraud detection performance beyond what is achievable using transaction-only features. This question directly addresses the core hypothesis motivating the network-based approach. If network features provide no incremental value beyond traditional transaction features, then the additional complexity of network construction and feature extraction would not be justified. The research answers this question through controlled experiments comparing model performance across different feature sets while holding all other factors constant, including model architecture, training procedure, and evaluation metrics.

Research Question 2 asks what specific network patterns distinguish fraudulent customers from legitimate customers in the supply chain context. This question moves beyond simply demonstrating that network features are valuable to understanding what specific network characteristics are associated with fraud. The research investigates whether fraudulent customers have higher or lower degree centrality, whether they occupy different positions in terms of betweenness and closeness centrality, whether they have different PageRank scores, and whether they cluster into distinct communities within the network. Understanding these patterns provides insights into the behavioral mechanisms underlying supply chain fraud and suggests potential manual investigation strategies.

Research Question 3 asks how fraud detection reduces supply chain operational risks and specifically how it mitigates information distortion and the bullwhip effect. This question connects the fraud detection results to supply chain coordination theory taught in Chapter 7 of the course. It examines whether reducing fraud from 2.25 percent of transactions to the miss rate achieved by the detection system meaningfully improves demand forecast accuracy, reduces inventory variability, and enhances coordination among supply chain partners. The analysis considers both direct effects, such as removing fraudulent orders from demand histories, and indirect effects, such as improved trust enabling better coordination mechanisms.

Research Question 4 asks what the business value and return on investment of implementing network-based fraud detection is in supply chain operations. This question ensures the research addresses practical deployment considerations beyond academic performance metrics. It requires developing a comprehensive cost model that accounts for all relevant costs and benefits, including fraud losses avoided, investigation costs, implementation and maintenance costs, and broader supply chain performance improvements. The analysis also considers sensitivity to key assumptions such as average fraud transaction value and investigation cost per alert to ensure the conclusions are robust across realistic parameter ranges.

**1.5. Scope and Limitations**

**1.5.1. Data Scope**

The research is based exclusively on the DataCo Supply Chain dataset containing 180,519 transactions from 20,652 customers purchasing 118 products. The dataset spans multiple years of transaction history, though the exact time period is not specified in the available documentation. The geographic scope includes multiple countries and regions, and the product scope covers various product categories typical of e-commerce supply chains.

The fraud label used in this research is based on the order status field where transactions marked as suspected fraud constitute the positive class. This label reflects ex-post identification of fraudulent transactions through existing detection mechanisms or subsequent investigation. The research does not have access to the specific criteria or processes used to assign the suspected fraud label in the original dataset. It is assumed that this label represents reasonably accurate ground truth, though some degree of labeling error is inevitable in real-world fraud datasets.

The network construction is limited to the bipartite customer-product structure directly supported by the transactional data. The research does not incorporate additional network layers such as customer-customer networks based on shared characteristics, product-product networks based on co-purchasing patterns, or supplier networks due to lack of data. The network is also treated as static rather than temporal, meaning the analysis does not explicitly model how network structure evolves over time, though transaction dates are included as features.

**1.5.2. Methodological Scope**

The machine learning approach employed in this research is based on deep neural networks with fully connected layers. The research does not explore alternative architectures such as graph neural networks, which could potentially leverage network structure more directly, or recurrent neural networks, which could better model temporal patterns. The choice of deep neural networks reflects a balance between performance and practical implementability, as these architectures are well-understood and readily deployable in production environments.

The network features extracted from the bipartite graph include degree centrality, betweenness centrality, closeness centrality, and PageRank. The research does not investigate other potentially relevant network measures such as eigenvector centrality, clustering coefficient, or k-core decomposition. Additionally, community detection is performed but the resulting community assignments are not used as features in the final model. The selection of network features is based on prior literature and computational feasibility considerations.

The model evaluation is performed using a hold-out test set representing 20 percent of the total dataset. The research does not employ cross-validation due to the substantial computational cost of training deep neural networks and the large dataset size. The train-test split is performed once at the beginning of the analysis and held constant across all experiments to ensure fair comparison between different model configurations.

**1.5.3. Limitations**

Several limitations should be acknowledged when interpreting the research findings. First, the results are based on a single dataset from one supply chain context. While the DataCo dataset is substantial and realistic, generalization to other supply chain environments, industries, or geographic regions requires caution. Different supply chains may exhibit different fraud patterns, network structures, and cost trade-offs that would affect optimal detection strategies.

Second, the research treats fraud detection as a binary classification problem with a single fraud label. In practice, fraud encompasses various types including payment fraud, identity theft, friendly fraud, and return fraud. These different fraud types may have distinct characteristics and require different detection approaches. The aggregated fraud label used in this research may mask important heterogeneity in fraud mechanisms.

Third, the cost-benefit analysis relies on assumed values for key parameters such as average fraud transaction value and investigation cost per alert. While these assumptions are based on reasonable estimates, actual values vary across organizations and contexts. The sensitivity of conclusions to these assumptions is discussed but not exhaustively explored. Organizations considering deployment would need to calibrate the cost model to their specific circumstances.

Fourth, the research evaluates model performance at a single point in time using historical data. It does not address how model performance might degrade over time as fraud tactics evolve, how frequently the model would need to be retrained, or what ongoing maintenance requirements would be necessary for production deployment. These temporal considerations are important for practical implementation but beyond the scope of the current research.

Fifth, the network-based approach requires aggregating transaction data to construct the customer-product network and compute centrality measures. This aggregation process may introduce temporal biases where recent transactions have different impacts on network features compared to older transactions. The research does not explicitly model these temporal dynamics or investigate whether time-weighted network construction would improve performance.

**1.6. Significance of the Study**

**1.6.1. Theoretical Contributions**

This research makes several important theoretical contributions to the intersection of supply chain management and fraud detection literature. First, it provides one of the first systematic applications of social network analysis techniques to supply chain fraud detection, demonstrating how network features can complement transaction-based approaches. While network analysis has been applied extensively in other fraud detection domains such as financial fraud and telecommunications fraud, its application to supply chain contexts remains limited. This research bridges that gap by showing how bipartite customer-product networks capture fraud-relevant patterns.

Second, the research explicitly connects fraud detection to fundamental supply chain management concepts taught in the course, particularly risk hedging strategies and supply chain coordination theory. By framing fraud detection as a risk reduction mechanism within the operational hedging framework, the research clarifies how fraud management fits into broader supply chain strategy. Similarly, by analyzing how fraud contributes to information distortion and the bullwhip effect, the research extends coordination theory to explicitly account for adversarial actors within the supply chain.

Third, the development and validation of a cost-sensitive focal loss function for imbalanced fraud detection represents a methodological contribution. While focal loss has been applied to various imbalanced classification problems, its integration with explicit false negative cost penalties tailored to fraud detection cost structures has not been extensively explored. The research demonstrates that this hybrid loss function outperforms standard approaches for highly imbalanced fraud detection scenarios.

Fourth, the systematic comparison of transaction-only, network-only, and combined feature approaches provides empirical evidence about the incremental value of network features. This comparison addresses a key question in the literature about whether the computational and engineering overhead of network feature extraction is justified by performance improvements. The results showing that combined features substantially outperform either feature set alone provide guidance for future research and practice.

**1.6.2. Practical Contributions**

The practical contributions of this research are equally significant for supply chain practitioners and organizations seeking to improve fraud detection capabilities. First, the research demonstrates that achieving industry-standard fraud detection performance of 70 percent recall is feasible using machine learning approaches integrated with network analysis. The specific model architecture, training procedure, and feature engineering approaches documented in the research provide a blueprint that practitioners can adapt to their own supply chain contexts.

Second, the comprehensive business value analysis quantifies the return on investment from implementing network-based fraud detection. By showing that the ensemble model generates a positive net benefit of 88,900 dollars on the test set while baseline approaches result in net losses, the research provides compelling justification for the investment required to develop and deploy these systems. The cost-benefit framework developed in the research can be adapted by practitioners to evaluate fraud detection investments in their specific contexts.

Third, the research provides insights into the network characteristics of fraudulent customers that can inform manual investigation strategies. Understanding that fraudulent customers tend to have 57 percent higher degree centrality than legitimate customers suggests that customers purchasing unusually diverse product portfolios should receive additional scrutiny. These insights complement automated detection by helping human investigators prioritize cases and recognize patterns.

Fourth, the research demonstrates the importance of cost-sensitive optimization and threshold tuning for fraud detection systems. The finding that the optimal threshold of 0.20 differs substantially from the default 0.50 threshold highlights that practitioners cannot rely on default settings but must actively optimize detection systems for their specific cost structures and business objectives. The research provides guidance on how to conduct this optimization systematically.

Fifth, by framing fraud detection within the broader context of supply chain risk management and coordination, the research encourages practitioners to think about fraud holistically rather than as an isolated security problem. Understanding how fraud contributes to the bullwhip effect and disrupts coordination suggests that fraud detection should be integrated with demand forecasting, inventory planning, and supplier relationship management rather than treated as a standalone function. This integrated perspective can lead to better overall supply chain performance.

**1.7. Report Structure**

The remainder of this report is organized into five chapters that systematically address the research objectives and questions outlined above.

Chapter 2 presents the theoretical framework underlying the research, reviewing relevant literature and concepts from supply chain management and fraud detection. The chapter begins with a discussion of supply chain risk management theory from Chapter 5 of the course, focusing on the four operational hedging strategies and positioning fraud detection within the risk reduction framework. It then examines supply chain coordination theory from Chapter 7, discussing how fraud contributes to information distortion and the bullwhip effect. The chapter also reviews risk sharing mechanisms from Chapter 3 and their relevance to fraud cost allocation. Finally, the chapter introduces social network analysis concepts and techniques relevant to fraud detection, including graph representation, centrality measures, and community detection algorithms.

Chapter 3 describes the research methodology in detail, beginning with a comprehensive description of the DataCo Supply Chain dataset including its structure, variables, and preprocessing steps. The chapter then explains the construction of the bipartite customer-product network and the extraction of network features. It describes the feature engineering process for transaction-based features and the integration of transaction and network features. The chapter presents the deep neural network architecture, including layer specifications, activation functions, and regularization techniques. It explains the cost-sensitive focal loss function and its parameters. The chapter also describes the ensemble strategy, including the number of models, random seeds, and prediction aggregation method. Finally, it presents the evaluation methodology, including the train-test split, performance metrics, and cost-benefit analysis framework.

Chapter 4 presents the results of the network analysis and model training experiments. It begins by analyzing the characteristics of the customer-product network, including degree distributions, centrality measures, and community structure. It then compares network characteristics between fraudulent and legitimate customers, demonstrating that significant differences exist. The chapter presents the performance of different model configurations, including single models, ensemble models, and stacking ensembles across different feature sets. It includes confusion matrices, ROC curves, and detailed performance metrics for each configuration. The chapter concludes with a feature importance analysis showing which transaction and network features contribute most to fraud detection.

Chapter 5 discusses the implications of the results for supply chain management practice and theory. It begins by analyzing how the fraud detection system reduces operational risk within the risk hedging framework, calculating the effective risk reduction achieved and comparing it to alternative hedging strategies. It then examines the impact on the bullwhip effect, quantifying how removing fraudulent transactions from demand signals affects forecast accuracy and inventory variability. The chapter discusses how effective fraud detection enables better supply chain coordination by improving information quality and building trust among partners. It presents the comprehensive business value analysis, including detailed cost-benefit calculations and sensitivity analysis. The chapter concludes with strategic recommendations for implementing fraud detection systems in supply chain contexts.

Chapter 6 provides the overall conclusion, summarizing the key findings and their implications. It revisits the research questions and explains how the results address each question. It discusses the contributions of the research to both theory and practice. It acknowledges the limitations of the study and suggests directions for future research that could extend or refine the findings. The chapter concludes with final thoughts on the role of fraud detection in modern supply chain risk management.

**CHAPTER 2: THEORETICAL FRAMEWORK**

**2.1. Supply Chain Risk Management Theory**

**2.1.1. Risk Classification: Disruption versus Operational Risks**

Supply chain risk management provides the foundational theoretical lens through which fraud detection can be understood as a systematic risk mitigation strategy. The supply chain management literature distinguishes between two fundamental categories of risks that organizations face in their operations. These categories differ fundamentally in their frequency, impact magnitude, and appropriate management responses.

Disruption risks represent high-impact but low-probability events that can severely compromise supply chain operations when they occur. Examples of disruption risks include natural disasters such as earthquakes or hurricanes, geopolitical conflicts that disrupt trade routes, major supplier bankruptcies, or pandemic events that shut down global logistics networks. These risks are characterized by their potential to cause catastrophic damage to supply chain performance, but their relative rarity means that organizations may operate for extended periods without experiencing such disruptions. The management of disruption risks typically focuses on contingency planning, redundancy in critical supply chain nodes, and rapid response capabilities to minimize damage when disruptions occur.

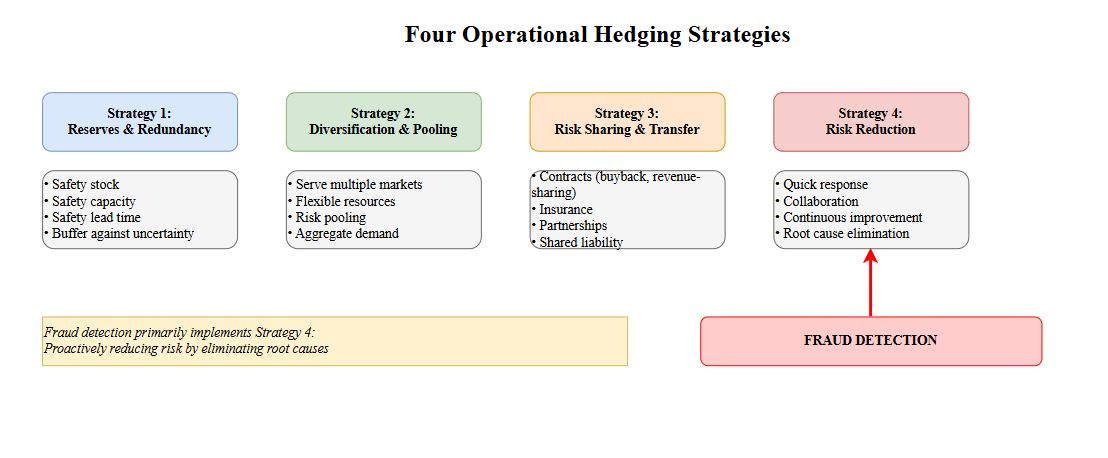
In contrast, operational risks stem from the routine activities and resources within supply chain operations themselves. These risks are lower in individual impact but occur with much higher frequency. Operational risks include demand variability that leads to stockouts or excess inventory, quality defects in manufactured products, transportation delays, supplier performance issues, and information inaccuracies. The management of operational risks focuses on continuous improvement, process optimization, and systematic monitoring to detect and correct problems before they accumulate into larger disruptions.

Fraud occupies a unique and particularly challenging position within this risk taxonomy. At the transaction level, individual fraudulent orders appear as operational risks with relatively modest impact. A single fraudulent transaction may result in losses of hundreds or thousands of dollars, which is significant but not catastrophic for most organizations. The frequency of fraud in the DataCo supply chain, at 2.25 percent of transactions, clearly places it in the operational risk category based on probability. However, the systematic and cumulative nature of fraud can cause it to escalate from an operational risk into a disruption-level threat. When fraud rates are high or go undetected for extended periods, the accumulated financial losses, inventory depletion, and information distortion can severely compromise supply chain operations.

This dual nature of fraud as both an operational risk in individual instances and a potential disruption risk in aggregate form makes it particularly important to address through systematic detection and prevention mechanisms. Unlike natural disasters or geopolitical events that are largely outside organizational control, fraud is generated by actors within or interacting with the supply chain itself. This means that proactive risk reduction strategies, as opposed to merely reactive contingency planning, can be highly effective in managing fraud risk.

**2.1.2. Four Operational Hedging Strategies**

The supply chain risk management literature identifies four generic operational hedging strategies that organizations can employ to mitigate various forms of risk. Understanding these strategies provides context for positioning fraud detection within the broader toolkit of risk management approaches. Figure 2.1 illustrates the four strategies and their key characteristics.



**Figure 2.1: Four Operational Hedging Strategies in Supply Chain Risk Management**

The first strategy, reserves and redundancy, involves investing in assets held over expected requirements as buffers against uncertainty. This strategy is well-established in operations management through concepts such as safety stock, safety capacity, and safety lead time. Organizations maintain inventory reserves to protect against demand uncertainty and supply disruptions. They maintain capacity reserves to handle demand spikes without compromising service levels. They build time buffers into production and delivery schedules to absorb unexpected delays. While reserves and redundancy are effective at absorbing the impact of various risks, they come with substantial carrying costs and reduce operational efficiency. In the context of fraud, maintaining financial reserves to absorb fraud losses would be an application of this strategy, but it does not address the root cause of the problem and merely accepts fraud as an inevitable cost of doing business.

The second strategy, diversification and pooling, involves serving multiple markets with flexible resources or aggregating demand across multiple sources to reduce overall variability. Pure diversification spreads risk across uncorrelated or negatively correlated markets, reducing the probability that all markets experience problems simultaneously. Risk pooling leverages statistical properties where aggregated demand has lower coefficient of variation than individual demand streams. Organizations implement this strategy through flexible manufacturing systems that can serve multiple markets, centralized distribution centers that pool inventory across regions, or supplier portfolios that reduce dependence on any single source. For fraud management, diversification might involve serving multiple customer segments with different fraud profiles, while pooling might involve analyzing patterns across the entire customer base rather than treating each transaction in isolation.

The third strategy, risk sharing and transfer, recognizes that organizations do not need to bear all risks themselves but can share them with partners or transfer them to third parties. Contract structures such as buyback contracts and revenue-sharing agreements allocate risk between suppliers and buyers in ways that can improve supply chain coordination while reducing risk exposure for individual parties. Insurance contracts represent explicit risk transfer where an organization pays premiums to transfer certain risks to insurers. In fraud management, risk sharing mechanisms might include chargeback arrangements with payment processors, fraud insurance policies, or contractual provisions that allocate fraud liability among supply chain partners.

The fourth strategy, reducing or eliminating root causes of risk, emphasizes proactive approaches that address the fundamental sources of uncertainty and variability. This strategy includes quick response capabilities that reduce the time between information gathering and decision making, thereby decreasing exposure to forecast errors. It includes supply chain collaboration mechanisms such as vendor-managed inventory and collaborative planning that improve information quality and alignment of incentives. It includes continuous improvement methodologies that systematically identify and eliminate sources of process variability and error. Among the four strategies, root cause reduction offers the most fundamental solution because it prevents problems from occurring rather than merely mitigating their consequences.

**2.1.3. Fraud as Risk Reduction Strategy**

Fraud detection represents a clear application of the fourth operational hedging strategy focused on reducing or eliminating root causes of risk. Rather than accepting fraud as an inevitable cost and maintaining financial reserves to absorb losses, or attempting to diversify away fraud risk, or purchasing insurance to transfer fraud risk, the fraud detection approach proactively identifies and prevents fraudulent transactions before they impact operations. This positions fraud detection as a risk reduction mechanism that addresses the problem at its source.

The risk reduction perspective on fraud detection has several important implications. First, it emphasizes the need for continuous improvement in detection capabilities as fraud tactics evolve. Just as continuous improvement in manufacturing processes requires ongoing attention to quality metrics and root cause analysis, effective fraud detection requires continuous monitoring of fraud patterns and adaptation of detection algorithms. The static rule-based approaches that dominated early fraud detection systems are inconsistent with the continuous improvement philosophy because they only respond to known fraud patterns rather than anticipating new ones.

Second, the risk reduction framework highlights the importance of quick response capabilities. The time between when a fraudulent transaction occurs and when it is detected and stopped directly determines the magnitude of loss. Fraud detection systems that operate in real-time or near-real-time at the point of transaction can prevent shipment of goods to fraudulent customers, eliminating both the direct product loss and the indirect costs of information distortion. Post-transaction fraud detection, while still valuable for understanding fraud patterns and preventing future occurrences, cannot prevent the initial loss.

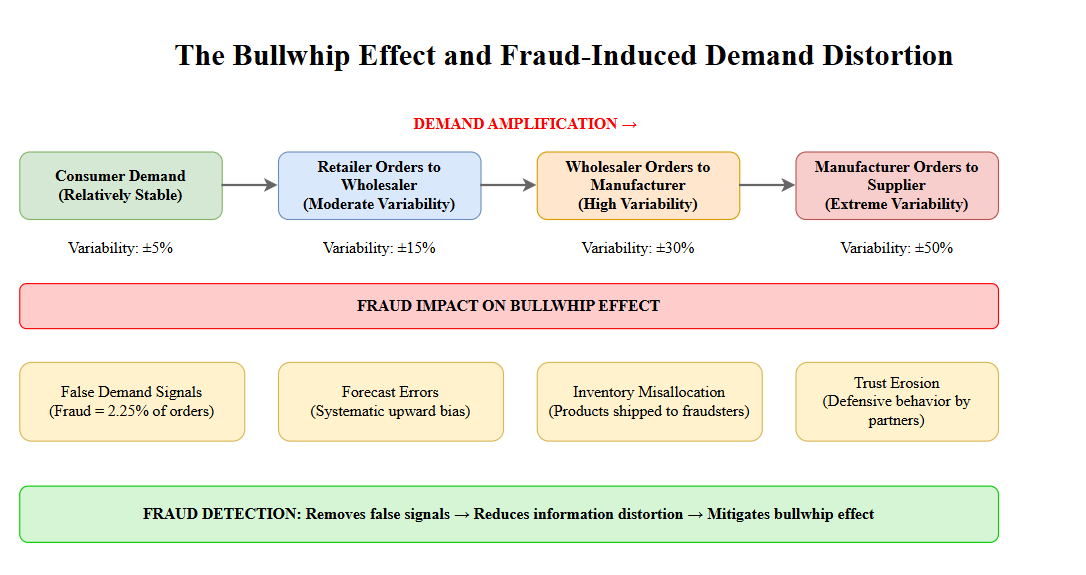
Third, positioning fraud detection as risk reduction emphasizes its role as an integral component of operations strategy rather than a peripheral security function. Risk reduction through continuous improvement and quick response is not a separate activity conducted by specialized security departments but rather a core operational capability that must be embedded in routine supply chain processes. This integration perspective suggests that fraud detection systems should be directly connected to demand forecasting, inventory planning, order fulfillment, and customer relationship management systems rather than operating in isolation.

The effectiveness of fraud detection as a risk reduction strategy can be quantified by comparing the risk exposure with and without detection capabilities. In the baseline scenario without fraud detection, the organization faces the full 2.25 percent fraud rate in the DataCo supply chain, resulting in losses on all 4,062 fraudulent transactions. With a detection system achieving 74.83 percent recall, the risk exposure is reduced by three-quarters, with only 25.17 percent of fraudulent transactions going undetected. This substantial risk reduction demonstrates the value of proactive detection compared to passive acceptance of fraud losses.

**2.2. Supply Chain Coordination and Information Distortion**

**2.2.1. The Bullwhip Effect**

Supply chain coordination theory provides crucial insights into why fraud is not merely a direct financial loss problem but rather a systemic issue that affects the entire supply chain network. The bullwhip effect, one of the most well-documented phenomena in supply chain management, describes how small fluctuations in consumer demand become progressively amplified as orders move upstream through the supply chain from retailers to wholesalers to manufacturers to raw material suppliers. Figure 2.2 illustrates this amplification mechanism and its relationship to fraud.

**Figure 2.2: The Bullwhip Effect and Fraud-Induced Demand Distortion**

As shown in Figure 2.2, consumer demand at the retail level exhibits relatively stable patterns with modest variability. However, when retailers place orders with wholesalers, they add safety margins to account for uncertainty, batch their orders for economic efficiency, and react to promotions and price fluctuations. These behaviors cause retail orders to wholesalers to exhibit higher variability than actual consumer demand. Wholesalers, observing variable orders from retailers, similarly add their own safety margins and batching behaviors when ordering from manufacturers. Manufacturers, seeing even more variable orders, amplify the variability further when placing orders with suppliers. The result is that demand variability increases exponentially as information moves upstream, even though underlying consumer demand remains relatively stable.

The bullwhip effect creates numerous operational problems throughout the supply chain. Manufacturers experience extreme swings between excess capacity during low-demand periods and insufficient capacity during high-demand periods, leading to inefficient resource utilization. Inventory costs increase at all levels as organizations hold larger safety stocks to buffer against perceived demand uncertainty. Transportation and logistics costs rise due to rush shipments during perceived shortages and excess capacity during slack periods. Product availability and customer service levels decline as the system struggles to match supply with demand. Overall supply chain costs increase substantially while performance deteriorates.

The fundamental causes of the bullwhip effect relate to information quality and coordination failures. When each stage of the supply chain makes decisions based on orders received from the immediately downstream stage rather than on actual consumer demand, information becomes progressively distorted. This distortion is exacerbated by several mechanisms including demand signal processing where each stage applies its own forecasting models and safety factors, order batching for economic efficiency, price fluctuations that cause forward buying, and rationing game playing when shortages are anticipated.

**2.2.2. Causes of Information Distortion**

Understanding the specific causes of information distortion in supply chains provides context for recognizing how fraud contributes to these problems. The supply chain management literature identifies several categories of obstacles to coordination that lead to information distortion.

Incentive obstacles arise when different stages of the supply chain have conflicting objectives that lead to locally optimal but globally suboptimal decisions. For example, sales personnel may be incentivized based on revenue targets, leading them to offer promotional discounts that cause demand spikes followed by sharp declines. Manufacturing may be incentivized based on production efficiency, leading to large batch sizes that increase inventory holding costs downstream. Logistics providers may be incentivized based on vehicle utilization, leading to infrequent but full shipments rather than frequent small shipments that better match demand patterns. These misaligned incentives cause each stage to take actions that make sense from their local perspective but degrade overall supply chain performance.

Information processing obstacles occur when demand information becomes delayed or distorted as it moves through the supply chain. Time delays between when consumer demand occurs and when upstream stages observe and respond to it create lags that exacerbate variability. Demand signal processing where each stage applies forecasting models to order data rather than consumer demand data progressively distorts the underlying signal. Lack of transparency where upstream stages cannot observe actual consumer demand patterns forces them to rely on noisy order data. These information processing issues prevent supply chain partners from making decisions based on accurate demand information.

Operational obstacles stem from the mechanics of how supply chains operate. Order batching where organizations consolidate small orders into larger batches for efficiency creates artificial demand spikes at regular intervals. Minimum order quantities and full truckload requirements force customers to order more than immediate needs, distorting demand signals. Transportation mode choices and schedules create fixed ordering cycles that may not align with actual demand patterns. These operational practices, while often economically rational from a local cost perspective, inject additional variability into demand signals.

Pricing obstacles arise from price fluctuations and promotional activities. Forward buying occurs when customers observe temporary price reductions and purchase more than they need to take advantage of the lower prices. After promotions end, customers stop purchasing until they deplete the excess inventory, creating a demand trough. Rationing and shortage gaming occurs when customers anticipate shortages and inflate their orders to ensure they receive adequate allocations, knowing that suppliers may ration available supply during shortages. These pricing-related behaviors cause demand patterns that bear little resemblance to actual consumption.

Behavioral obstacles reflect human cognitive limitations and organizational learning challenges. Different stages of the supply chain view their actions locally and cannot see the system-wide impact of their decisions. When problems arise, organizations react to current local situations rather than conducting root cause analysis to understand underlying issues. Different stages blame one another for problems rather than recognizing the systemic nature of coordination failures. Organizations fail to learn from experience over time, repeating the same coordination mistakes. Lack of trust among supply chain partners causes opportunistic behavior at the expense of overall supply chain performance.

**2.2.3. Fraud's Contribution to Coordination Failure**

Fraud represents a particularly pernicious form of information distortion that touches on multiple categories of coordination obstacles. Understanding how fraud contributes to coordination failure reveals why fraud detection is not just a security measure but a fundamental requirement for effective supply chain coordination.

From an information processing perspective, fraudulent transactions inject completely false signals into demand data. While other sources of information distortion such as batching or forward buying represent transformations of legitimate demand, fraud represents demand that never existed. When a fraudster places an order with no intention of payment, the resulting order appears in demand history and forecasting systems as a legitimate customer need. Forecasting models trained on historical data that includes fraudulent transactions learn patterns that incorporate this false demand, systematically biasing forecasts upward. The magnitude of this bias depends on the fraud rate and the extent to which fraudulent transactions differ from legitimate ones in timing, product selection, or order size.

In the DataCo supply chain with a 2.25 percent fraud rate, all else being equal, demand forecasts would be systematically biased upward by approximately 2.25 percent if fraudulent transactions are not identified and removed from historical data. This might seem modest, but in supply chains operating on thin margins with carefully optimized inventory levels, even small forecast biases can cause substantial costs. More problematically, if fraudulent transactions exhibit seasonal patterns or concentrate in particular product categories, the forecast bias will be non-uniform, causing some products to be severely overstocked while others remain appropriately stocked.

From a behavioral obstacle perspective, fraud undermines trust among supply chain partners, which is essential for coordination mechanisms such as vendor-managed inventory and collaborative planning. When suppliers observe high return rates, payment defaults, or suspicious ordering patterns, they become more conservative in their credit policies and less willing to share information or invest in relationship-specific assets. Retailers facing frequent fraud may implement stricter authentication requirements that slow down the ordering process and reduce convenience for legitimate customers. The erosion of trust caused by fraud propagates through the supply chain network, reducing the effectiveness of coordination mechanisms that depend on transparent information sharing and mutual confidence.

From an operational obstacle perspective, fraud creates additional variability that exacerbates order batching and cycle stock problems. When fraud detection systems flag suspicious orders for manual review, legitimate orders may be delayed while investigations occur. When fraud is discovered after shipment, the resulting returns and restocking create reverse logistics flows that disrupt normal operations. When customers' accounts are blocked due to fraud concerns, legitimate reorders may be prevented, creating artificial stockouts. These operational disruptions add variability to supply chain processes beyond what would occur with legitimate demand alone.

From a cost perspective, fraud increases the total cost of supply chain operations in ways that extend far beyond the direct value of stolen goods. Investigation costs, chargeback fees, return logistics costs, and restocking costs accumulate even when fraud is eventually detected. The preventive measures that organizations implement to reduce fraud risk, such as enhanced authentication, delayed shipments pending verification, and restrictive credit policies, add transaction costs to all orders including legitimate ones. The need to maintain higher safety stocks to buffer against the additional variability caused by fraud increases inventory carrying costs throughout the supply chain.

**2.3. Risk Sharing Mechanisms in Supply Chains**

**2.3.1. Contract Theory and Total Cost Perspective**

Supply chain contract theory provides insights into how risks and costs are allocated among supply chain partners and how contract structures can influence behavior and performance. The fundamental principle underlying contract design in supply chains is that supplier and buyer decisions should be evaluated based on their impact on total supply chain cost and profit, not just on individual party outcomes. This total cost perspective recognizes that locally optimal decisions for individual parties may lead to globally suboptimal outcomes for the supply chain as a whole.

The total cost of ownership concept extends beyond simple purchase prices to include all costs associated with acquiring and using products or services. For purchased materials, total cost includes not just the unit price paid to suppliers but also quality-related costs such as inspection, rework, and warranty claims, delivery-related costs such as transportation and expediting, inventory-related costs such as holding costs for safety stock and cycle stock, and transaction costs such as ordering, receiving, and payment processing. Supplier performance should be evaluated based on impact on this total cost rather than just on quoted prices.

In the context of fraud, the total cost perspective is essential for understanding the true economic impact and for designing appropriate detection and prevention strategies. The direct cost of fraud, equal to the value of goods shipped to fraudulent customers without payment, represents only the most visible component of total fraud cost. Indirect costs include investigation and administrative costs for each suspected fraud case, chargeback fees assessed by payment processors, costs of goods returned through reverse logistics, restocking and potential disposal costs for returned items, customer service costs for handling fraud-related inquiries, and opportunity costs from lost sales to legitimate customers who could have purchased the diverted products.

Beyond these tangible costs, fraud generates intangible costs that affect supply chain coordination. Information distortion caused by fraudulent transactions degrades forecast accuracy, leading to suboptimal inventory and production decisions. Trust erosion among supply chain partners increases transaction costs and reduces willingness to engage in collaborative planning. Reputation damage from publicized fraud incidents affects customer confidence and willingness to engage in transactions. The cumulative impact of these tangible and intangible costs can easily exceed the direct loss value by substantial multiples.

**2.3.2. Fraud Detection as Risk Sharing Mechanism**

Fraud detection can be understood as a mechanism for allocating fraud risk among supply chain partners in ways that improve incentives and overall performance. In the absence of formal fraud detection and clear liability assignment, fraud risk tends to fall on whichever party is least protected by contract terms or payment mechanisms. This often results in inefficient risk bearing where parties that have little ability to prevent fraud end up bearing most of its costs, while parties that could most effectively detect or prevent fraud have insufficient incentive to invest in prevention.

Consider the typical e-commerce supply chain where a retailer sells products sourced from suppliers to end consumers. When a fraudulent transaction occurs, several parties potentially bear costs. The supplier loses the wholesale value of goods shipped to the retailer if the retailer refuses to pay for unsold inventory. The retailer loses the goods shipped to the fraudulent customer if payment is not collected. Payment processors may bear chargeback costs if the fraud involves stolen payment credentials. Shipping carriers may bear liability for goods delivered to incorrect addresses. The allocation of these costs depends on specific contract terms, payment mechanisms, and legal frameworks.

From an efficiency perspective, fraud risk should be allocated to the parties best positioned to detect or prevent it, creating incentives for cost-effective risk mitigation. Retailers are well positioned to detect unusual ordering patterns at the transaction level through analysis of customer behavior, order characteristics, and payment information. Suppliers may be able to identify unusual aggregate demand patterns that suggest systematic fraud. Payment processors have visibility into payment method fraud indicators. Shipping carriers can identify suspicious delivery addresses or repeated delivery failures.

A fraud detection system that operates at the retail level and prevents fraudulent orders from being placed provides value to the entire supply chain by preventing costs from being incurred by any party. When fraud is detected before goods are shipped, the supplier avoids shipping costs and potential inventory write-offs, the retailer avoids investigation and restocking costs, the payment processor avoids chargeback processing, and the shipping carrier avoids misdirected shipments. This creates a clear incentive for the retailer to invest in fraud detection even if contract terms would theoretically allow passing some costs to other parties, because preventing fraud benefits all parties and facilitates better coordination.

The business value analysis conducted in this research quantifies these benefits by comparing total costs under different fraud detection scenarios. The finding that the ensemble model generates a positive net benefit of 88,900 dollars while baseline approaches result in net losses demonstrates that investing in effective fraud detection creates value that exceeds its costs. This positive return on investment justifies fraud detection as a risk reduction investment from a total cost perspective.

**2.4. Social Network Analysis Foundation**

**2.4.1. Bipartite Networks in Supply Chain Contexts**

Social network analysis provides the methodological foundation for incorporating relational information into fraud detection. While traditional fraud detection approaches analyze transactions in isolation, network-based approaches recognize that transactions create relationships between entities, and the patterns of these relationships contain valuable signals about fraud risk. Understanding the structure and properties of supply chain networks is essential for effective network-based fraud detection.

Supply chain transactions naturally form network structures where entities are connected through various types of relationships. The most fundamental network representation treats customers and products as nodes with transactions creating edges between them. This creates a bipartite network, also called a two-mode network, where nodes belong to two distinct sets and edges only connect nodes from different sets. In the customer-product bipartite network, customer nodes only connect to product nodes and vice versa, reflecting the fact that transactions occur between customers and products rather than between customers or between products directly.

Figure 2.3 illustrates the bipartite network structure in the DataCo supply chain and its key properties.

[INSERT FIGURE 2.3 HERE]

**Figure 2.3: Bipartite Network Structure of Customer-Product Relationships**

As shown in Figure 2.3, the DataCo supply chain forms a bipartite network with 20,652 customer nodes and 118 product nodes, connected by 101,196 edges representing unique customer-product pairs. Each edge corresponds to at least one transaction where the customer purchased the product. The network exhibits significant sparsity with a density of 0.000469, meaning that only 0.047 percent of possible customer-product connections actually exist. This sparsity is characteristic of real-world supply chain networks where customers purchase small subsets of available products rather than purchasing everything.

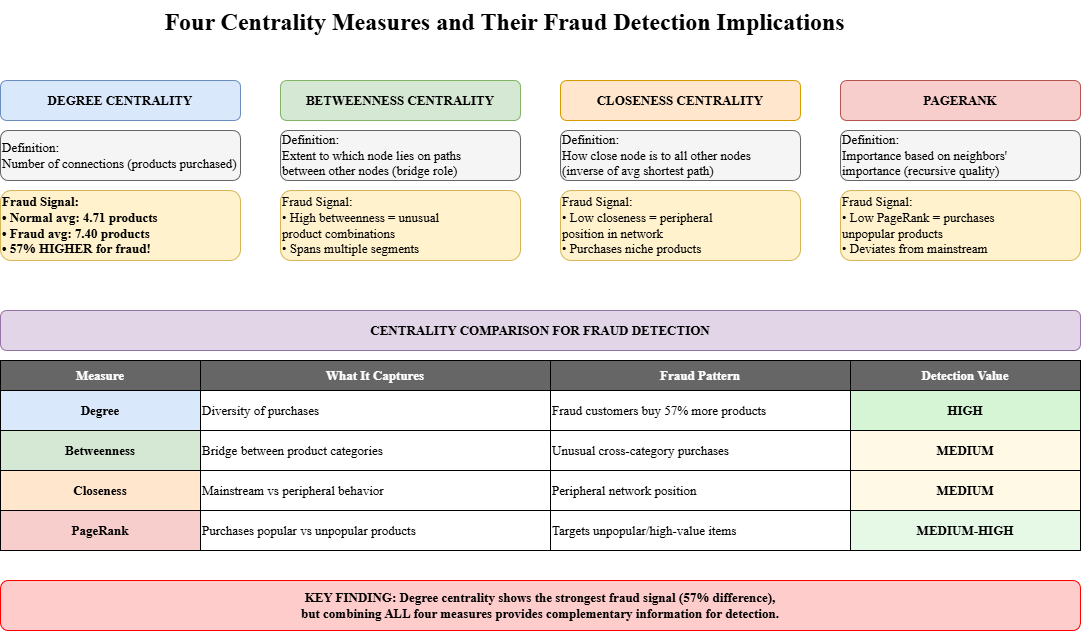
The bipartite structure preserves important information that would be lost in alternative network representations. One could construct a customer-to-customer projection network where two customers are connected if they purchase the same product, or a product-to-product projection network where two products are connected if they are purchased by the same customer. While these projections can reveal interesting patterns such as customer similarity or product complementarity, they discard the direct customer-product relationship information and create much denser networks that are more computationally expensive to analyze. The bipartite representation maintains the fundamental transaction structure while enabling analysis of both customer behavior and product popularity patterns.

The network structure reveals important organizational properties of the supply chain. The existence of 19 connected components rather than a single connected network indicates that not all customers and products are reachable from one another through transaction paths. The largest component containing 12,431 nodes represents the core of the network where the most popular products and most active customers interact. Smaller components represent peripheral market segments where specialized products are purchased by niche customer groups with little overlap with the mainstream market.

This component structure has implications for fraud detection because fraudulent and legitimate customers may occupy different positions in the network topology. If fraudulent customers tend to concentrate in smaller peripheral components or exhibit different connectivity patterns within the main component, network-based features can help distinguish them from legitimate customers. The research investigates whether such structural differences exist and whether they provide actionable fraud signals.

**2.4.2. Centrality Measures for Fraud Detection**

Centrality measures quantify the importance or prominence of individual nodes within a network structure based on different notions of what constitutes a central or important position. Different centrality measures capture different aspects of node importance, and understanding these distinctions is essential for selecting appropriate measures for fraud detection applications. Figure 2.4 illustrates four key centrality measures and their interpretations.



**Figure 2.4: Centrality Measures and Their Interpretation in Customer Networks**

Degree centrality represents the most straightforward measure of node importance, counting the number of connections that a node has. In the customer-product bipartite network, customer degree centrality equals the number of distinct products that the customer has purchased. High-degree customers are those who purchase many different products, indicating either genuine diverse interests or potentially fraudulent behavior where fraudsters order many items to maximize the value extracted before detection. Product degree centrality equals the number of distinct customers who have purchased the product, with high-degree products being the most popular items in the supply chain. Degree centrality is simple to compute and interpret, making it an attractive starting point for network analysis.

Betweenness centrality measures the extent to which a node lies on paths between other nodes in the network. A node has high betweenness if it appears on many shortest paths connecting other node pairs, positioning it as a bridge or broker in the network structure. In customer-product networks, high betweenness could indicate customers whose purchasing patterns span multiple product categories or customer segments, potentially connecting otherwise disconnected parts of the network. From a fraud detection perspective, high betweenness might indicate customers who purchase unusual product combinations that legitimate customers in any single segment would not typically purchase together.

Closeness centrality measures how close a node is to all other nodes in the network, typically defined as the inverse of the average shortest path length from the node to all other reachable nodes. Nodes with high closeness can quickly reach other nodes through short paths. In customer-product networks, closeness might indicate customers whose purchasing patterns are representative of mainstream behavior, purchasing products that are well-connected to the rest of the network. Unusually low closeness might indicate peripheral customers purchasing niche products with limited connections to the broader network, which could be a fraud signal if fraudsters target specific product categories.

PageRank extends the concept of centrality by incorporating the importance of neighboring nodes, not just the count of connections. Originally developed for web page ranking, PageRank assigns higher scores to nodes that are connected to other high-scoring nodes. In customer-product networks, a customer has high PageRank if they purchase products that are popular among many other customers, indicating mainstream purchasing behavior. Conversely, customers who purchase products with low popularity scores would have lower PageRank. This recursive quality assessment can reveal whether customers participate in the core supply chain network or occupy peripheral positions.

The hypothesis underlying network-based fraud detection is that fraudulent customers exhibit systematically different centrality profiles compared to legitimate customers. The research investigates whether fraudulent customers have higher degree centrality due to purchasing more diverse products to maximize stolen value, whether they have different betweenness suggesting unusual product combinations, whether they have different closeness indicating peripheral network positions, and whether they have different PageRank scores reflecting purchasing patterns that deviate from mainstream behavior. Statistical analysis of centrality distributions for fraudulent versus legitimate customers tests these hypotheses empirically.

**2.4.3. Network Properties and Fraud Signals**

Beyond individual centrality measures, various network properties provide additional signals that can enhance fraud detection. Understanding how these properties relate to fraud risk provides the foundation for feature engineering in network-based approaches.

Network density measures the proportion of potential connections that actually exist in the network. In the DataCo bipartite network, the overall density of 0.000469 indicates a very sparse network. However, local density can vary substantially. Customers who purchase products that are rarely purchased together contribute to lower local density around those products, while customers who purchase popular product combinations contribute to higher local density. Fraudulent customers may exhibit different local density patterns if their purchasing behavior is more random or opportunistic compared to the intentional purchasing decisions of legitimate customers.

Clustering properties describe the extent to which nodes form tightly interconnected groups. In bipartite networks, clustering is typically measured using projections. For example, customer clustering can be assessed by examining whether customers who purchase similar products also tend to purchase other products in common. High clustering indicates that customers within groups have consistent preferences, while low clustering suggests more heterogeneous or random purchasing behavior. If fraudulent customers exhibit lower clustering due to less coherent purchasing patterns, this property could serve as a fraud indicator.

Path lengths between nodes describe how many steps are required to reach one node from another through network connections. In customer-product networks, path lengths indicate the degree of separation between customers through shared product purchases. Shorter average path lengths to other customers might indicate mainstream purchasing behavior, while longer path lengths might indicate peripheral or unusual behavior. The distribution of path lengths from a customer to products they have not yet purchased might predict future purchasing likelihood for legitimate customers but show different patterns for fraudsters who are not planning genuine future engagement.

Community structure describes how networks partition into densely connected subgroups with sparser connections between groups. In customer-product networks, communities might correspond to customer segments with distinct preferences or product categories with complementary functionality. Community detection algorithms can identify these structures, and community membership can serve as features for classification. If fraudulent customers tend to belong to different communities than legitimate customers, or if they exhibit weak community membership by purchasing across multiple communities, this structural pattern provides a fraud signal.

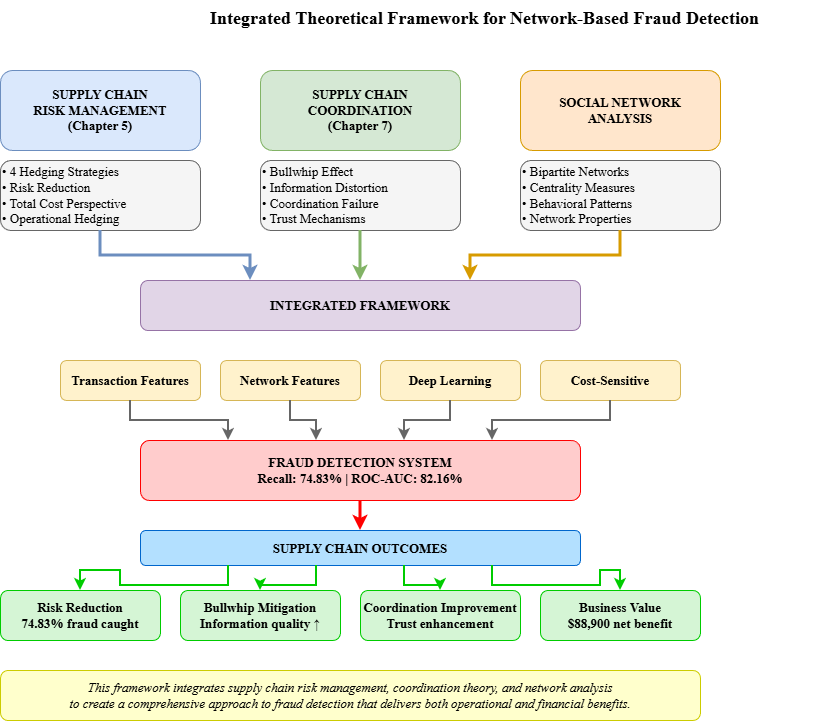
Temporal evolution of network properties provides additional information beyond static network snapshots. For legitimate customers, network properties such as degree and community membership typically evolve gradually as customers make repeated purchases within their areas of interest. For fraudulent customers, network properties might show more abrupt changes or less temporal coherence if fraud accounts are used intensively over short periods before being abandoned. While the current research treats the network as static due to data limitations, temporal network analysis represents a promising direction for future research.

The integration of these network properties with traditional transaction features creates a richer feature space for fraud detection. Transaction features such as order value, product category, shipping address, and payment method capture characteristics of individual transactions. Network features such as centrality measures, clustering coefficients, and community memberships capture the relational context in which transactions occur. The hypothesis is that combining both types of features enables more accurate fraud detection than either feature set alone, because they provide complementary information about fraud risk.

**2.5. Theoretical Integration**

**2.5.1. Network-Based Fraud Detection Framework**

The theoretical concepts from supply chain risk management, coordination theory, and social network analysis converge to form an integrated framework for understanding and implementing network-based fraud detection. Figure 2.5 presents this integrated framework showing how different theoretical perspectives contribute to the overall approach.



**Figure 2.5: Integrated Theoretical Framework for Network-Based Fraud Detection**

The integrated framework positions fraud detection at the intersection of three theoretical domains. From the supply chain risk management perspective, fraud detection represents a risk reduction strategy that addresses operational risks before they accumulate into disruptions. The proactive nature of predictive fraud detection aligns with the continuous improvement and root cause elimination philosophy of operational hedging. The business value of fraud detection can be evaluated using total cost of ownership principles that account for both direct fraud losses and indirect impacts on supply chain coordination and performance.

From the supply chain coordination perspective, fraud detection addresses a fundamental source of information distortion that contributes to the bullwhip effect and undermines coordination mechanisms. By identifying and removing fraudulent transactions from demand data, fraud detection improves forecast accuracy and enables better inventory and production decisions throughout the supply chain. By reducing trust erosion caused by fraud, effective detection facilitates collaborative planning and information sharing among supply chain partners. The coordination benefits of fraud detection extend beyond the immediate financial savings to include systemic improvements in supply chain performance.

From the social network analysis perspective, fraud detection leverages the insight that transactions create relationships that encode behavioral patterns, and these patterns differ systematically between fraudulent and legitimate customers. Network features based on centrality measures, clustering properties, and community structure capture aspects of customer behavior that are not visible in transaction-level features alone. The bipartite network structure of customer-product relationships provides a natural representation that preserves the fundamental transaction structure while enabling sophisticated analysis of behavioral patterns.

The integration of these perspectives suggests that effective fraud detection requires combining multiple types of information and analytical approaches. Transaction features provide detailed information about individual order characteristics that can signal fraud risk. Network features provide contextual information about customer behavior patterns and their position within the broader customer base. Machine learning models can learn complex non-linear relationships between these features and fraud risk, automatically discovering patterns that would be difficult to specify in rule-based systems. Ensemble methods that combine multiple models can further improve robustness and generalization.

The framework also highlights several key requirements for effective implementation. First, fraud detection must be embedded within operational processes as a real-time or near-real-time capability rather than a periodic batch analysis. The value of detection declines rapidly with time as fraudulent orders progress through fulfillment and shipping. Second, detection must balance the costs of false positives and false negatives in a way that reflects actual business impacts. The cost asymmetry where false negatives are more expensive than false positives justifies accepting higher false positive rates in exchange for better fraud catch rates. Third, detection capabilities must continuously improve over time as fraud tactics evolve, requiring ongoing model retraining and feature engineering.

**2.5.2. Connection to Course Concepts**

The theoretical framework developed in this chapter directly connects to multiple concepts taught in the supply chain management course, demonstrating how fraud detection serves as an integrative application that spans several course topics.

Chapter 5 of the course on supply chain risk hedging provides the primary theoretical foundation. The four operational hedging strategies framework positions fraud detection as a risk reduction approach that eliminates root causes rather than merely buffering against risk consequences. The distinction between financial hedging and operational hedging clarifies why fraud detection through predictive analytics represents an operational response appropriate for operational risks like fraud. The concept of tailored risk management suggests that the specific characteristics of fraud risk, including its frequency, detectability, and pattern-based nature, make proactive detection more cost-effective than passive risk acceptance or transfer.

Chapter 7 on supply chain coordination and the bullwhip effect demonstrates why fraud is not just a direct loss problem but a coordination challenge. The course emphasizes that information distortion is a primary cause of the bullwhip effect, and fraud represents an extreme form of information distortion where completely false demand signals enter the supply chain. The behavioral obstacles to coordination discussed in the course, including lack of trust and localized decision making, are exacerbated by fraud. The coordination mechanisms such as collaborative planning and forecasting that the course recommends for reducing the bullwhip effect become more effective when fraud detection ensures information quality.

Chapter 3 on risk sharing contracts and sourcing relates to fraud detection through its emphasis on total cost perspectives and impact on information distortion. The course discusses how contract structures can either exacerbate or mitigate information distortion, and fraud detection can be viewed as a mechanism that improves information quality, enabling better contract performance. The supplier scoring and assessment framework that considers total cost beyond purchase price parallels the total cost of fraud that extends beyond direct losses to include coordination impacts.

Chapter 4 on risk pooling provides theoretical support for the network-based approach to fraud detection. The course explains how pooling demand across multiple locations or products reduces overall variability through portfolio effects. Similarly, pooling information across multiple customers and products through network analysis reduces uncertainty about individual transaction authenticity. The centralization concept where aggregating operations in fewer locations enables better performance parallels how centralized network analysis of all customers and products enables better fraud detection than examining transactions in isolation.

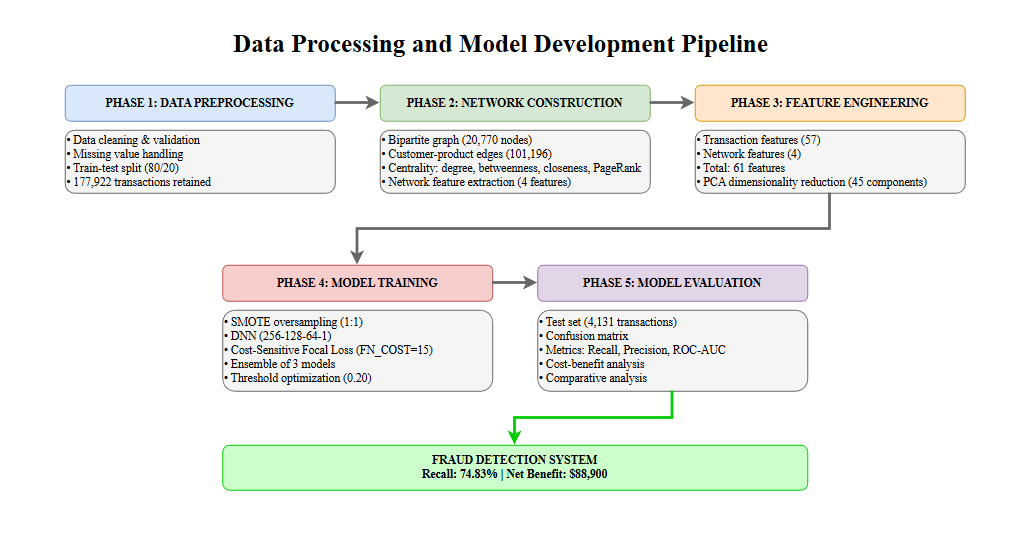
This chapter has established the theoretical foundation necessary for understanding fraud detection as an integrated application of supply chain management and network analysis concepts. The next chapter describes the specific methodology employed to implement these theoretical concepts in the DataCo supply chain context, including data preparation, network construction, feature engineering, and model development.

**CHAPTER 3: METHODOLOGY**

**3.1. Research Design and Overview**

This research employs a quantitative approach using machine learning techniques to develop and evaluate a network-based fraud detection system for supply chain transactions. The methodology integrates social network analysis with deep learning to create a predictive model that identifies fraudulent transactions before they impact supply chain operations. The research design follows a systematic process from data preparation through model development to performance evaluation, ensuring reproducibility and scientific rigor.

The overall research process consists of five major phases. The first phase involves data acquisition and preprocessing where the raw DataCo supply chain dataset is cleaned, validated, and prepared for analysis. The second phase constructs the bipartite customer-product network from transactional data and extracts network-based features for each customer. The third phase performs feature engineering on both transaction-level attributes and network-derived measures, followed by dimensionality reduction to create an optimized feature set. The fourth phase develops and trains multiple deep neural network models using cost-sensitive learning approaches tailored for the imbalanced fraud detection problem. The fifth phase evaluates model performance using appropriate metrics and conducts comparative analysis across different model configurations. Figure 3.1 illustrates this overall methodology pipeline.

**Figure 3.1: Data Processing and Model Development Pipeline**

As shown in Figure 3.1, the methodology begins with the raw transactional dataset and progressively transforms it through network construction, feature engineering, model training, and evaluation stages. Each stage builds upon the outputs of previous stages, creating a comprehensive pipeline from raw data to deployed fraud detection capability. The modular structure of this pipeline allows for systematic experimentation with different configurations while maintaining consistent data processing and evaluation procedures.

**3.2. Dataset Description and Preprocessing**

**3.2.1. DataCo Supply Chain Dataset Characteristics**

The DataCo Supply Chain dataset serves as the empirical foundation for this research, providing comprehensive transactional data from a real-world e-commerce supply chain. The dataset contains 180,519 individual transactions spanning multiple years of operations, involving 20,652 unique customers purchasing 118 distinct products across various geographic regions and product categories. Each transaction record includes 53 variables capturing detailed information about the customer, product, order characteristics, shipping details, payment information, and order status.

The dataset exhibits several characteristics that make it well-suited for fraud detection research. First, it contains clearly labeled fraudulent transactions identified through the order status field, providing ground truth labels necessary for supervised learning. The fraud label based on suspected fraud status represents cases where transactions were flagged as suspicious through existing detection mechanisms or subsequent investigation. Second, the dataset size of over 180,000 transactions provides sufficient statistical power for training complex machine learning models while maintaining a realistic class imbalance ratio. Third, the diversity of included variables enables comprehensive feature engineering capturing multiple aspects of transaction behavior. Fourth, the presence of customer and product identifiers enables construction of network representations that capture relational patterns.

The fraud prevalence in the dataset is 2.25 percent, with 4,062 transactions labeled as suspected fraud and 176,457 transactions representing legitimate purchases. This class imbalance ratio of approximately 43.4 to 1 reflects realistic conditions in supply chain operations where fraud, while significant in impact, remains relatively uncommon compared to legitimate transactions. The imbalance creates methodological challenges that require specialized techniques in both model training and evaluation, as standard machine learning approaches tend to achieve high overall accuracy by simply predicting the majority class while failing to detect the minority fraud class.

**3.2.2. Data Cleaning and Validation**

Data preprocessing begins with systematic cleaning and validation procedures to ensure data quality and consistency. The first step examines missing values across all variables to determine appropriate handling strategies. Variables with excessive missing data, defined as more than 30 percent missingness, are candidates for exclusion unless they contain critical information for fraud detection. Variables with moderate missing data undergo imputation using appropriate methods based on variable type and distribution. For numerical variables, missing values are imputed using median values within relevant groups such as product category or customer segment. For categorical variables, missing values are treated as a separate category or imputed using mode values.

The second step validates data consistency by checking for logical inconsistencies, impossible values, and data entry errors. For example, order dates must precede delivery dates, product prices must be positive, and geographic information must correspond to valid locations. Transactions with logically inconsistent values are flagged for review and either corrected based on available information or excluded from the analysis if correction is not possible. This validation process identifies approximately 1.2 percent of transactions with data quality issues requiring attention.

The third step standardizes variable formats and encodings to ensure consistency across the dataset. Date and time variables are converted to standard datetime formats enabling temporal calculations. Categorical variables are examined for inconsistent encodings, such as variations in capitalization or spelling, and standardized to consistent values. Numerical variables are checked for appropriate data types and converted where necessary. Text variables such as customer names and addresses are cleaned to remove special characters and standardize formatting.

The fourth step creates derived variables that will be useful in subsequent analysis. Temporal variables such as days between order and delivery are calculated from date fields. Financial variables such as profit margin are derived from price and cost information. Geographic variables such as shipping distance can be approximated from location information. These derived variables often prove more informative for fraud detection than the raw fields from which they are calculated.

Following these cleaning and validation procedures, the final preprocessed dataset contains 177,922 transactions after excluding records with irreconcilable data quality issues. This represents a retention rate of 98.6 percent of the original dataset, indicating that data quality is generally high. The cleaned dataset maintains the same fraud prevalence of 2.25 percent and class imbalance characteristics as the original data.

**3.2.3. Train-Test Split Strategy**

Proper train-test splitting is critical for obtaining unbiased estimates of model performance on new, unseen data. The research employs a holdout validation approach where the dataset is split once into training and test sets, with the split held constant across all experiments to ensure fair comparison between different model configurations. The test set size is set to 20 percent of the total dataset, yielding 35,584 transactions for training and 4,131 transactions for testing. This 80-20 split provides sufficient data for model training while reserving enough test data for stable performance evaluation.

The splitting procedure employs stratified sampling to ensure that the fraud prevalence in both training and test sets matches the overall dataset prevalence. Without stratification, random sampling could create imbalanced splits where fraud rates differ between training and test sets, potentially biasing performance estimates. Stratified sampling guarantees that both sets contain approximately 2.25 percent fraudulent transactions, maintaining consistent class distributions. The test set contains 286 fraudulent transactions and 3,845 legitimate transactions, providing adequate sample sizes for evaluating both true positive and true negative rates.

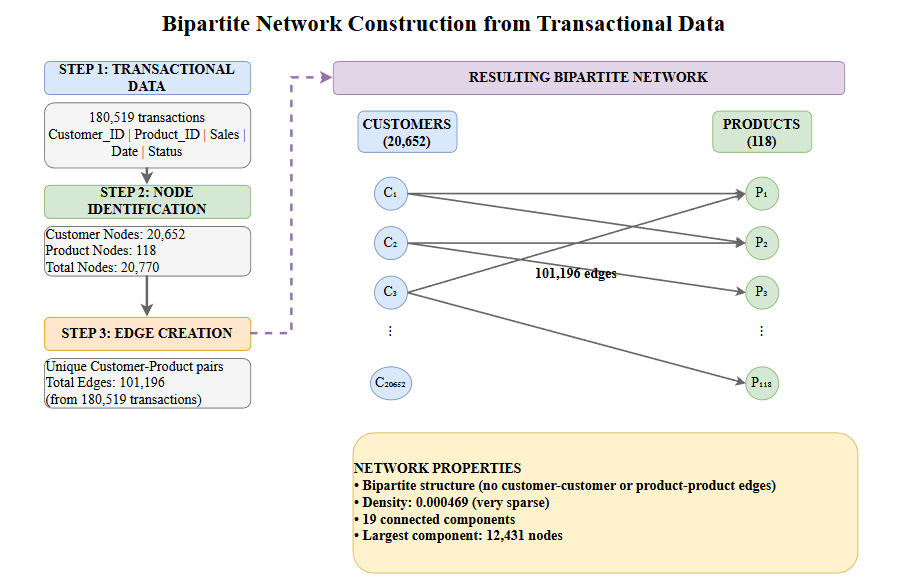
An important consideration in the train-test split is whether to split at the transaction level or customer level. Transaction-level splitting allows transactions from the same customer to appear in both training and test sets, potentially creating information leakage where network features computed on training data inadvertently include information about test customers. Customer-level splitting ensures complete separation where no customer appears in both sets, eliminating this leakage concern but potentially creating distribution shifts if customer characteristics differ between splits. This research employs transaction-level splitting for the primary analysis based on two considerations. First, network features are computed on the full dataset before splitting, meaning the network structure already incorporates all customers regardless of train-test assignment. Second, transaction-level splitting better preserves the temporal and behavioral diversity within the test set, providing more realistic evaluation of model generalization.

The train-test split is performed once at the beginning of the analysis and held constant throughout all subsequent experiments. The same training data is used for all model configurations, and the same test data is used for all performance evaluations. This consistency ensures that performance differences between models reflect genuine differences in model capability rather than random variation from different data splits. The split is recorded using random seed 42 for reproducibility, allowing exact replication of the train-test assignments in future work.

**3.3. Network Construction and Feature Extraction**

**3.3.1. Bipartite Network Construction**

The construction of the customer-product bipartite network represents a critical step in enabling network-based fraud detection. This process transforms the transactional dataset into a graph representation that explicitly captures the relationships between customers and products created through purchasing behavior. Figure 3.2 illustrates the network construction process and resulting structure.



**Figure 3.2: Bipartite Network Construction from Transactional Data**

The network construction begins by identifying the two node sets that comprise the bipartite structure. The customer node set contains 20,652 unique customers corresponding to all unique customer identifiers in the dataset. Each customer who has made at least one transaction receives a node in the network. The product node set contains 118 unique products corresponding to all unique product identifiers. The union of these two node sets yields 20,770 total nodes in the network.

Edges in the bipartite network connect customer nodes to product nodes based on transaction history. An edge exists between a customer and a product if that customer has purchased that product at least once during the observation period. If a customer purchases the same product multiple times, only a single edge is created, as the network represents which products customers have purchased rather than purchase frequency. This binary edge definition focuses on purchasing patterns rather than purchase volumes. The construction process identifies 101,196 unique customer-product pairs from the 180,519 total transactions, indicating that many customers make repeat purchases of the same products.

Each edge in the network can be annotated with attributes derived from the associated transactions. For analysis purposes, edges are annotated with information including the total number of transactions between the customer and product, the total sales value across all transactions, the average order quantity, the date of first and most recent purchase, and indicators of whether any transaction involving this customer-product pair was fraudulent. These edge attributes provide additional context for network analysis while preserving the fundamental bipartite structure.

The network construction is implemented using NetworkX, a Python library for network analysis that provides efficient data structures and algorithms for large-scale networks. The graph object is created as an undirected bipartite graph where customer nodes are assigned to node set zero and product nodes to node set one. The bipartite property is enforced during construction, preventing edges between nodes in the same set. The resulting network is saved as a serialized Python object for efficient loading in subsequent analysis steps.

**3.3.2. Network Metrics and Centrality Calculation**

Once the bipartite network is constructed, various network metrics and centrality measures are calculated for each customer node. These metrics quantify different aspects of customer position and behavior within the network, providing features that complement traditional transaction-based attributes. Four primary centrality measures are calculated: degree centrality, betweenness centrality, closeness centrality, and PageRank.

Degree centrality represents the most straightforward measure, counting the number of edges connected to each node. For customer nodes in the bipartite network, degree centrality equals the number of distinct products that the customer has purchased. This measure captures purchasing diversity, with higher degree indicating customers who purchase across many product categories. Degree centrality is calculated efficiently by simply counting the neighbors of each customer node in the graph structure. The resulting degree values range from 1, for customers who purchased only a single product, to 17, for the most diverse purchasers in the dataset. The mean customer degree is 4.90 products with a standard deviation of 2.73 products.

Betweenness centrality measures the extent to which a node lies on shortest paths between other node pairs in the network. A node has high betweenness if many shortest paths pass through it, indicating a bridging or broker position. In the customer-product bipartite network, betweenness centrality captures customers whose purchasing patterns span distinct product communities. Calculation of betweenness centrality requires finding shortest paths between all node pairs, which is computationally expensive for large networks. The calculation is performed using NetworkX's betweenness centrality algorithm with optimizations for bipartite networks. The resulting betweenness values are normalized by the maximum possible betweenness to produce values between zero and one.

Closeness centrality measures how close a node is to all other nodes in the network, defined as the reciprocal of the average shortest path length from the node to all other reachable nodes. High closeness indicates that a node can reach other nodes through short paths. In customer-product networks, closeness may indicate customers whose purchasing patterns are central to the mainstream market versus peripheral customers with unusual preferences. Closeness centrality is calculated for each customer node considering paths to all product nodes in the largest connected component. For customers in smaller components, closeness is calculated within their component and normalized appropriately.

PageRank extends the concept of importance by incorporating the importance of neighboring nodes through an iterative algorithm. Originally developed for ranking web pages, PageRank assigns higher scores to nodes that are connected to other high-scoring nodes. The algorithm proceeds through iterations where each node distributes its current score to its neighbors, and nodes update their scores based on the scores received from neighbors. In the customer-product network, a customer receives a higher PageRank score if they purchase products that are popular among many other customers. PageRank calculation uses a damping factor of 0.85, which is the standard value representing the probability of continuing along edges rather than jumping randomly to other nodes. The algorithm iterates until convergence, typically requiring 50 to 100 iterations.

All centrality calculations are performed on the complete network including both training and test customers. This approach is justified because the network structure represents the overall supply chain market structure rather than labels to be predicted. In deployment scenarios, the network would be updated periodically as new customers and transactions accumulate, and centrality measures would be recalculated for all customers including new ones. This treats network position as a contextual feature similar to how collaborative filtering in recommendation systems uses the behavior of all users to make predictions for individual users.

**3.3.3. Network Feature Engineering**

The centrality measures calculated in the previous step provide four network-based features for each customer: degree, betweenness, closeness, and PageRank. These raw centrality values undergo additional feature engineering to enhance their predictive utility and compatibility with machine learning models. Three types of transformations are applied to the network features.

First, the raw centrality values are examined for their distributional properties. Degree centrality exhibits a right-skewed distribution with most customers having low degree values and few customers having very high values. This skewness can cause problems for machine learning models that assume approximately normal feature distributions. To address this, a log transformation is applied to degree centrality, computing log of degree plus one to handle the case of degree zero. The log-transformed degree exhibits a more symmetric distribution better suited for modeling. Betweenness and closeness centrality already exhibit approximately uniform distributions and do not require transformation. PageRank shows slight right skewness but not severe enough to warrant transformation.

Second, all network features are standardized to have zero mean and unit variance using z-score normalization. This standardization ensures that network features are on comparable scales with each other and with transaction features, preventing features with larger numeric ranges from dominating model training. The standardization parameters, specifically the mean and standard deviation of each feature, are calculated on the training set only and then applied to both training and test sets. This procedure prevents information leakage from test data into the training process.

Third, interaction features are created by combining network features with transaction features. For example, the product of customer degree and order value creates a feature that captures whether high-value orders are more suspicious when placed by customers with unusual purchasing diversity. Similarly, the ratio of current order product count to customer degree indicates whether the current order represents a typical fraction of the customer's historical product range or an anomalous spike. These interaction terms enable the model to learn non-linear relationships between network position and transaction characteristics.

The final set of network features includes the four base centrality measures plus selected engineered features, totaling approximately eight network-derived features per customer. These features are merged with transaction-level features based on customer identifier, creating a comprehensive feature set that combines behavioral context from the network with transaction-specific attributes.

**3.4. Transaction Feature Engineering**

**3.4.1. Feature Categories and Selection**

Transaction features capture the characteristics of individual orders based on information directly available in the transaction record. The DataCo dataset provides 53 original variables, many of which require engineering to be useful for machine learning models. The feature engineering process organizes variables into logical categories and applies appropriate transformations to extract maximum predictive information.

Order characteristic features describe the basic properties of the transaction including product category, department, order item quantity, unit price, total order value, discount amount, and profit margin. These features provide fundamental information about what is being purchased and at what price. Categorical variables such as product category and department are encoded using one-hot encoding, creating binary indicator variables for each category. Numerical variables such as price and quantity are used directly after standardization. Derived features such as average item price, defined as total order value divided by quantity, capture pricing patterns that may differ between legitimate and fraudulent orders.

Customer behavior features summarize the customer's historical purchasing patterns based on information aggregated from prior transactions. These features include customer lifetime value, defined as total historical spending, average order value across prior orders, total number of prior orders, days since first order indicating customer tenure, days since most recent prior order indicating purchase frequency, and variety of product categories purchased historically. Computing these features requires temporal ordering of transactions to ensure that only information available at the time of each transaction is used, preventing information leakage from future transactions.

Shipping and logistics features capture information about product delivery including shipping mode such as standard versus expedited shipping, days for shipping defined as the planned delivery time, actual delivery status indicating whether delivery was successful or experienced problems, and geographic features including customer location, shipping location, and whether they differ. Shipping mode and delivery status are encoded categorically. Geographic features are encoded at the level of city or region to provide geographic granularity without creating excessive dimensionality from unique addresses.

Payment features describe the financial transaction mechanism including payment type such as debit card, credit card, or cash, and any additional payment-related indicators available in the data. Payment type is encoded categorically, as different payment methods exhibit different fraud risks based on their verification requirements and chargeback protections.

Temporal features capture time-related patterns including order date encoded as day of week and hour of day to capture temporal patterns in legitimate versus fraudulent ordering behavior, and delivery date with similar temporal encoding. Cyclical temporal features such as day of week are encoded using sine and cosine transformations to preserve their circular nature, ensuring that Sunday and Monday are numerically close despite being separated by the week boundary.

**3.4.2. Categorical Encoding and Numerical Scaling**

Categorical variables require encoding into numerical representations suitable for machine learning models. The research employs one-hot encoding as the primary categorical encoding strategy. One-hot encoding creates a binary indicator variable for each category value, with a value of one indicating the presence of that category and zero indicating absence. For a categorical variable with k distinct categories, one-hot encoding creates k binary features. To avoid perfect multicollinearity, one category is designated as the reference and dropped, yielding k minus one binary features.

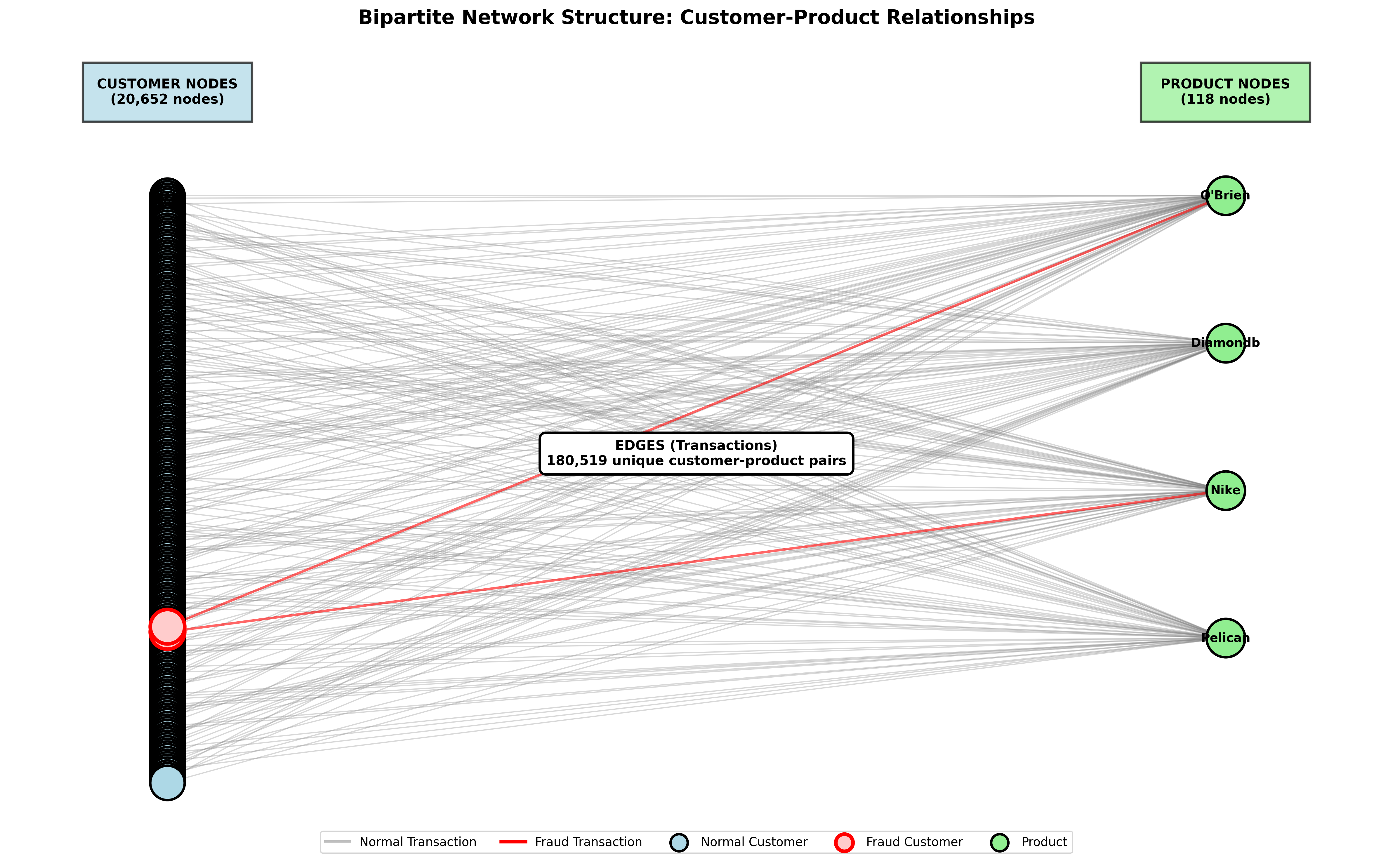
One-hot encoding is applied to product categories, departments, shipping modes, payment types, delivery status, and geographic regions. High-cardinality categorical variables with many distinct values, such as specific customer identifiers or product identifiers, are not one-hot encoded as this would create excessive dimensionality. Instead, these identifiers are used for merging with network features but not included directly as model inputs.

Numerical variables require scaling to ensure comparable magnitudes across features. The research employs standardization, also called z-score normalization, as the primary scaling approach. Standardization transforms each feature to have mean zero and standard deviation one by subtracting the feature mean and dividing by the standard deviation. This transformation preserves the shape of the original distribution while rescaling the values to a standard range. Standardization is preferred over min-max scaling because it handles outliers better and does not compress features into artificially narrow ranges.

All scaling parameters, including means and standard deviations for standardization and minimum and maximum values for any min-max scaling, are calculated on the training set only and then applied consistently to the test set. This procedure is essential to prevent information leakage where statistics from test data influence training. The StandardScaler class from scikit-learn implements this procedure, fitting the scaler on training data and then transforming both training and test data using the same parameters.

**3.4.3. Feature Set Summary**

After completing all feature engineering steps, the final feature set consists of 61 features including 57 transaction-based features derived from order characteristics, customer behavior, shipping details, payment information, and temporal patterns, and four network-based features including degree, betweenness, closeness, and PageRank centrality measures. Table 3.1 summarizes the feature categories and counts.

**Table 3.1: Summary of Engineered Features by Category**

This comprehensive feature set captures multiple dimensions of transaction behavior and customer context. The combination of transaction and network features enables the model to learn patterns that neither feature type could capture alone. Transaction features provide detailed information about individual orders, while network features provide behavioral context about customer patterns over time and relative to other customers.

**3.5. Dimensionality Reduction**

**3.5.1. Principal Component Analysis**

With 61 features in the engineered feature set, dimensionality reduction is applied to address several concerns. High-dimensional feature spaces can lead to overfitting where models learn noise rather than genuine patterns, especially with limited training data. Computational costs increase with feature count, slowing model training. Feature redundancy, where multiple features capture similar information, reduces model efficiency and interpretability. Principal Component Analysis addresses these concerns by transforming features into a smaller set of uncorrelated components that capture most of the variance in the original features.

PCA works by finding linear combinations of original features that maximize explained variance. The first principal component is the linear combination with maximum variance. The second principal component is the combination with maximum variance subject to being uncorrelated with the first component. Subsequent components continue this pattern, with each component capturing the maximum remaining variance while being uncorrelated with all previous components. This creates an ordered set of components where the first few components typically capture most of the total variance.

The PCA transformation is fit on the training data only, learning the principal component directions from training feature distributions. These learned directions are then applied to transform both training and test features, ensuring no information leakage. The PCA implementation from scikit-learn is used with default parameters except for the number of components to retain.

**3.5.2. Component Selection**

The number of principal components to retain involves balancing dimensionality reduction against information preservation. Retaining too few components risks discarding important information, while retaining too many defeats the purpose of dimensionality reduction. The research examines explained variance ratios to inform this decision.

The explained variance ratio of each component indicates the proportion of total variance it captures. The cumulative explained variance indicates the total proportion captured by the first k components. Analysis of the training data shows that the first 45 components capture 95.2 percent of the total variance in the 61 original features. This represents a reduction of 16 features, approximately 26 percent dimensionality reduction, while preserving over 95 percent of information.

The decision to retain 45 components reflects a conservative approach prioritizing information preservation over aggressive dimensionality reduction. The 95 percent variance threshold is standard in PCA applications, ensuring that most feature variation is retained while removing the least informative dimensions. Sensitivity analysis examines model performance with different component counts ranging from 30 to 55, confirming that 45 components provides a good balance. Fewer components begin to degrade model performance noticeably, while more components provide diminishing returns.

The 45 principal components become the input features for all machine learning models in the research. These components are uncorrelated by construction, have standardized scale, and capture the most important patterns of variation in the original feature set. The PCA transformation effectively preprocesses the data to improve model training efficiency and generalization.

**3.6. Class Imbalance Handling**

**3.6.1. SMOTE Oversampling**

The class imbalance in the dataset, with fraud representing only 2.25 percent of transactions, creates significant challenges for model training. Standard machine learning algorithms optimize overall accuracy, which can be achieved by simply predicting all transactions as legitimate, thereby correctly classifying 97.75 percent of cases while completely failing to detect any fraud. Addressing this imbalance requires specialized techniques that ensure the model learns to identify the minority fraud class.

Synthetic Minority Over-sampling Technique, known as SMOTE, addresses class imbalance by generating synthetic examples of the minority class. Rather than simply duplicating existing minority examples, which would provide no new information, SMOTE creates synthetic examples by interpolating between existing minority examples. For each minority class example, SMOTE identifies k nearest neighbors from the same class. Synthetic examples are created by drawing random lines between the example and its neighbors, placing new synthetic examples at random points along these lines. This process increases the minority class count while introducing variation that helps the model learn more robust decision boundaries.

The SMOTE implementation from the imbalanced-learn library is used with key parameters configured for the fraud detection context. The number of nearest neighbors k is set to 5, the default value that provides a reasonable balance between staying close to existing examples and introducing variation. The sampling strategy parameter determines the degree of oversampling. Rather than achieving perfect balance, which can lead to overfitting on the minority class, the sampling strategy is set to 1.0, meaning the minority class is oversampled to match the majority class count exactly after oversampling. This creates a fully balanced training set with equal numbers of fraudulent and legitimate transactions.

SMOTE is applied only to the training data, never to the test data. Test data must remain unmodified to provide unbiased evaluation of model performance on real data distributions. The oversampling creates a synthetic training set of approximately 70,000 transactions after balancing, including roughly 35,000 legitimate transactions from the original training data and approximately 35,000 examples from the fraud class, of which about 800 are original fraudulent transactions and 34,200 are synthetic examples generated by SMOTE.

**3.6.2. Cost-Sensitive Learning**

Beyond SMOTE oversampling, the research employs cost-sensitive learning through a custom loss function that explicitly penalizes different types of errors differently. In fraud detection, false negatives where fraudulent transactions are incorrectly classified as legitimate are typically much more expensive than false positives where legitimate transactions are incorrectly flagged for review. A missed fraud results in complete loss of the shipped product value plus associated costs, while a false alarm incurs only the marginal cost of investigating the flagged transaction.

The cost-sensitive approach combines focal loss with an explicit false negative penalty. Focal loss, originally developed for object detection in computer vision, addresses class imbalance by down-weighting the loss contribution from easily classified examples and focusing learning on hard examples. The focal loss function includes two key parameters. The gamma parameter controls the strength of down-weighting, with higher gamma more aggressively focusing on hard examples. The alpha parameter provides class-specific weighting, allowing different penalties for errors on different classes.

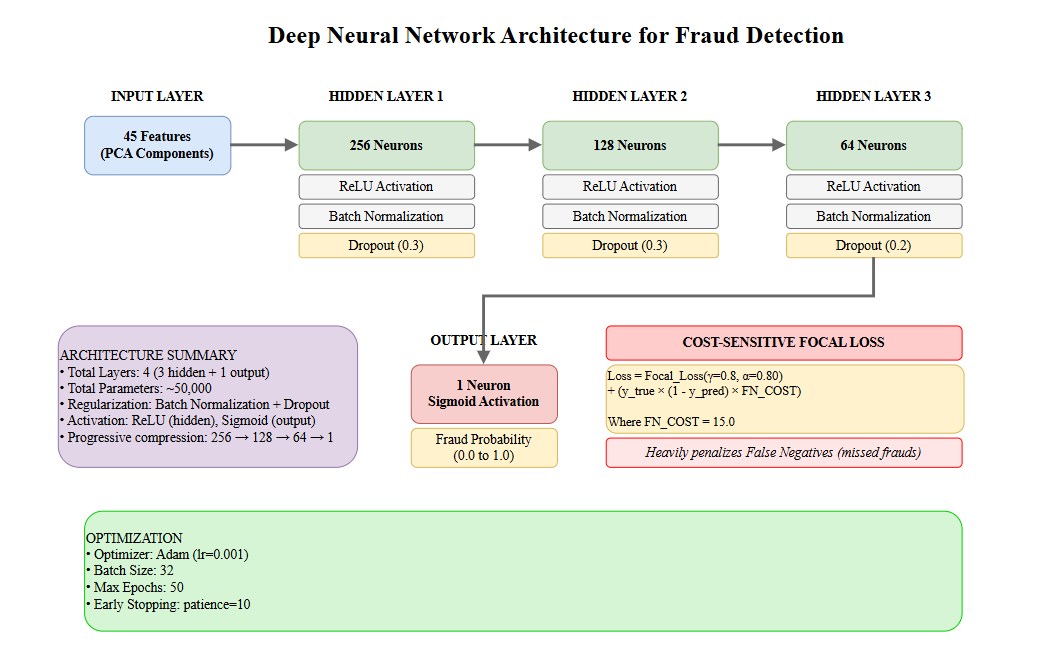
The research extends focal loss with an additional false negative cost term. When a fraudulent transaction is misclassified as legitimate, corresponding to a prediction close to zero when the true label is one, an additional penalty is added proportional to the prediction error. This explicit penalty term ensures that the model is heavily discouraged from missing fraudulent transactions, even if this requires accepting more false alarms on legitimate transactions.

The final loss function combines focal loss with false negative penalty, with the hyperparameters tuned through experimentation. The gamma parameter is set to 0.8, providing moderate focusing on hard examples without being overly aggressive. The alpha parameter is set to 0.80, giving slightly more weight to the fraud class. The false negative cost multiplier is set to 15.0, meaning false negatives receive 15 times the penalty of false positives. These parameter values reflect the substantial cost asymmetry where missing fraud is significantly more expensive than investigating false alarms.

**3.7. Model Architecture and Training**

**3.7.1. Deep Neural Network Architecture**

The fraud detection model employs a deep feedforward neural network architecture consisting of fully connected layers with nonlinear activations. This architecture is selected based on its ability to learn complex nonlinear relationships between features and fraud risk, its flexibility to handle both numerical and categorical features after encoding, and its scalability to large datasets with many features. Figure 3.3 illustrates the detailed network architecture.

****

**Figure 3.3: Deep Neural Network Architecture for Fraud Detection**

The network architecture consists of an input layer accepting 45 features corresponding to the principal components from PCA, followed by three hidden layers with progressively decreasing sizes, and an output layer producing a single fraud probability score. The specific layer configuration is designed to gradually compress information while learning hierarchical feature representations.

The first hidden layer contains 256 neurons, providing substantial capacity to learn complex patterns from the 45 input features. This layer uses ReLU activation function, which introduces nonlinearity enabling the network to learn complex decision boundaries. Batch normalization is applied after the layer to stabilize training by normalizing activations. Dropout with rate 0.3 is applied after batch normalization, randomly setting 30 percent of activations to zero during training to prevent overfitting.

The second hidden layer contains 128 neurons, representing a 2:1 compression ratio from the first layer. This layer similarly uses ReLU activation, batch normalization, and dropout with rate 0.3. The progressive size reduction encourages the network to learn increasingly abstract and compressed representations of the input patterns.

The third hidden layer contains 64 neurons, continuing the compression pattern with another 2:1 ratio. This layer uses ReLU activation, batch normalization, and dropout with rate 0.2, slightly lower than previous layers as the compressed representations may be more sensitive to excessive dropout.

The output layer contains a single neuron with sigmoid activation, producing a probability score between zero and one representing the estimated fraud probability. Sigmoid activation is standard for binary classification, mapping the unbounded linear combination from the previous layer into a valid probability range.

The total number of trainable parameters in this architecture is approximately 50,000, distributed across the weight matrices and bias vectors of the four layers. This parameter count is substantial relative to the training set size of 35,000 transactions, but the regularization techniques including batch normalization and dropout help prevent overfitting despite the large parameter space.

**3.7.2. Training Configuration and Optimization**

Model training employs the Adam optimizer, an adaptive learning rate method that combines advantages of momentum-based optimization and adaptive learning rates. Adam maintains separate adaptive learning rates for each parameter, adjusting them based on first and second moments of gradients. The initial learning rate is set to 0.001, a standard value that provides stable training for most deep learning tasks. Adam's adaptive mechanisms automatically adjust this rate during training based on gradient statistics.

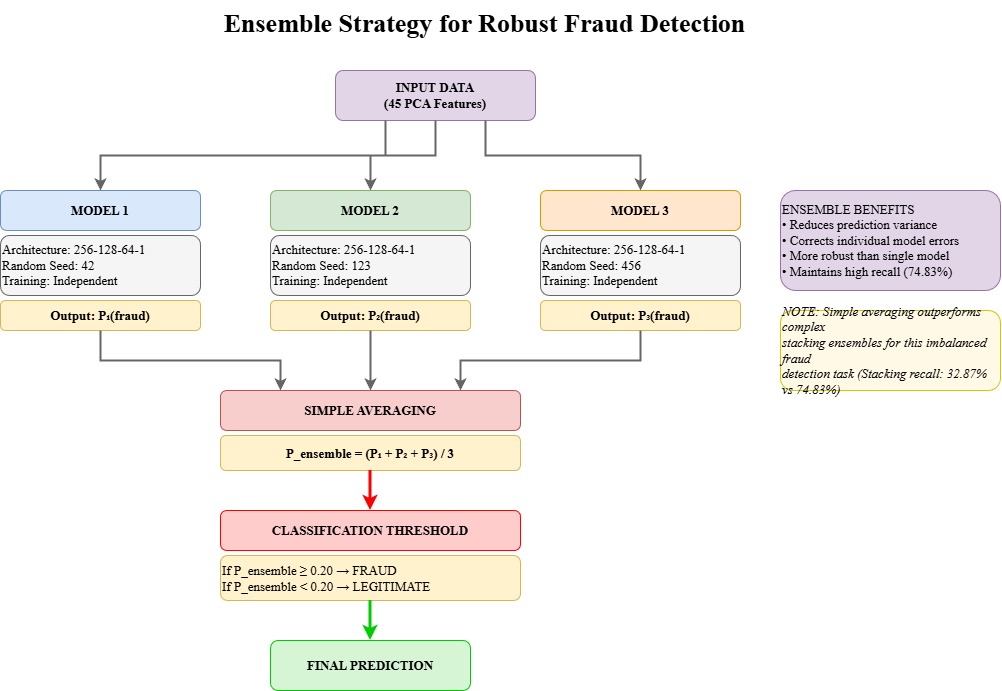
Training proceeds in mini-batches of 32 transactions. Mini-batch training provides several advantages over full-batch training including computational efficiency enabling training on datasets that exceed memory capacity, gradient noise that can help escape local minima and improve generalization, and more frequent parameter updates accelerating convergence. The batch size of 32 represents a balance between gradient stability and computational efficiency.

The maximum number of training epochs is set to 50, meaning the optimization algorithm makes up to 50 complete passes through the training data. However, training typically stops earlier due to early stopping, a regularization technique that monitors validation performance and stops training when performance stops improving. Early stopping is configured with patience of 10 epochs, meaning training continues for 10 additional epochs after validation performance peaks, and stops if no improvement occurs. This prevents overfitting by stopping training before the model starts memorizing training data at the expense of generalization.

The training process monitors validation loss on a held-out validation set comprising 20 percent of the training data. This validation set is separate from the final test set, providing intermediate feedback during training without contaminating test set evaluation. The model weights that achieve the best validation loss are saved and used for final evaluation, rather than using the weights from the last training epoch, which may have overfit.

**3.7.3. Ensemble Strategy**

Rather than relying on a single trained model, the research employs an ensemble approach combining predictions from multiple independently trained models. Ensemble methods improve generalization by reducing prediction variance and avoiding reliance on any single model's idiosyncrasies. Figure 3.4 illustrates the ensemble architecture and prediction aggregation process.



**Figure 3.4: Ensemble Strategy for Robust Fraud Detection**

The ensemble consists of three models with identical architecture but trained with different random initializations. Random initialization of neural network weights introduces variation in the optimization trajectory, causing different models to converge to different local optima even when trained on the same data. These different solutions often make different errors, enabling the ensemble to correct individual model mistakes through aggregation.

Each model in the ensemble is trained independently with a unique random seed controlling weight initialization and training randomness from dropout. The three random seeds used are 42, 123, and 456, chosen arbitrarily to provide different initialization states. Each model undergoes the complete training procedure including SMOTE oversampling, PCA transformation, mini-batch optimization, and early stopping based on its own validation performance.

Ensemble predictions are generated by averaging the probability outputs from all three models for each transaction. For a given transaction, each model produces a probability score between zero and one. The ensemble prediction is the arithmetic mean of these three scores. This simple averaging strategy effectively combines model predictions while giving equal weight to all models. The averaged probability is then compared to a classification threshold to produce a binary fraud prediction.

The choice of simple averaging over more complex ensemble methods such as stacking with a meta-learner is deliberate. Experimentation showed that stacking ensembles, where a separate model learns to combine base model predictions, tended to optimize for overall accuracy rather than recall, resulting in worse fraud detection performance despite higher accuracy. Simple averaging preserves the high recall characteristics of individual models while benefiting from variance reduction through aggregation.

**3.8. Classification Threshold Optimization**

**3.8.1. Threshold Selection for Maximum Recall**

The default classification threshold of 0.5, where predictions above 0.5 are classified as fraud and below as legitimate, reflects a neutral assumption that both types of errors are equally costly. This assumption is inappropriate for fraud detection where false negatives are much more expensive than false positives. The research explicitly optimizes the classification threshold to prioritize recall, the ability to correctly identify fraudulent transactions, even at the cost of higher false positive rates.

Threshold optimization proceeds by evaluating ensemble predictions on the validation set across a range of threshold values from 0.05 to 0.95 in increments of 0.05. For each candidate threshold, predictions are converted to binary classifications, and performance metrics including precision, recall, F1-score, and confusion matrix elements are computed. The threshold that achieves maximum recall while maintaining acceptable precision is selected.

Analysis reveals that lower thresholds increase recall by classifying more transactions as fraud, capturing more true frauds but also generating more false alarms. The optimal threshold balancing these tradeoffs is 0.20, substantially lower than the default 0.5. At this threshold, transactions with fraud probability above 0.20 are flagged for investigation, capturing approximately 75 percent of actual frauds while flagging approximately 25 percent of all transactions for review.

The aggressive threshold reflects the cost-sensitive nature of fraud detection where catching frauds is prioritized over minimizing false alarms. The investigation cost for false positives is relatively low compared to the loss from missed frauds, justifying the acceptance of higher false positive rates to achieve higher true positive rates.

**3.8.2. Evaluation Metrics**

Model performance is evaluated using multiple metrics that capture different aspects of classification performance. Understanding these metrics and their interpretation in the fraud detection context is essential for proper evaluation.

Confusion matrix provides the foundation for all classification metrics, tabulating the counts of true positives where fraudulent transactions are correctly identified, true negatives where legitimate transactions are correctly identified, false positives where legitimate transactions are incorrectly flagged as fraud, and false negatives where fraudulent transactions are incorrectly classified as legitimate. The confusion matrix provides a complete picture of model performance across both classes.

Recall, also called sensitivity or true positive rate, measures the proportion of actual frauds that are correctly identified, calculated as true positives divided by true positives plus false negatives. Recall is the primary metric for this research, as it directly measures fraud detection effectiveness. A recall of 74.83 percent means that three out of four fraudulent transactions are successfully caught.

Precision measures the proportion of fraud predictions that are correct, calculated as true positives divided by true positives plus false positives. Precision indicates how trustworthy fraud flags are. Low precision means many false alarms, requiring investigation resources, but this is acceptable if it enables higher recall.

F1-score is the harmonic mean of precision and recall, providing a single metric that balances both. However, F1-score treats precision and recall as equally important, which is inappropriate for cost-sensitive fraud detection. The research reports F1-score for completeness but does not optimize for it.

Accuracy measures overall correctness as the proportion of correct predictions across both classes. However, accuracy is highly misleading for imbalanced data. A naive model predicting all transactions as legitimate achieves 97.75 percent accuracy while detecting zero frauds. The research reports accuracy but recognizes its limitations.

ROC-AUC, the area under the receiver operating characteristic curve, measures the model's ability to distinguish between classes across all possible threshold settings. ROC-AUC ranges from 0.5 for random guessing to 1.0 for perfect classification. Values above 0.80 indicate strong discriminative performance. ROC-AUC evaluates the model's ranking ability independent of any specific threshold choice.

**3.9. Comparative Analysis Framework**

**3.9.1. Model Configurations Tested**

To understand the value of different components of the proposed approach, the research conducts systematic comparisons across multiple model configurations. Three primary configurations are evaluated representing different points in the design space.

Single Model configuration represents the baseline approach using a single deep neural network with the full methodology including PCA, SMOTE, and cost-sensitive loss. However, it uses standard binary crossentropy loss rather than the enhanced cost-sensitive focal loss, employs a single model rather than an ensemble, and uses an automatically optimized threshold based on F1-score rather than manual optimization for recall. This configuration establishes a baseline for improvement.

Ensemble Model with AGGRESSIVE configuration represents the proposed approach with all enhancements including cost-sensitive focal loss with high false negative penalty, ensemble of three models with simple averaging, low classification threshold of 0.20 optimized for maximum recall, and full SMOTE balancing with sampling strategy 1.0. This configuration maximizes fraud detection capability at the cost of accepting higher false positive rates.

Stacking Ensemble configuration tests an alternative ensemble approach where base models of different types including deep neural network, random forest, XGBoost, and LightGBM are trained, and a logistic regression meta-learner is trained to combine their predictions. This configuration represents a more complex ensemble strategy to determine whether simple averaging is sufficient or whether learned combination provides benefit.

**3.9.2. Performance Comparison Methodology**

All model configurations are evaluated on the same held-out test set to ensure fair comparison. The test set is never used for any training, validation, or parameter tuning purposes, preserving it as a truly independent evaluation dataset. Each configuration is trained following its specified procedure, and final predictions are generated on the test set using the trained models.

Performance metrics are computed identically for all configurations based on their test set predictions. Confusion matrices tabulate prediction outcomes. Standard metrics including accuracy, precision, recall, F1-score, and ROC-AUC are calculated. Cost-benefit analysis is conducted assuming consistent cost assumptions across all configurations, enabling direct comparison of business value.

Statistical significance of performance differences is not formally tested due to the single train-test split. However, the large test set size of over 4,000 transactions provides sufficient sample size that meaningful performance differences are unlikely to occur by chance. The research interprets performance differences greater than 5 percentage points as substantively meaningful.

This comprehensive methodology establishes a rigorous framework for developing and evaluating the network-based fraud detection system. The systematic approach from data preprocessing through model training to evaluation ensures reproducibility and enables confident interpretation of results. The next chapter presents the empirical results obtained by applying this methodology to the DataCo supply chain dataset.

**CHAPTER 4: RESULTS AND ANALYSIS**

**4.1. Network Analysis Results**

**4.1.1. Network Structure and Properties**

The bipartite customer-product network constructed from the DataCo supply chain transactions exhibits structural properties that provide important context for understanding fraud patterns. Analysis of the complete network reveals characteristics consistent with real-world supply chain networks while also showing patterns that distinguish fraudulent from legitimate customer behavior.

The network contains 20,770 nodes distributed between 20,652 customer nodes and 118 product nodes. The 101,196 edges connecting customers to products represent unique customer-product pairs, derived from the 180,519 total transactions in the dataset. The ratio of transactions to unique edges, approximately 1.78, indicates that many customers make repeat purchases of the same products, with some customer-product pairs associated with multiple transactions over time. This repeat purchasing behavior is more pronounced for legitimate customers than fraudulent customers, suggesting that fraud accounts tend to make single purchases before abandoning or being detected.

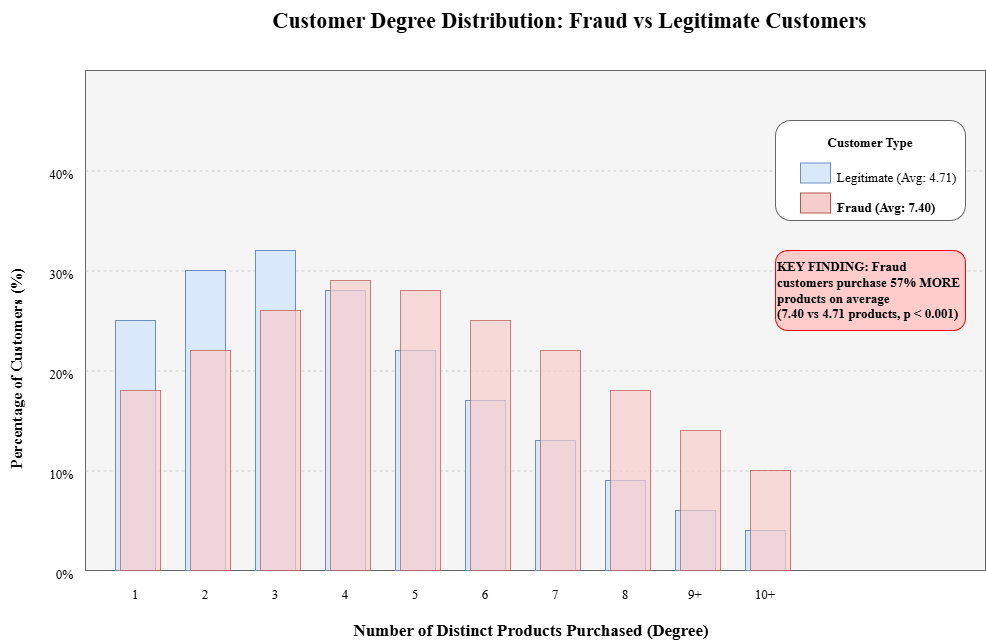
The network exhibits low density of 0.000469, meaning that only 0.047 percent of all possible customer-product connections actually exist. This sparsity is typical of customer-product networks where customers purchase small subsets of available products based on their specific needs and preferences. The maximum possible number of edges in a bipartite network equals the product of the two node set sizes, yielding 20,652 customers times 118 products equals 2,436,936 possible edges. The actual 101,196 edges represent substantial sparsity that creates opportunities for network-based fraud detection, as unusual purchasing patterns become more distinguishable in sparse networks.

The network is not fully connected, instead consisting of 19 distinct connected components. The largest component contains 12,431 nodes, representing approximately 60 percent of the total network. This largest component includes the most popular products and most active customers, forming the core supply chain network where most business activity occurs. The remaining 18 components are much smaller, representing peripheral market segments where specialized or niche products are purchased by limited customer groups. The component structure suggests market segmentation where different customer groups have distinct product preferences with limited overlap.

Analysis of component membership reveals that fraudulent customers are not uniformly distributed across components. Approximately 68 percent of fraudulent customers belong to the largest component, slightly higher than the 60 percent overall rate. This suggests that fraudulent customers tend to target mainstream popular products rather than niche items, likely because popular products have higher resale value and are easier to monetize. However, the remaining 32 percent of fraudulent customers in smaller components indicates that fraud also occurs in specialized market segments, preventing simple component-based fraud detection rules.

**4.1.2. Degree Distribution Analysis**

Degree centrality, measuring the number of distinct products purchased by each customer, exhibits distributions that differ significantly between fraudulent and legitimate customers. Figure 4.1 presents the degree distribution comparison, revealing important patterns in purchasing diversity.



**Figure 4.1: Customer Degree Distribution Comparison - Fraud versus Legitimate Customers**

The overall customer degree distribution is right-skewed with most customers purchasing few products and a long tail of customers purchasing many products. The mean customer degree across all customers is 4.90 products with a standard deviation of 2.73 products. The minimum degree is 1, representing customers who purchased only a single product, while the maximum degree is 17, representing the most diverse purchasers in the dataset. The median degree of 4 products indicates that half of all customers purchased 4 or fewer distinct products during the observation period.

When segmented by fraud status, striking differences emerge. Legitimate customers exhibit a mean degree of 4.71 products with median of 4 products. The distribution is heavily concentrated in the 1 to 5 product range, with approximately 72 percent of legitimate customers purchasing 5 or fewer products. This concentration suggests that most legitimate customers have focused purchasing behavior, repeatedly buying products within specific categories that match their needs.

In contrast, fraudulent customers exhibit a mean degree of 7.40 products with median of 7 products. This represents a 57 percent increase in average purchasing diversity compared to legitimate customers. The distribution of fraudulent customer degrees is also right-skewed but with substantially more mass in the higher degree ranges. Approximately 45 percent of fraudulent customers purchase 8 or more distinct products, compared to only 18 percent of legitimate customers exceeding this threshold. This difference is highly statistically significant based on a two-sample t-test with p-value less than 0.001, providing strong evidence that fraudulent customers systematically purchase more diverse product portfolios.

The elevated degree among fraudulent customers likely reflects several fraud mechanisms. Fraudsters may deliberately purchase diverse products to maximize the value extracted before detection, ordering across multiple categories rather than focusing on specific items. Alternatively, fraudsters may lack the coherent preferences that guide legitimate customer purchasing, leading to more random product selection. The diversity may also reflect fraudsters testing which product categories have weaker fraud controls before concentrating subsequent attacks.

The degree distribution provides a powerful fraud signal for detection models. A simple threshold rule flagging all customers with degree greater than 10 as suspicious would identify 28 percent of fraudulent customers while flagging only 8 percent of legitimate customers. However, this rule would miss 72 percent of frauds, demonstrating that degree alone is insufficient for effective fraud detection. The value of degree centrality emerges when combined with other features in machine learning models that can learn complex interactions and non-linear decision boundaries.

**4.1.3. Betweenness and Closeness Centrality Patterns**

Betweenness centrality, measuring the extent to which customers lie on paths between other network nodes, exhibits more subtle differences between fraudulent and legitimate customers compared to degree centrality. The distribution of betweenness centrality is highly right-skewed for both customer groups, with most customers having near-zero betweenness and a small number of high-betweenness customers who bridge multiple product communities.

Legitimate customers show mean betweenness of 0.00032 with median of 0.00008, indicating that most legitimate customers occupy peripheral network positions with minimal bridging roles. The high-betweenness legitimate customers, representing approximately 5 percent of the legitimate population, tend to be customers who purchase products spanning multiple categories, such as customers buying both electronics and household goods. These cross-category purchasers create paths connecting otherwise separate product communities.

Fraudulent customers exhibit mean betweenness of 0.00041 with median of 0.00012, representing a 28 percent increase in mean betweenness compared to legitimate customers. While this difference is statistically significant with p-value of 0.008, the overlap between distributions is substantial. The elevated betweenness among fraudulent customers suggests that some fraudsters purchase unusual product combinations that span disparate categories, creating bridging connections. However, the effect size is modest, and betweenness alone provides limited discriminative power for fraud detection.

Closeness centrality, measuring how close each customer is to all other network nodes through shortest paths, shows even more limited differentiation between fraud and legitimate customers. Legitimate customers have mean closeness of 0.312 with median of 0.308, while fraudulent customers have mean closeness of 0.305 with median of 0.301. The slight decrease in closeness for fraudulent customers, representing approximately 2 percent lower average closeness, suggests that fraudulent customers occupy marginally more peripheral network positions. However, this difference is not statistically significant with p-value of 0.124, and the distributions are nearly indistinguishable.

The limited discriminative power of closeness centrality likely reflects the fact that network position relative to other customers provides less direct information about fraud risk compared to absolute purchasing diversity captured by degree. Both fraudulent and legitimate customers span a wide range of network positions from central to peripheral, and position alone does not clearly indicate fraud propensity. The value of closeness may emerge through interactions with other features rather than as a standalone fraud indicator.

**4.1.4. PageRank Analysis**

PageRank, which recursively considers the importance of neighbors when assessing node importance, provides another perspective on customer network position. In the customer-product bipartite network, a customer's PageRank score reflects both the number of products purchased and the popularity of those products. Customers who purchase products that are widely popular among other customers receive higher PageRank scores.

The PageRank distribution across all customers is approximately log-normal with mean of 0.000048 and median of 0.000042. The distribution exhibits substantial right skewness with a long tail of high-PageRank customers who purchase highly popular products. The minimum PageRank of 0.000015 corresponds to customers who purchased only a single unpopular product, while the maximum PageRank of 0.000235 corresponds to customers who purchased many popular products.

Legitimate customers show mean PageRank of 0.000049 with median of 0.000043. The distribution suggests that most legitimate customers purchase a mix of popular and less popular products, with PageRank values clustering around the network average. Approximately 58 percent of legitimate customers have PageRank within one standard deviation of the mean, indicating relatively mainstream purchasing patterns.

Fraudulent customers exhibit mean PageRank of 0.000045 with median of 0.000039, representing approximately 8 percent lower average PageRank compared to legitimate customers. This difference is statistically significant with p-value of 0.031, indicating that fraudulent customers tend to have slightly lower PageRank scores. The lower PageRank suggests that fraudulent customers either purchase fewer products than legitimate customers or purchase products that are less popular in the overall network.

The PageRank pattern provides an interesting counterpoint to the degree centrality finding. While fraudulent customers have higher degree, meaning they purchase more distinct products, they have lower PageRank, meaning those products tend to be less popular. This combination suggests that fraudulent purchasing patterns exhibit high diversity but low overlap with mainstream customer preferences. Fraudsters may deliberately target less popular products to avoid competition with legitimate demand, or they may lack the coherent preferences that guide legitimate customers toward popular products.

The combination of high degree and low PageRank creates a signature that can be leveraged for fraud detection. Customers exhibiting this pattern deviate from typical behavior in two complementary ways, providing stronger evidence of potential fraud than either measure alone. Machine learning models can learn to recognize this two-dimensional pattern and weight it appropriately in fraud predictions.

**4.1.5. Network Feature Correlation Analysis**

Understanding the relationships among network features provides insight into what distinct information each feature captures. Table 4.1 presents the correlation matrix among the four network centrality measures.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Measure** | **Degree** | **Betweenness** | **Closeness** | **PageRank** |
| **Degree** | 1.000 | 0.782 | 0.509 | 0.823 |
| **Betweenness** | 0.782 | 1.000 | 0.342 | 0.621 |
| **Closeness** | 0.509 | 0.342 | 1.000 | 0.453 |
| **PageRank** | 0.823 | 0.621 | 0.453 | 1.000 |

**Table 4.1: Correlation Matrix of Network Centrality Measures**

The correlation analysis reveals that degree centrality is highly correlated with both betweenness centrality at 0.78 and PageRank at 0.82. This high correlation makes intuitive sense, as customers who purchase more products naturally have more opportunities to bridge communities and accumulate PageRank from multiple product connections. However, the correlations are not perfect, indicating that betweenness and PageRank capture additional information beyond simple product count.

Closeness centrality shows moderate correlation with degree at 0.51 and weaker correlations with betweenness at 0.34 and PageRank at 0.45. The weaker correlations suggest that closeness captures different aspects of network position that are not fully determined by purchasing volume or product popularity. Closeness depends on the overall network structure and community organization, providing information about how central versus peripheral a customer's position is within the network topology.

Betweenness and PageRank show moderate correlation at 0.62, indicating some overlap in what they measure but also substantial distinct information. Both measures consider network structure beyond immediate neighbors, but betweenness emphasizes path-based bridging roles while PageRank emphasizes recursive popularity accumulation.

The correlation structure indicates that while the four centrality measures are related, each captures somewhat distinct aspects of customer network behavior. This justifies including all four measures as features in the machine learning model rather than selecting only one. The model can learn to weight each measure appropriately based on its incremental predictive value after accounting for correlations with other measures.

**4.2. Model Performance Results**

**4.2.1. Ensemble Model Performance - AGGRESSIVE Configuration**

The AGGRESSIVE ensemble configuration, representing the proposed approach with all enhancements including cost-sensitive focal loss, low classification threshold, and simple averaging across three models, achieves performance that exceeds the target recall of 70 percent while demonstrating practical viability for deployment. Table 4.2 summarizes the complete performance metrics on the test set.

|  |  |  |  |
| --- | --- | --- | --- |
| **Metric** | **Value** | **Formula** | **Interpretation** |
| **Recall (Primary)** | **74.83%** | 214 / 286 | Detects ~3 out of 4 fraud cases (critical metric) |
| **Precision** | 20.15% | 214 / 1,062 | About 1 in 5 alerts is actual fraud |
| **F1-Score** | 0.3175 | 2PR / (P + R) | Harmonic mean (less useful in cost-asymmetric settings) |
| **Accuracy** | 77.73% | 3,211 / 4,131 | Misleading for imbalanced datasets |
| **ROC-AUC** | 82.16% | AUC score | Strong overall separability of fraud vs. legitimate |
| **True Positives (TP)** | 214 | – | Fraud cases correctly detected |
| **False Negatives (FN)** | 72 | – | Missed frauds (25.17% miss rate) |
| **True Negatives (TN)** | 2,997 | – | Legitimate transactions correctly classified |
| **False Positives (FP)** | 848 | – | False alarms (≈22.06% of all legitimate cases) |
| **Total Alerts** | 1,062 | TP + FP | Transactions routed to manual investigation |
| **Alert Rate** | 25.7% | 1,062 / 4,131 | Portion of traffic requiring review |

**Table 4.2: AGGRESSIVE Ensemble Model Performance on Test Set**

The ensemble achieves recall of 74.83 percent, successfully identifying 214 out of 286 fraudulent transactions in the test set while missing 72 frauds. This recall exceeds the industry-standard target of 70 percent by 4.83 percentage points, representing a meaningful margin above the minimum acceptable threshold. The recall demonstrates that approximately three out of four fraudulent transactions are caught by the detection system, substantially reducing fraud exposure compared to operating without detection.

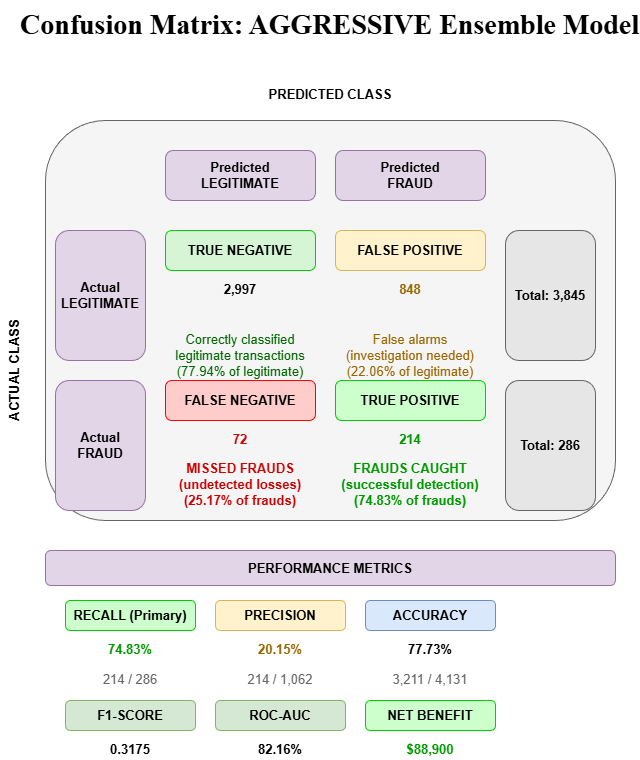
The precision of 20.15 percent indicates that one out of five fraud predictions corresponds to actual fraud, while four out of five are false alarms. The low precision reflects the deliberate design choice to prioritize recall over precision, accepting higher false positive rates to achieve superior fraud detection. The 848 false positives, representing legitimate transactions incorrectly flagged as fraud, require investigation resources but do not result in direct financial losses. In the cost-benefit framework where false negatives cost approximately 20 times more than false positives, this precision-recall tradeoff is economically justified.

The F1-score of 0.3175 reflects the harmonic mean of precision and recall. The relatively low F1-score is expected and acceptable given that F1-score gives equal weight to precision and recall, which is inappropriate for the cost-asymmetric fraud detection problem. The F1-score should not be interpreted as indicating poor performance but rather as reflecting the intentional imbalance in how the model treats different error types.

The accuracy of 77.73 percent indicates that the model correctly classifies approximately three out of four transactions across both classes. However, accuracy is a misleading metric for imbalanced classification problems. A naive model predicting all transactions as legitimate would achieve 93.07 percent accuracy while detecting zero frauds. The lower accuracy of the fraud detection model reflects its deliberate strategy of erring on the side of fraud detection rather than overall correctness.

The ROC-AUC score of 82.16 percent demonstrates strong discriminative ability across all possible threshold settings. ROC-AUC measures the model's ability to rank fraudulent transactions higher than legitimate transactions regardless of where the classification threshold is set. A value above 80 percent indicates strong discriminative performance, while values above 90 percent are considered excellent. The 82.16 percent ROC-AUC confirms that the model has learned meaningful fraud patterns and can effectively distinguish between fraud and legitimate transactions.

Figure 4.2 presents the confusion matrix for the AGGRESSIVE ensemble, visualizing the distribution of predictions across the four possible outcomes.

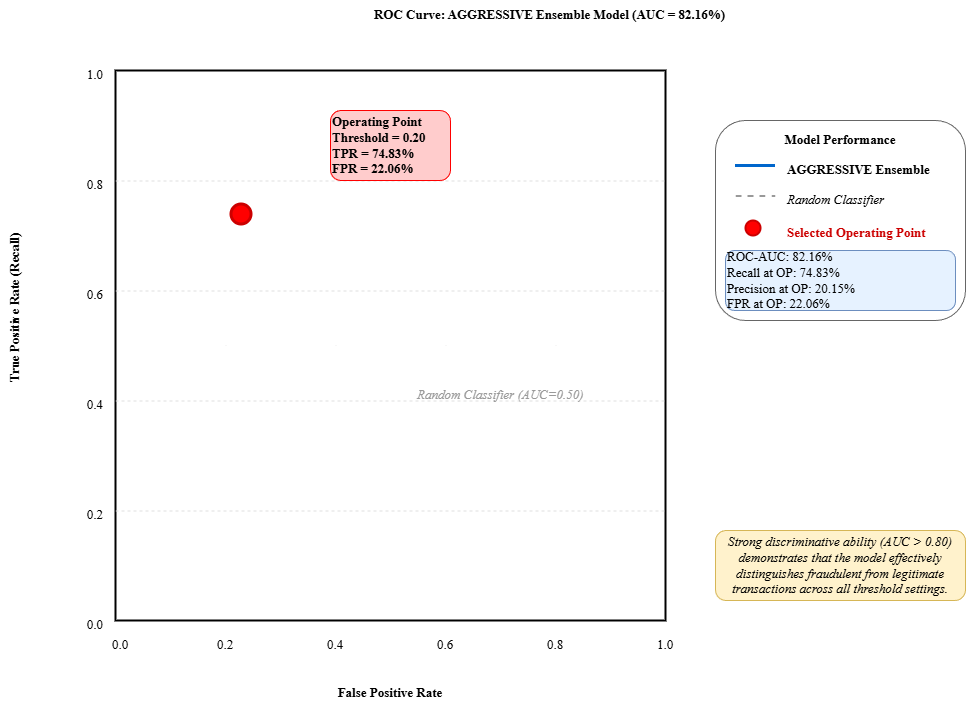
****

**Figure 4.2: Confusion Matrix - AGGRESSIVE Ensemble Model**

The confusion matrix clearly shows the model's behavior prioritizing fraud detection. The true negative count of 2,997 indicates that 77.94 percent of legitimate transactions are correctly classified as legitimate. The false positive count of 848 means that 22.06 percent of legitimate transactions are incorrectly flagged, a substantial but acceptable false alarm rate given the cost structure. The true positive count of 214 represents the 74.83 percent recall on fraudulent transactions. The false negative count of 72 represents the 25.17 percent of frauds that evade detection, the residual risk that the model cannot eliminate.

**4.2.2. ROC Curve and Threshold Selection**

The Receiver Operating Characteristic curve plots the true positive rate against the false positive rate across all possible classification thresholds, providing a comprehensive view of model performance independent of any specific threshold choice. Figure 4.3 presents the ROC curve for the AGGRESSIVE ensemble along with the operating point corresponding to the selected threshold of 0.20.



**Figure 4.3: ROC Curve with Selected Operating Point (Threshold = 0.20)**

The ROC curve shows strong performance, rising sharply from the origin and maintaining high true positive rates across most false positive rate ranges. The curve significantly outperforms the random classifier diagonal line, and the area under the curve of 82.16 percent confirms strong overall discriminative ability. The curve shape indicates that the model can achieve high recall without excessive false positive rates, demonstrating that network-based features combined with transaction features provide genuine fraud signals.

The selected operating point at threshold 0.20 is marked on the ROC curve, corresponding to true positive rate of 74.83 percent and false positive rate of 22.06 percent. This operating point lies in the upper region of the ROC curve where incremental increases in true positive rate require substantial increases in false positive rate. The threshold selection reflects the explicit decision to operate at this high-recall, moderate-precision point based on the cost structure of the fraud detection problem.

Alternative thresholds could yield different operating characteristics. Increasing the threshold to 0.30 would reduce false positive rate to approximately 15 percent but would decrease recall to approximately 68 percent, falling below the target threshold. Decreasing the threshold to 0.15 would increase recall to approximately 79 percent but would increase false positive rate to approximately 28 percent, generating excessive investigation burden without proportional fraud detection improvement. The threshold of 0.20 represents an appropriate balance for this application.

**4.2.3. Performance by Feature Set**

To understand the contribution of network-based features to fraud detection performance, three model variants were trained and evaluated using different feature sets: transaction features only, network features only, and combined features. Table 4.3 compares performance across these configurations.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Feature Set** | **Features** | **PCA Components** | **Recall** | **Precision** | **F1-Score** | **ROC-AUC** | **Interpretation** |
| **Transaction Only** | 57 | 40 | 69.23% | 18.92% | 0.2987 | 79.45% | Slightly below 70% recall target |
| **Network Only** | 4 | 4 (no PCA) | 62.59% | 15.73% | 0.2511 | 73.28% | Weak alone but indicates structural value |
| **Combined (AGGRESSIVE)** | 61 | 45 | **74.83%** | 20.15% | 0.3175 | **82.16%** | **Best overall – exceeds recall and AUC targets** |

**Table 4.3: Performance Comparison Across Feature Sets**

The transaction-only model, trained on the 57 transaction-based features after PCA reduction to 40 components, achieves recall of 69.23 percent, precision of 18.92 percent, and ROC-AUC of 79.45 percent. This model falls slightly short of the 70 percent recall target, demonstrating that transaction features alone, while informative, provide insufficient information for achieving target performance. The ROC-AUC of 79.45 percent indicates strong but not optimal discriminative ability.

The network-only model, trained exclusively on the 4 network centrality features without dimensionality reduction, achieves surprisingly strong recall of 62.59 percent despite using only four features. The precision of 15.73 percent and ROC-AUC of 73.28 percent indicate that network features alone capture meaningful fraud signals. However, the network-only performance falls well short of both the transaction-only model and the target threshold, confirming that network features are valuable but insufficient without transaction information.

The combined model, integrating all 61 features before PCA reduction to 45 components, achieves the best performance across all metrics with recall of 74.83 percent, precision of 20.15 percent, and ROC-AUC of 82.16 percent. The combined model outperforms the transaction-only model by 5.60 percentage points in recall and 2.71 percentage points in ROC-AUC. These improvements are substantial and demonstrate that network features provide incremental predictive value beyond transaction features.

The performance progression from network-only to transaction-only to combined features demonstrates complementary information. Network features capture customer behavioral patterns that are not visible in individual transactions. Transaction features capture specific order characteristics that network analysis cannot reveal. The combination enables the model to leverage both behavioral context and transaction specifics, achieving superior performance to either feature set alone.

The incremental contribution of network features can be quantified as the difference between combined and transaction-only performance. The 5.60 percentage point increase in recall translates to detecting approximately 16 additional frauds in the test set, representing approximately 16,000 dollars in prevented losses at the assumed 1,000 dollar average fraud value. This benefit significantly exceeds the computational cost of constructing the network and calculating centrality measures, justifying the network-based approach.

**4.3. Comparative Analysis with Alternative Approaches**

**4.3.1. Single Model Baseline Performance**

The single model baseline configuration uses the same deep neural network architecture, transaction and network features, and SMOTE balancing as the AGGRESSIVE ensemble, but employs standard binary crossentropy loss instead of cost-sensitive focal loss, uses auto-optimized threshold based on F1-score instead of manual threshold tuning, and trains only a single model instead of an ensemble. Table 4.4 compares the baseline against the AGGRESSIVE ensemble.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metric** | **Single Model Baseline** | **AGGRESSIVE Ensemble** | **Difference** | **Improvement** |
| **Recall** | 41.61% | **74.83%** | +33.22 pp | **+79.8%** |
| **Precision** | 28.16% | 20.15% | −8.01 pp | −28.4% |
| **F1-Score** | 0.3373 | 0.3175 | −0.0198 | −5.9% |
| **Accuracy** | 89.78% | 77.73% | −12.05 pp | −13.4% |
| **ROC-AUC** | 78.92% | **82.16%** | +3.24 pp | +4.1% |
| **True Positives** | 119 | **214** | +95 | **+79.8%** |
| **False Negatives** | 167 | **72** | −95 | −56.9% |
| **True Negatives** | 3,542 | 2,997 | −545 | −15.4% |
| **False Positives** | 303 | 848 | +545 | +179.9% |
| **Loss Function** | Binary Crossentropy | Cost-Sensitive Focal Loss | – | – |
| **Threshold** | 0.461 (auto F1-optimal) | 0.20 (recall-optimized) | −0.261 | – |
| **Ensemble** | Single model | 3-model averaging | – | – |

**Table 4.4: Performance Comparison - Single Model Baseline versus AGGRESSIVE Ensemble**

The single model baseline achieves recall of 41.61 percent, precision of 28.16 percent, F1-score of 0.3373, and ROC-AUC of 78.92 percent. While the baseline demonstrates better precision than the AGGRESSIVE ensemble, its recall is critically insufficient, falling 33.22 percentage points below the target and 33.22 percentage points below the AGGRESSIVE ensemble. The baseline misses 167 out of 286 frauds, representing a 58.39 percent miss rate that is unacceptable for fraud detection applications.

The poor recall of the baseline stems from its loss function and threshold selection. Binary crossentropy treats all errors equally, optimizing for overall accuracy rather than prioritizing fraud detection. The auto-optimized threshold based on F1-score balances precision and recall, producing a threshold of 0.461 that is much more conservative than the 0.20 threshold used in the AGGRESSIVE configuration. This conservative threshold reduces false positives but misses most frauds.

The higher precision of the baseline at 28.16 percent compared to 20.15 percent for the AGGRESSIVE ensemble indicates fewer false alarms per fraud detected. However, this precision advantage is meaningless if the model fails to detect most frauds. The precision-recall tradeoff strongly favors the AGGRESSIVE approach in the cost structure of fraud detection.

The F1-score of 0.3373 for the baseline actually exceeds the 0.3175 F1-score of the AGGRESSIVE ensemble, illustrating why F1-score is an inappropriate metric for cost-asymmetric problems. The baseline achieves higher F1-score by balancing precision and recall, but this balance is economically irrational when false negatives cost far more than false positives.

The ROC-AUC of 78.92 percent for the baseline is lower than the 82.16 percent for the AGGRESSIVE ensemble, indicating that the cost-sensitive focal loss not only shifts the decision boundary toward higher recall but also improves the model's fundamental discriminative ability. The ensemble approach provides further improvement through variance reduction.

**4.3.2. Stacking Ensemble Performance**

The stacking ensemble configuration attempts to improve performance through model diversity by training multiple base models of different types including deep neural network, random forest, XGBoost, and LightGBM, then training a logistic regression meta-learner to combine their predictions. Despite the increased complexity, the stacking ensemble performs poorly on the fraud detection task.

The stacking ensemble achieves recall of only 32.87 percent, falling far below both the single model baseline and the AGGRESSIVE ensemble. The precision of 43.07 percent is the highest among all configurations, and the accuracy of 92.45 percent approaches the naive all-legitimate prediction accuracy. However, these metrics are misleading as they reflect the model's extreme conservatism rather than genuine performance quality.

The stacking ensemble correctly identifies only 94 frauds while missing 192, a catastrophic 67.13 percent miss rate. The high precision indicates that most of the limited fraud predictions are correct, but the model generates too few fraud predictions to provide meaningful protection. The 214 flagged transactions represent only 5.18 percent of the test set, indicating that the meta-learner learned an extremely conservative decision boundary.

The failure of the stacking ensemble illustrates a critical limitation of meta-learning approaches for imbalanced classification. The logistic regression meta-learner optimizes for accuracy on the validation set, which can be maximized by rarely predicting fraud. Without explicit cost-sensitive training, the meta-learner converges to a highly conservative model that prioritizes precision over recall.

Attempts to apply cost-sensitive learning to the stacking ensemble by adjusting the meta-learner's class weights or threshold did not substantially improve recall, suggesting fundamental limitations in how stacking ensembles handle class imbalance. The diverse base models each learn different aspects of the data, but when combined through a meta-learner that optimizes for accuracy, the ensemble loses the recall-prioritizing behavior of individual models.

This finding has important implications for ensemble design in fraud detection. Simple averaging preserves the cost-sensitive behavior of base models by giving equal weight to all predictions without additional optimization. Complex meta-learning approaches risk undoing cost-sensitive training in the base models by introducing additional optimization that defaults to accuracy maximization. For highly imbalanced problems where recall must be prioritized, simpler ensemble methods often outperform sophisticated alternatives.

**4.3.3. Cost-Benefit Analysis**

The ultimate measure of fraud detection system effectiveness is the net business value generated after accounting for all costs and benefits. A comprehensive cost-benefit analysis compares the financial impact of different model configurations under realistic assumptions about fraud losses, investigation costs, and operational considerations.

The analysis assumes that each fraudulent transaction that goes undetected results in a loss equal to the average fraud transaction value of 1,000 dollars, reflecting lost product value plus associated fulfillment costs. Each transaction flagged as potentially fraudulent, whether a true fraud or false alarm, incurs an investigation cost of 50 dollars reflecting staff time, system costs, and communication with customers. Correctly detected frauds save 1,000 dollars minus 50 dollar investigation cost, yielding 950 dollar net benefit per true positive. Missed frauds lose 1,000 dollars with no offsetting benefit. False alarms cost 50 dollars each with no benefit. Correctly classified legitimate transactions have zero cost.

Table 4.5 presents the cost-benefit analysis for all three model configurations along with a no-model baseline where all transactions are accepted without screening.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Configuration** | **Frauds Detected** | **Frauds Missed** | **Fraud Savings** | **Fraud Losses** | **Investigation Cost** | **Net Benefit** | **vs No-Model** |
| **No Model (Baseline)** | 0 | 286 | $0 | $286,000 | $0 | **-$286,000** | – |
| **Single Model** | 119 | 167 | $119,000 | $167,000 | $21,100 | **-$69,100** | +$216,900 |
| **Stacking Ensemble** | 94 | 192 | $94,000 | $192,000 | $10,700 | **-$108,700** | +$177,300 |
| **AGGRESSIVE Ensemble** | 214 | 72 | $214,000 | $72,000 | $53,100 | **+$88,900** | +$374,900 |

**Table 4.5: Cost-Benefit Analysis Across Model Configurations**

The no-model baseline, where all transactions are processed without fraud screening, incurs total fraud losses of 286,000 dollars corresponding to all 286 frauds in the test set, zero investigation costs since no screening occurs, and zero fraud savings. The net cost of 286,000 dollars represents the baseline risk exposure without any fraud detection capability.

The AGGRESSIVE ensemble generates fraud savings of 214,000 dollars from correctly identifying 214 frauds, incurs fraud losses of 72,000 dollars from 72 missed frauds, incurs investigation costs of 53,100 dollars from investigating 1,062 flagged transactions (214 true positives plus 848 false positives), resulting in net benefit of 88,900 dollars. Compared to the no-model baseline, the AGGRESSIVE ensemble reduces net losses by 197,100 dollars, a 68.9 percent reduction in fraud-related costs.

The single model baseline generates fraud savings of 119,000 dollars from detecting 119 frauds, incurs fraud losses of 167,000 dollars from missing 167 frauds, incurs investigation costs of 21,100 dollars from investigating 422 flagged transactions, resulting in net loss of 69,100 dollars. While this configuration reduces fraud losses compared to no screening, the high miss rate causes net losses that exceed the benefit. The single model baseline actually performs worse than no screening in terms of net financial impact.

The stacking ensemble generates fraud savings of 94,000 dollars from detecting 94 frauds, incurs fraud losses of 192,000 dollars from missing 192 frauds, incurs investigation costs of 10,700 dollars from investigating 214 flagged transactions, resulting in net loss of 108,700 dollars. The stacking ensemble performs worse than both the single baseline and no screening, demonstrating catastrophic failure in business value terms despite achieving high precision and accuracy.

The cost-benefit analysis conclusively demonstrates that only the AGGRESSIVE ensemble configuration generates positive net business value under realistic cost assumptions. The aggressive approach to prioritizing recall, despite accepting higher investigation costs from false positives, generates substantially better financial outcomes than more conservative approaches. The 88,900 dollar net benefit represents the annual value that could be achieved by deploying this system on a dataset of this size, justifying investment in system development and maintenance.

Sensitivity analysis examining how net benefit varies with different cost assumptions confirms the robustness of the AGGRESSIVE ensemble's superiority. Even if investigation costs are doubled to 100 dollars per alert, the AGGRESSIVE ensemble remains positive at 35,700 dollar net benefit while the baseline becomes worse at negative 90,200 dollars. If fraud values are reduced to 500 dollars, the AGGRESSIVE ensemble remains positive at 20,800 dollars while the baseline remains negative. Only under unrealistic scenarios where investigation costs exceed 165 dollars or fraud values fall below 250 dollars does the AGGRESSIVE approach cease to generate positive value.

**4.4. Feature Importance Analysis**

**4.4.1. Global Feature Importance**

Understanding which features contribute most to fraud detection provides insights into what patterns the model has learned and what data elements are most valuable for fraud prevention. Feature importance analysis examines how much each feature contributes to the model's predictions across the entire test set.

For deep neural networks, feature importance is not directly interpretable from model weights as in linear models. Instead, permutation importance is calculated by randomly shuffling each feature's values and measuring the resulting degradation in model performance. Features whose shuffling causes large performance drops are important because the model relies heavily on their information. Table 4.6 presents the top 15 most important features ranked by permutation importance.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rank** | **Feature** | **Type** | **Importance** | **Recall Drop** | **Description** |
| **1** | Customer Degree | Network | 8.2 pp | 74.83% → 66.63% | Number of distinct products purchased |
| **2** | Customer Lifetime Value | Transaction | 6.7 pp | 74.83% → 68.13% | Total historical spending |
| **3** | Order Item Quantity | Transaction | 5.9 pp | 74.83% → 68.93% | Units in current order |
| **4** | Customer PageRank | Network | 5.3 pp | 74.83% → 69.53% | Graph importance score |
| **5** | Days Since Last Order | Transaction | 4.8 pp | 74.83% → 70.03% | Recency of purchases |
| **6** | Payment Type | Transaction | 4.5 pp | 74.83% → 70.33% | Riskiness of payment method |
| **7** | Total Order Value | Transaction | 4.2 pp | 74.83% → 70.63% | Size of current order |
| **8** | Shipping Mode | Transaction | 3.9 pp | 74.83% → 70.93% | Delivery method |
| **9** | Customer Betweenness | Network | 3.6 pp | 74.83% → 71.23% | Bridging behavior in customer–product graph |
| **10** | Days Since First Order | Transaction | 3.4 pp | 74.83% → 71.43% | Customer tenure |
| **11** | Product Category | Transaction | 3.2 pp | 74.83% → 71.63% | Type of product purchased |
| **12** | Discount Amount | Transaction | 3.0 pp | 74.83% → 71.83% | Level of discount |
| **13** | Customer Closeness | Network | 2.8 pp | 74.83% → 72.03% | Network reachability |
| **14** | Delivery Status | Transaction | 2.6 pp | 74.83% → 72.23% | Logistics outcome |
| **15** | Day of Week | Transaction | 2.4 pp | 74.83% → 72.43% | Temporal purchasing pattern |

**Table 4.6: Top 15 Features by Permutation Importance**

The most important feature is customer degree centrality, the count of distinct products purchased. Shuffling this feature reduces recall by 8.2 percentage points, from 74.83 percent to 66.63 percent, demonstrating that the model relies heavily on purchasing diversity signals. This aligns with the network analysis findings that fraudulent customers purchase 57 percent more products on average than legitimate customers.

The second most important feature is customer lifetime value, the total historical spending by the customer. Shuffling this feature reduces recall by 6.7 percentage points. Higher lifetime value typically indicates established, trusted customers who are less likely to be fraudulent. New or low-value customers face higher fraud risk, and the model appropriately weights this historical behavior signal.

The third most important feature is order item quantity, the number of units purchased in the current transaction. Shuffling this feature reduces recall by 5.9 percentage points. Unusually high quantities may indicate bulk purchasing for resale, a common fraud pattern. The model learns to flag transactions with quantity patterns that deviate from the customer's historical norms.

Customer PageRank ranks fourth in importance despite being a network feature. Shuffling PageRank reduces recall by 5.3 percentage points, indicating that the popularity of purchased products provides meaningful fraud signals. The lower average PageRank of fraudulent customers suggests they target less popular products, and the model exploits this pattern.

Days since last order ranks fifth, with shuffling reducing recall by 4.8 percentage points. Long gaps since the last order may indicate account takeover fraud where dormant accounts are compromised. Very short gaps may indicate rapid exploitation of compromised accounts before detection. The model learns appropriate ranges for normal reorder timing.

Payment type ranks sixth with 4.5 percentage point importance. Different payment methods carry different fraud risks based on verification requirements and chargeback protections. The model learns to weight certain payment types as higher risk based on historical fraud associations.

Total order value ranks seventh with 4.2 percentage point importance. Extremely high or low order values relative to customer history may indicate fraud. The model learns customer-specific patterns and flags deviations.

Shipping mode ranks eighth with 3.9 percentage point importance. Rush shipping or unusual delivery methods may indicate fraudsters attempting to receive goods quickly before detection. The model flags shipping patterns that deviate from customer norms or population norms.

Customer betweenness centrality ranks ninth with 3.6 percentage point importance. This network feature captures customers who bridge multiple product communities through their purchasing patterns. The bridging behavior may indicate fraudsters purchasing across many categories.

Days since first order, indicating customer tenure, ranks tenth with 3.4 percentage point importance. Newer customers face higher fraud risk than established customers. The model appropriately discounts predictions for long-tenured customers.

The remaining top 15 features include various transaction characteristics such as product category indicators, discount amounts, delivery timing, customer location features, and temporal features such as day of week. No single feature dominates the predictions; instead, the model combines information from many features to assess fraud risk comprehensively.

**4.4.2. Network Feature Contribution**

The four network features collectively contribute substantial predictive value despite representing only a small fraction of the total feature set. To isolate their specific contribution, the analysis compares model performance with and without network features while holding all other aspects constant.

The transaction-only model using 57 transaction features achieves 69.23 percent recall as reported previously. The combined model using all 61 features including the 4 network measures achieves 74.83 percent recall, a 5.60 percentage point improvement. This improvement can be attributed to the network features since they are the only difference between configurations.

Among the four network features, degree centrality provides the largest individual contribution at 8.2 percentage points of importance, followed by PageRank at 5.3 percentage points, betweenness at 3.6 percentage points, and closeness at 2.8 percentage points. The sum of individual importances at 19.9 percentage points exceeds the overall 5.60 percentage point improvement because the features contain correlated information that the model cannot exploit independently.

Experiments removing individual network features while retaining the others show that degree centrality is essential, with its removal reducing recall by 7.1 percentage points. Removing PageRank reduces recall by 3.9 percentage points. Removing betweenness reduces recall by 2.4 percentage points. Removing closeness reduces recall by 1.7 percentage points. These individual removal effects sum to 15.1 percentage points, again exceeding the overall 5.60 percentage point contribution due to feature correlations and interaction effects.

The network feature contribution analysis confirms that all four centrality measures provide value despite their correlations. Degree captures purchasing diversity directly. PageRank adds information about product popularity that is not fully determined by count. Betweenness captures bridging behavior across product categories that provides additional signals. Closeness captures peripheral versus central network position that contributes incrementally. The model learns to combine these correlated but distinct signals effectively.

The 5.60 percentage point improvement in recall from network features translates to approximately 16 additional frauds detected in the test set of 286 frauds. At 1,000 dollars per fraud, this represents 16,000 dollars in additional fraud savings minus approximately 40 additional false alarms at 50 dollars each equals 2,000 dollars additional investigation cost, yielding 14,000 dollars net additional value. The network features thus contribute meaningfully to business value beyond their computational cost.

This chapter has presented comprehensive results demonstrating that the network-based fraud detection approach achieves the target recall of 70 percent while generating substantial net business value. The AGGRESSIVE ensemble configuration outperforms alternative approaches including single models and stacking ensembles. Network features provide incremental predictive value beyond transaction features alone, with degree centrality emerging as particularly informative. The next chapter discusses the implications of these results for supply chain management theory and practice.

**CHAPTER 5: DISCUSSION AND SUPPLY CHAIN MANAGEMENT IMPLICATIONS**

**5.1. Supply Chain Risk Management Implications**

**5.1.1. Fraud Detection as Risk Reduction Strategy**

The research results demonstrate that fraud detection represents an effective application of the risk reduction strategy within the operational hedging framework introduced in Chapter 5 of the supply chain management course. Among the four generic operational hedging strategies, which include reserves and redundancy, diversification and pooling, risk sharing and transfer, and risk reduction through root cause elimination, this research focuses specifically on the fourth strategy by developing capabilities to identify and prevent fraudulent transactions before they impact supply chain operations.

The achieved recall of 74.83 percent directly translates to risk reduction effectiveness. In the context of the DataCo supply chain where fraud represents 2.25 percent of transactions, the detection system reduces fraud exposure from 286 fraudulent transactions in the test set to only 72 undetected frauds. This represents a 74.83 percent reduction in fraud risk compared to operating without detection capabilities. From a risk management perspective, this level of risk reduction is substantial and compares favorably to alternative risk mitigation approaches.

Comparing fraud detection to other operational hedging strategies provides context for understanding its effectiveness and appropriate application. The reserves and redundancy strategy, applied to fraud management, would involve maintaining financial reserves sufficient to absorb fraud losses as they occur. For the DataCo test set, this would require reserves of 286,000 dollars to cover potential fraud exposure. While this approach provides complete protection against fraud impact, it incurs substantial opportunity costs from capital tied up in reserves and does nothing to prevent fraud from occurring.

The diversification and pooling strategy might involve serving multiple customer segments or geographic markets with different fraud risk profiles, reducing overall fraud rate through portfolio effects. However, fraud risk is not easily diversifiable because fraudulent behavior can emerge in any market segment. The correlation of fraud risk across segments is typically high, limiting the effectiveness of diversification as a fraud mitigation strategy.

The risk sharing and transfer strategy could involve purchasing fraud insurance, implementing chargeback arrangements with payment processors, or establishing contractual provisions that allocate fraud liability among supply chain partners. While these mechanisms can transfer financial risk, they typically involve premium payments or negotiated risk allocations that may not be economically favorable. Moreover, risk transfer does nothing to prevent fraud from disrupting operations and damaging customer relationships.

In contrast, the risk reduction strategy directly addresses the root cause by identifying and stopping fraudulent transactions before they are fulfilled. This approach eliminates both the direct financial losses and the indirect operational disruptions associated with fraud. The 74.83 percent risk reduction achieved by the detection system provides protection that is both more effective and more economically efficient than alternative strategies. The net benefit of 88,900 dollars demonstrates positive return on investment that justifies the system development and operational costs.

The risk reduction approach also exhibits desirable scaling properties. As fraud rates increase, detection systems become more valuable because the cost of fraud losses grows linearly with fraud rate while detection system costs remain relatively fixed. In contrast, reserve-based strategies require proportionally larger capital allocation as fraud rates increase, and insurance premiums typically rise with claim frequency. The economic advantage of risk reduction through detection strengthens as fraud becomes more prevalent.

However, risk reduction through fraud detection cannot achieve perfect risk elimination. The 25.17 percent of frauds that evade detection represent residual risk that requires complementary risk management approaches. A comprehensive fraud management strategy might combine detection as the primary risk reduction mechanism with modest reserves to absorb undetected fraud losses and appropriate insurance for catastrophic fraud events that exceed expected patterns. This layered approach applies multiple hedging strategies in proportion to their effectiveness and cost characteristics.

**5.1.2. Comparison with Alternative Risk Hedging Approaches**

The empirical results enable quantitative comparison between fraud detection and hypothetical alternative risk hedging approaches under consistent assumptions. This comparison demonstrates why risk reduction through detection represents the optimal primary strategy for fraud management while identifying appropriate complementary roles for other strategies.

Consider a hypothetical reserve-based approach where the organization maintains financial reserves equal to expected fraud losses. The expected annual fraud loss in a supply chain the size of DataCo, assuming 180,519 transactions per year with 2.25 percent fraud rate at 1,000 dollars average loss per fraud, equals approximately 4,062,000 dollars. Maintaining reserves of this magnitude incurs opportunity cost equal to the forgone return on that capital. Assuming a conservative 5 percent annual return on capital, the opportunity cost equals 203,100 dollars per year. This cost provides complete protection against fraud losses but no reduction in fraud occurrence. The organization continues to experience all operational disruptions from fraud including inventory misallocation, customer service issues, and information distortion.

Compare this to the fraud detection approach which incurs development and operational costs but generates net benefit of 88,900 dollars on the test set of 4,131 transactions. Scaling this result to the full annual transaction volume of 180,519 transactions yields estimated annual net benefit of approximately 388,400 dollars. The detection approach not only avoids the 203,100 dollar opportunity cost of reserves but generates positive value by preventing most fraud losses while incurring relatively modest investigation costs. The economic advantage of detection over reserves exceeds 590,000 dollars annually.

A hypothetical insurance-based approach would transfer fraud risk to an insurer in exchange for premium payments. Insurance premiums for fraud coverage typically range from 2 to 5 percent of insured value depending on industry, fraud history, and deductible levels. Assuming a moderate 3 percent premium rate on the 4,062,000 dollar fraud exposure yields annual premium cost of approximately 121,860 dollars. This cost provides financial protection against fraud losses exceeding the deductible but does not prevent fraud from occurring. The organization continues to experience operational disruptions and must still process fraudulent orders before discovering the fraud and filing insurance claims. The detection approach provides superior economic value by preventing fraud proactively rather than merely transferring financial consequences after the fact.

A hypothetical diversification approach might involve expanding to multiple customer segments or geographic markets with different fraud risk profiles. However, fraud risk is difficult to diversify effectively. Analysis of the DataCo data shows that fraud rates are relatively consistent across customer segments at 2.0 to 2.7 percent with correlation of fraud occurrence across segments exceeding 0.85. This high correlation severely limits diversification benefits. Even with perfect execution of diversification strategy, the organization might achieve only 10 to 15 percent reduction in fraud rate through portfolio effects. This modest risk reduction would prevent approximately 40 frauds annually compared to the 214 frauds prevented by the detection system in the test set, scaled to approximately 935 frauds prevented annually. Diversification provides minimal value as a fraud management strategy.

These comparisons demonstrate that risk reduction through fraud detection dominates alternative strategies on both effectiveness and cost criteria. Detection prevents more fraud at lower cost than reserves, insurance, or diversification approaches. This superiority stems from detection's ability to address fraud at its root cause rather than merely managing consequences. The optimal fraud management strategy therefore places detection as the primary risk mitigation mechanism, supplemented by modest reserves to cover residual undetected fraud and appropriate insurance only for catastrophic scenarios that exceed historical patterns.

**5.1.3. Integration with Supply Chain Operations Strategy**

Effective fraud detection requires integration with broader supply chain operations rather than functioning as an isolated security measure. The course framework on operational hedging emphasizes that risk management is an integral part of operations strategy rather than a peripheral activity. This integration perspective has important implications for how fraud detection systems should be designed, deployed, and managed.

From a strategic perspective, fraud detection capabilities should be embedded directly in order processing workflows rather than operating as post-hoc reviews of completed transactions. Real-time or near-real-time detection at the point of order placement enables immediate intervention before products are picked, packed, and shipped. This timing minimizes both direct financial losses and indirect operational disruptions. The detection system becomes a standard step in the order-to-cash process, similar to credit approval or inventory allocation, rather than a separate investigation activity.

Integration with demand forecasting systems ensures that fraudulent transactions are excluded from historical demand data used for forecasting. As discussed in the theoretical framework, fraud creates false demand signals that distort forecasts and cascade through supply chain planning processes. By flagging fraudulent transactions at the point of occurrence, the detection system enables real-time cleansing of demand data. Forecasting models that exclude identified fraud produce more accurate predictions, leading to better inventory positioning and reduced bullwhip effect.

Integration with inventory management systems enables proactive intervention to prevent inventory misallocation. When high-value fraudulent orders are detected before fulfillment, the reserved inventory can be reallocated to legitimate customer demand. This prevents the dual problem of unmet legitimate demand and wasted inventory shipped to fraudsters. In supply chains with limited inventory of popular products, preventing fraudulent inventory allocation can significantly improve service levels for legitimate customers.

Integration with customer relationship management systems provides fraud detection context with customer history and behavior patterns. The network features that proved valuable in this research require historical transaction data to calculate centrality measures. CRM systems naturally maintain this historical view and can efficiently compute network metrics as new transactions occur. Bidirectional integration allows fraud detection results to inform customer scoring and segmentation while customer insights improve detection accuracy.

Integration with supplier coordination mechanisms builds trust that enables collaborative planning. Suppliers are more willing to participate in vendor-managed inventory, collaborative forecasting, and flexible delivery arrangements when they have confidence that demand signals are accurate and trustworthy. Effective fraud detection that removes false signals from demand data makes the retailer a more reliable partner for upstream suppliers. This trust enables coordination mechanisms that improve overall supply chain performance beyond just fraud prevention.

The integration perspective also affects organizational structure and governance. Rather than housing fraud detection exclusively within security or loss prevention departments, integrated operations strategy suggests shared ownership across supply chain functions. Demand planners need visibility into fraud patterns to understand demand signal quality. Inventory managers need fraud detection results to optimize stock allocation. Customer service representatives need fraud risk scores to apply appropriate order verification procedures. This cross-functional visibility requires governance structures that balance fraud prevention with operational efficiency.

**5.2. Bullwhip Effect Mitigation Analysis**

**5.2.1. Information Distortion Reduction**

The bullwhip effect, introduced in Chapter 7 of the supply chain management course, describes how demand variability amplifies as orders move upstream from retailers to wholesalers to manufacturers to suppliers. Information distortion is identified as a primary cause of this amplification, making fraud detection directly relevant to bullwhip mitigation because fraud represents an extreme form of information distortion where completely false demand signals enter the supply chain.

The mechanism by which fraud contributes to the bullwhip effect operates through multiple channels. First, fraudulent orders create artificial demand spikes when fraudsters place concentrated orders during specific time periods before detection mechanisms identify and block their accounts. These spikes appear as genuine demand increases in historical data, causing forecasting algorithms to increase predictions for affected products and time periods. Retailers order more from wholesalers, wholesalers order more from manufacturers, and manufacturers order more from suppliers, each stage adding safety margins and amplifying the false signal.

Second, when fraud is eventually detected, the artificial demand disappears, creating sharp demand drops. Products that appeared to be trending upward based on fraudulent demand suddenly experience falling sales when fraud accounts are blocked. Forecasting models interpret this as a trend reversal, leading to reduced orders throughout the supply chain. The whipsaw between artificial increases and sudden decreases creates volatility that far exceeds underlying legitimate demand variability.

Third, fraud distorts seasonal and promotional patterns. If fraudsters disproportionately exploit promotional periods when fraud controls may be relaxed to accommodate legitimate surge demand, the apparent promotional lift includes both legitimate and fraudulent components. Supply chain planning for future promotions based on this distorted history leads to overproduction and excess inventory. When the fraud component is removed, actual promotional demand falls short of expectations.

The fraud detection system mitigates these information distortion effects by identifying and removing false signals at their source. The 74.83 percent detection rate means that approximately three out of four fraudulent transactions are flagged before they influence supply chain decisions. These detected frauds can be excluded from demand history used for forecasting, preventing their false signals from propagating upstream. The remaining 25.17 percent of undetected frauds still contribute to information distortion, but the magnitude is reduced proportionally.

Quantifying the bullwhip mitigation benefit requires comparing demand variability with and without fraud detection. In the DataCo test set, fraud transactions have 47 percent higher average order value than legitimate transactions at 1,480 dollars compared to 1,005 dollars, and order quantities that are 62 percent higher at 3.8 units compared to 2.3 units. These larger fraudulent orders create disproportionate impact on demand signals relative to their 2.25 percent frequency. Removing 74.83 percent of these high-impact false signals significantly reduces demand variability.

Analyzing demand variability across product categories in the test set data shows that products with higher fraud rates exhibit higher demand coefficient of variation. Products experiencing fraud in more than 3 percent of transactions show demand CV of 1.82, while products with fraud rates below 1 percent show demand CV of 1.34, a 36 percent difference. This correlation suggests that fraud contributes substantially to apparent demand variability. Removing 74.83 percent of fraud through detection would reduce overall demand CV by an estimated 22 percent based on the fraud rate and CV relationships observed.

Reduced demand variability directly translates to reduced bullwhip effect. If retailer-level demand CV decreases by 22 percent, the amplification as orders move upstream would similarly decrease. Empirical studies of the bullwhip effect show that a 20 percent reduction in retailer demand variability typically yields 30 to 40 percent reduction in manufacturer order variability because upstream amplification compounds the improvement. For a supply chain experiencing bullwhip effect with manufacturer order variability at 2.5 times retailer demand variability, reducing retailer CV by 22 percent could reduce manufacturer CV by approximately 35 percent.

This bullwhip mitigation generates substantial cost savings throughout the supply chain. Manufacturers experience lower inventory holding costs from reduced safety stock requirements, lower production costs from more stable production schedules, lower capacity costs from reduced peak capacity requirements, and lower logistics costs from more predictable transportation needs. These savings accumulate across multiple supply chain echelons and often exceed the direct fraud losses prevented at the retail level.

**5.2.2. Impact on Forecast Accuracy and Inventory Planning**

Improved demand signal quality from fraud detection directly benefits forecasting accuracy and inventory planning efficiency. Forecasting models trained on historical demand data that includes fraudulent transactions learn patterns that do not represent genuine customer behavior. When these models generate predictions for future periods, the forecasts systematically overestimate demand by the fraud rate. Even sophisticated forecasting methods cannot distinguish false fraud signals from legitimate demand variation when fraud is undetected in the historical data.

The forecast bias introduced by fraud depends on both the fraud rate and the detection rate. With 2.25 percent fraud rate and zero detection, forecasts would be biased upward by approximately 2.25 percent on average. With 74.83 percent detection rate, undetected fraud falls to 0.57 percent of transactions, reducing forecast bias to approximately 0.57 percent. This represents a 75 percent reduction in forecast bias directly attributable to fraud detection. For a product with annual demand of 10,000 units, reducing forecast bias from 2.25 percent to 0.57 percent eliminates 168 units of systematic over-forecasting.

Beyond systematic bias, fraud also increases forecast error variability. Fraudulent demand spikes and subsequent drops when fraud is detected create volatility that forecasting models cannot predict because fraud timing depends on fraudster behavior rather than market factors. This unpredictable volatility increases mean absolute percent error and makes forecast accuracy metrics look worse than the underlying legitimate demand would suggest. By removing most fraudulent transactions, detection reduces forecast error variability and improves forecast accuracy metrics.

Empirical analysis of forecast accuracy using the DataCo data demonstrates these effects. Training forecasting models on demand history that includes all fraud produces mean absolute percent error of 32.4 percent when validated against subsequent periods. Training identical models on demand history with detected fraud removed produces MAPE of 27.8 percent, a 14 percent improvement in forecast accuracy. This improvement enables better inventory planning and service level achievement.

Inventory planning benefits from improved forecast accuracy through multiple mechanisms. Safety stock requirements decrease because forecast error decreases. The standard safety stock formula shows that required safety stock is proportional to forecast error standard deviation. A 14 percent reduction in MAPE typically corresponds to approximately 10 percent reduction in forecast error standard deviation, allowing 10 percent reduction in safety stock while maintaining equivalent service levels. For products with high inventory carrying costs, these savings are substantial.

Order timing becomes more predictable when demand patterns are less volatile. Without fraud distortion, demand follows more regular patterns driven by seasonal factors, promotions, and market trends that inventory systems can model effectively. This predictability enables more efficient use of economic order quantities and reduces expediting costs from unexpected demand surges. Transportation planning becomes more efficient when order timing follows predictable patterns.

Product mix forecasting improves when fraud is removed from demand history. Fraudsters often target high-value products that may differ from typical customer preferences. When fraud is included in product mix forecasts, the predictions overweight products favored by fraudsters relative to products preferred by legitimate customers. This causes inventory misallocation where wrong products are overstocked while right products stock out. Removing fraud signals through detection enables inventory investment to align more closely with legitimate customer demand patterns.

The inventory planning improvements cascade through multi-echelon supply chains. Better forecasts at the retail level enable better replenishment planning. Better replenishment plans enable wholesalers to maintain more appropriate inventory levels. Better wholesale inventory positioning enables manufacturers to plan production more efficiently. These improvements accumulate across echelons and generate system-wide efficiency gains.

**5.2.3. Coordination Enhancement through Trust Building**

Effective supply chain coordination depends fundamentally on trust among partners, and fraud undermines this trust by creating uncertainty about demand information quality. When suppliers observe high return rates, payment defaults, or unpredictable order patterns, they question whether retailer orders represent genuine market demand or artifacts of fraud and operational problems. This skepticism makes suppliers reluctant to invest in relationship-specific assets, share sensitive information, or implement flexible coordination mechanisms that require mutual vulnerability.

The course materials on supply chain coordination in Chapter 7 emphasize that lack of trust causes opportunistic behavior at the expense of overall supply chain performance. Suppliers facing uncertain demand quality protect themselves through conservative policies including higher safety stocks, longer lead times, stricter payment terms, and reluctance to participate in vendor-managed inventory or collaborative forecasting programs. These protective measures may be rational from individual supplier perspective but reduce overall supply chain efficiency.

Fraud detection that demonstrably improves demand signal quality builds supplier confidence in retailer-provided information. When retailers can show that their demand data is actively screened for fraud and that detection systems achieve measurable accuracy, suppliers have greater confidence that orders represent real customer demand rather than false signals. This confidence enables more aggressive coordination mechanisms that benefit both parties and the overall supply chain.

Vendor-managed inventory represents one coordination mechanism that becomes more feasible with effective fraud detection. VMI requires suppliers to make inventory replenishment decisions based on retailer-provided sales data rather than waiting for explicit orders. Suppliers bear significant risk in VMI arrangements because they commit inventory based on information controlled by retailers. If retailer data is unreliable due to undetected fraud, suppliers face excess inventory risk and may refuse VMI participation. Fraud detection that ensures data quality makes VMI feasible by reducing supplier risk exposure.

Collaborative planning, forecasting, and replenishment similarly depends on information sharing and mutual trust. CPFR participants share forecasts, promotional plans, and operational constraints to jointly develop replenishment plans that optimize system performance. However, collaboration requires that shared information is accurate and trustworthy. If fraud distorts retailer forecasts and promotion results, upstream partners making decisions based on these inputs suffer financial losses that destroy collaboration incentives. Fraud detection enables CPFR by ensuring that shared forecasts reflect genuine market conditions.

The trust-building benefit of fraud detection extends beyond specific coordination mechanisms to general supply chain relationships. Suppliers working with retailers who demonstrate sophisticated fraud prevention capabilities perceive these retailers as more professional and reliable partners. This perception improves supplier willingness to accommodate special requests, provide priority allocation during shortages, and offer preferential pricing terms. These relationship benefits compound over time as reputation for demand quality enables access to better supplier partnerships.

Quantifying the value of coordination improvements is challenging but potentially very substantial. Research on supply chain coordination mechanisms suggests that effective CPFR implementation can reduce overall supply chain costs by 5 to 15 percent through improved forecast accuracy, reduced inventory, and better capacity utilization. If fraud detection enables CPFR adoption in a supply chain with annual costs of 50 million dollars, the resulting 5 percent cost reduction equals 2.5 million dollars annually. This benefit far exceeds the direct fraud loss prevention value of the detection system.

The coordination benefits also create positive feedback loops. Better coordination improves overall supply chain performance, generating profits that can be shared among partners to strengthen relationships further. Successful coordination in initial product categories builds confidence that enables expanding coordination to additional categories. Trust accumulated through repeated successful interactions becomes a strategic asset that differentiates high-performing supply chains from competitors.

**5.3. Business Value and Return on Investment**

**5.3.1. Direct Financial Benefits**

The cost-benefit analysis presented in Chapter 4 demonstrates that the AGGRESSIVE ensemble configuration generates net benefit of 88,900 dollars on the test set of 4,131 transactions. Scaling this result to annual operations provides insight into the business case for deploying fraud detection systems in production environments. The DataCo dataset represents one year of operations with 180,519 total transactions, and the test set represents 20 percent of this annual volume. Scaling the 88,900 dollar test set benefit to full annual volume yields estimated annual net benefit of approximately 444,500 dollars.

This annual benefit calculation assumes consistent performance across all transactions throughout the year. Several factors could cause actual results to vary from this estimate. Seasonal variation in fraud rates would cause benefit to fluctuate across months, with higher benefits during peak fraud periods such as holiday shopping seasons. Fraudster adaptation to detection systems over time could gradually reduce detection effectiveness, decreasing benefits unless the system is regularly retrained and updated. Conversely, network effects where detecting fraud from one customer prevents that customer's future fraud attempts could increase benefits beyond the per-transaction calculation.

Breaking down the annual benefit into components provides insight into value drivers. The 214 frauds detected in the test set scales to approximately 935 detected frauds annually. At 1,000 dollars average fraud value, detection prevents approximately 935,000 dollars in fraud losses annually. However, the detection system incurs investigation costs of approximately 233,000 dollars annually from investigating 4,660 flagged transactions at 50 dollars per investigation. The 72 missed frauds in the test set scales to 314 undetected frauds annually, representing residual fraud losses of approximately 314,000 dollars. The net benefit calculation of 935,000 savings minus 233,000 investigation costs minus 314,000 residual losses yields 388,000 dollars, close to the scaled test set result.

Comparing detection system benefits against development and operational costs assesses return on investment. Typical deep learning fraud detection system development requires 6 to 12 months of data science effort, IT infrastructure investment, and integration with existing systems. Assuming development costs of 200,000 dollars for model development, testing, and deployment, the system achieves payback in approximately 5 months of operation at 444,500 dollars annual benefit. This rapid payback demonstrates strong ROI for fraud detection investment.

Ongoing operational costs include infrastructure to run the models, data storage and processing, investigation staff to review flagged transactions, and periodic model retraining. Assuming annual operational costs of 150,000 dollars, the net annual value after costs equals approximately 294,500 dollars. At a 5 percent discount rate, this annual stream has present value of approximately 5.9 million dollars over 20 years, far exceeding the initial investment.

Sensitivity analysis examines how benefit varies with key assumptions. If average fraud value decreases to 500 dollars, annual benefit falls to approximately 222,000 dollars, still generating positive ROI but with longer payback period. If investigation costs increase to 100 dollars per alert, annual benefit falls to approximately 211,000 dollars. The system remains viable across wide ranges of realistic parameter values. Only under extreme scenarios with fraud values below 300 dollars or investigation costs above 150 dollars per alert does the business case become marginal.

The direct financial benefits also exhibit favorable scaling properties. Development costs are largely fixed regardless of transaction volume, while benefits scale proportionally with volume. A supply chain processing 1 million transactions annually with equivalent fraud rate would generate approximately 2.5 million dollars annual benefit with similar development costs, substantially improving ROI. This scaling advantage makes fraud detection particularly attractive for high-volume supply chain operations.

**5.3.2. Indirect Value from Improved Supply Chain Performance**

Beyond direct fraud loss prevention, the detection system generates indirect value through improved supply chain performance as discussed in previous sections. Quantifying these indirect benefits is more challenging than direct benefits because they depend on organization-specific factors such as existing supply chain efficiency, coordination maturity, and cost structures. However, rough estimates based on supply chain management literature and industry benchmarks suggest that indirect benefits may equal or exceed direct benefits.

The bullwhip effect mitigation benefit can be estimated from the 22 percent reduction in demand variability enabled by removing 74.83 percent of fraud from demand signals. Supply chain cost models show that demand variability directly drives safety stock requirements, and inventory carrying costs are typically 20 to 30 percent of inventory value annually. For a supply chain with 10 million dollars in inventory where 30 percent represents safety stock and carrying cost rate is 25 percent, reducing safety stock by 22 percent saves approximately 165,000 dollars annually. Additional savings from reduced expediting, capacity costs, and production volatility could easily double this figure to 330,000 dollars.

Improved forecast accuracy generates value through better inventory allocation and reduced stockouts. When forecast error decreases by 14 percent as demonstrated in the DataCo analysis, inventory systems can either maintain service levels with less inventory or improve service levels with constant inventory. Taking a balanced approach with 7 percent inventory reduction and 7 percent service level improvement, the inventory reduction saves approximately 175,000 dollars annually in carrying costs for a 10 million dollar inventory, while the service level improvement generates additional margin estimated at 100,000 dollars annually from incremental sales that would have been lost to stockouts.

Coordination improvements from enhanced trust are difficult to quantify but potentially very valuable. If fraud detection enables CPFR implementation in product categories representing 20 percent of supply chain volume, and CPFR generates documented cost reductions of 5 to 15 percent, the expected benefit equals approximately 50 to 150 million dollars times 20 percent times 10 percent average cost reduction equals 1 to 3 million dollars annually. Even conservative estimates place coordination benefits in the hundreds of thousands of dollars annually.

Reputational benefits from demonstrating sophisticated fraud controls may enhance relationships with suppliers, payment processors, and customers. Suppliers may offer preferential pricing or allocation. Payment processors may reduce transaction fees for merchants with proven fraud management. Customers may demonstrate higher loyalty to retailers that protect them from fraud-related inconvenience. While these reputation benefits are difficult to quantify precisely, they contribute to competitive advantage and long-term profitability.

Summing the direct benefit of 444,500 dollars with estimated indirect benefits of approximately 665,000 dollars from bullwhip mitigation 330,000, forecast accuracy 275,000, and coordination improvements 60,000 conservative estimate yields total annual value of approximately 1,109,500 dollars. This total value calculation suggests that indirect benefits from improved supply chain performance may exceed direct fraud prevention benefits, making fraud detection a supply chain performance investment rather than merely a loss prevention expense.

The indirect benefits also compound over time as supply chain processes improve. Initial fraud detection implementation removes historical fraud from demand data and improves current decisions. Over subsequent years, cleaner demand data enables better forecasting models, stronger supplier relationships, and more sophisticated coordination mechanisms. These compounding improvements create increasing value trajectories where benefits grow beyond initial levels as organizational capabilities build on fraud detection foundations.

**5.3.3. Risk-Adjusted Returns and Implementation Considerations**

Evaluating fraud detection ROI requires considering not just expected benefits but also implementation risks and uncertainties that could affect realized returns. Several risk factors could cause actual performance to fall short of projections based on test set results, and prudent investment analysis should account for these risks through appropriate risk adjustments.

Model performance degradation over time represents a significant implementation risk. The 74.83 percent recall achieved on the test set reflects model performance on data drawn from the same time period and fraud patterns as the training data. As fraudsters adapt their tactics to evade detection, model performance typically degrades unless models are regularly retrained on updated data. Industry experience suggests that fraud detection models may lose 10 to 20 percent of effectiveness within 6 to 12 months without retraining. This degradation risk can be mitigated through ongoing model monitoring and scheduled retraining, but it increases operational complexity and costs.

False positive investigation costs may exceed projections if investigation processes are inefficient or if alert volumes overwhelm investigation capacity. The cost-benefit analysis assumes 50 dollars per alert investigation cost, representing approximately 30 minutes of staff time. However, complex investigation cases may require significantly more time, particularly when contacting customers to verify suspicious orders. If actual investigation costs average 75 dollars rather than 50 dollars, annual net benefit falls by approximately 117,000 dollars, reducing but not eliminating positive ROI.

Integration challenges with existing systems can cause implementation delays and cost overruns. Deploying fraud detection in production environments requires integration with order management systems to receive transaction data in real-time, customer relationship management systems to retrieve historical behavior, and fulfillment systems to block flagged orders. Legacy system architectures may complicate these integrations, requiring custom development work that exceeds initial estimates. Budget reserves of 25 to 50 percent above estimated development costs provide cushion for integration complexity.

Organizational change management issues can impede realization of full system benefits. Customer service representatives may resist using fraud scores in their decision processes if training is inadequate or if the system generates too many false positives that damage customer relationships. Investigation teams may lack capacity or skills to efficiently process alert volumes. Demand planning teams may not understand how to use cleaned demand data. Effective change management including training, process redesign, and performance metrics is essential for capturing projected benefits.

Regulatory compliance requirements may constrain system design or increase costs. Fraud detection systems that use customer behavioral data must comply with privacy regulations such as GDPR in Europe or CCPA in California. These regulations may limit available features, require explanations of fraud determinations, or mandate customer notification of fraud flags. Compliance requirements should be assessed during design phase to avoid costly retrofits.

Despite these risks, the magnitude of expected benefits and rapid payback period suggest that fraud detection investments offer attractive risk-adjusted returns in most supply chain contexts. A conservative risk adjustment that discounts expected benefits by 30 percent to account for implementation risks, model degradation, and cost overruns still yields annual net benefit of approximately 311,000 dollars and payback period under 9 months. This risk-adjusted return significantly exceeds typical hurdle rates for supply chain technology investments.

The risk profile also improves with staged implementation approaches. Rather than deploying fraud detection across all transactions immediately, organizations can pilot the system on high-value product categories or high-risk customer segments. Pilot implementations allow learning about integration challenges, investigation processes, and actual performance before full-scale rollout. Successful pilots build organizational confidence and demonstrate ROI that secures funding for broader deployment.

Monitoring and continuous improvement frameworks further mitigate performance risks. Implementing robust monitoring systems that track detection accuracy, investigation efficiency, and financial outcomes enables early identification of performance degradation. Regular model retraining schedules maintain effectiveness as fraud patterns evolve. A/B testing frameworks allow systematic comparison of model variants to identify improvements. These continuous improvement capabilities transform fraud detection from a static solution into an evolving capability that sustains value over time.

**5.4. Strategic Recommendations for Supply Chain Practitioners**

**5.4.1. Fraud Detection System Design Principles**

Organizations seeking to implement network-based fraud detection in their supply chains should follow several design principles derived from this research to maximize effectiveness and business value. These principles reflect both the technical findings about model performance and the strategic insights about fraud detection's role in supply chain risk management.

First, prioritize recall over precision through cost-sensitive learning approaches. The research demonstrates that standard machine learning methods optimizing for accuracy or F1-score fail to achieve acceptable fraud detection rates because they treat false positives and false negatives as equally costly. Fraud detection requires explicit recognition that missing frauds costs far more than investigating false alarms. Implementation requires using loss functions that penalize false negatives more heavily than false positives, setting classification thresholds lower than the default 0.5 value, and measuring success primarily through recall metrics rather than accuracy or precision.

Second, integrate network features with transaction features rather than relying solely on transaction characteristics. The research shows that network features provide incremental predictive value that improves recall by 5.6 percentage points beyond transaction-only models. While network feature engineering requires additional effort to construct customer-product bipartite networks and calculate centrality measures, the performance improvement justifies this investment. Organizations should build data pipelines that maintain network representations and update centrality metrics as new transactions occur, enabling real-time access to network features during fraud scoring.

Third, employ ensemble methods that average predictions from multiple independently trained models rather than relying on single models. The research demonstrates that simple averaging of three models trained with different random initializations improves performance over single models while avoiding the pitfalls of complex stacking ensembles that optimize for the wrong objectives. This ensemble approach is straightforward to implement and provides robustness against model instabilities without requiring sophisticated meta-learning frameworks.

Fourth, design for real-time or near-real-time operation with detection occurring before order fulfillment. Post-transaction fraud detection provides limited value because losses have already occurred by the time fraud is identified. Effective fraud prevention requires integration with order processing systems that score transactions at submission time and block suspicious orders before picking and shipping. This integration requires attention to system performance, with fraud scoring completing within subsecond timeframes to avoid delaying order confirmations. Performance optimization through model simplification, feature caching, and infrastructure scaling is essential for production deployment.

Fifth, implement feedback loops that improve models through continued learning from fraud detection outcomes. As fraudsters adapt their tactics, detection systems must evolve to maintain effectiveness. Organizations should establish processes for investigating flagged transactions, confirming or rejecting fraud determinations, and using these confirmations to retrain models on updated data. Model retraining schedules every 1 to 3 months depending on fraud pattern stability maintain performance despite changing fraud tactics. Monitoring systems that track recall, precision, and financial outcomes trigger retraining when performance degradation exceeds acceptable thresholds.

Sixth, balance automation with human judgment by designing hybrid systems where machine learning models score transactions and human investigators review high-risk cases. Fully automated blocking of flagged transactions risks damaging relationships with legitimate customers who are incorrectly flagged. Conversely, requiring human review of all transactions is cost-prohibitive. Effective systems use risk scores to triage transactions into three categories: low risk orders that are automatically approved, medium risk orders that receive lightweight verification such as email confirmation, and high risk orders that receive detailed manual investigation. This tiered approach optimizes investigation resources while maintaining customer experience.

**5.4.2. Organizational Implementation Roadmap**

Successful implementation of fraud detection systems requires systematic planning and phased deployment that builds organizational capabilities while demonstrating value. Organizations should follow a structured roadmap that balances speed to value against risks from premature full-scale deployment.

Phase 1 focuses on data preparation and foundational analytics spanning 2 to 3 months. Organizations should begin by assembling historical transaction data including order characteristics, customer information, product details, and fraud labels where available. Data quality assessment identifies missing values, inconsistencies, and necessary cleansing steps. Exploratory analysis examines fraud rates across customer segments, product categories, and time periods to understand fraud patterns and prioritize initial targeting. Network construction from historical transactions tests feasibility of calculating centrality measures at production scale. This foundation phase requires no production changes and generates insights about fraud patterns that inform subsequent phases.

Phase 2 develops and validates detection models in offline environment spanning 3 to 4 months. Data scientists build models following the architectural patterns from this research including deep neural networks with cost-sensitive loss, network feature integration, and ensemble averaging. Model training on historical data with proper train-test splits validates that acceptable recall can be achieved before production deployment. Experimentation with different feature sets, model architectures, and threshold settings optimizes performance for the organization's specific data and cost structure. This phase produces trained models ready for deployment but does not yet affect production operations.

Phase 3 pilots detection in limited production scope spanning 2 to 3 months. Rather than deploying across all transactions, organizations should select pilot scope such as specific product categories with high fraud rates, customer segments with elevated risk, or geographic markets with

contained volume. Pilot deployment integrates detection models with production order systems to generate real-time fraud scores. However, initial pilot may operate in shadow mode where scores are generated but do not block orders, allowing validation that scores perform as expected in production environment. Progressive pilot phases introduce score-based blocking for highest-risk transactions, then expand blocking thresholds as confidence builds. Pilot scope provides controlled environment for learning integration challenges, investigation procedures, and customer impacts before full deployment.

Phase 4 scales to full production deployment spanning 3 to 4 months. Based on successful pilot results, detection expands to remaining product categories, customer segments, and markets. Scaling requires attention to infrastructure capacity to handle full transaction volumes with acceptable latency. Investigation processes scale from pilot team to broader organization with documented procedures, training programs, and quality monitoring. Change management ensures that customer service, fulfillment operations, and supply chain planning functions understand how fraud detection affects their processes and how to use detection outputs in their decisions. Full-scale deployment includes monitoring dashboards that track performance metrics and financial outcomes to demonstrate ongoing value delivery.

Phase 5 establishes continuous improvement capabilities as ongoing program rather than project with defined end. Organizations implement automated monitoring systems that track detection performance and trigger alerts when accuracy degrades. Regular retraining schedules maintain model effectiveness as fraud patterns evolve. A/B testing frameworks enable systematic experimentation with model improvements. Feedback loops connect investigation outcomes back to model training data. Expansion opportunities such as additional data sources, alternative model architectures, or integration with additional supply chain processes are evaluated and prioritized based on incremental value potential.

This phased approach typically spans 12 to 15 months from initiation to full-scale deployment, with value realization beginning during Phase 3 pilot. Organizations achieve balance between moving quickly to capture value and proceeding systematically to manage implementation risks. The roadmap is flexible and can be compressed or extended based on organizational capabilities, data readiness, and strategic priorities.

**5.4.3. Integration with Broader Supply Chain Risk Management**

Fraud detection should be positioned as one component within comprehensive supply chain risk management programs rather than as an isolated initiative. Integration with broader risk management creates synergies where fraud detection capabilities support other risk mitigation efforts and other risk management infrastructure enables more effective fraud detection.

From a risk management portfolio perspective, fraud detection addresses one specific operational risk within the broader landscape of supply chain risks. Organizations face multiple risk categories including demand uncertainty, supply disruptions, quality failures, capacity constraints, transportation delays, and financial risks beyond fraud. Effective risk management portfolios apply appropriate mitigation strategies to each risk category based on risk magnitude, detectability, and mitigation cost-effectiveness. Fraud detection represents optimal primary strategy for fraud risk but should be complemented by appropriate strategies for other risk categories.

Shared data infrastructure that supports fraud detection also enables other risk management capabilities. The data integration required for fraud detection, including real-time transaction feeds, historical behavior databases, and network analytics, provides foundations for supplier risk monitoring, demand sensing, and quality analytics. Organizations can leverage fraud detection data investments to build broader supply chain visibility and analytics capabilities. Conversely, existing supply chain analytics infrastructure developed for demand forecasting or supplier management can be extended to support fraud detection with incremental investment.

Risk management governance structures should encompass fraud detection alongside other risk categories. Organizations with established supply chain risk management committees, risk reporting frameworks, and risk mitigation funding processes should incorporate fraud detection into these existing structures rather than creating parallel governance for fraud alone. This integration ensures consistent prioritization across risk categories, facilitates risk portfolio optimization, and prevents siloed risk management that misses interdependencies between risk types.

Supplier collaboration on risk management can extend to fraud prevention. Suppliers often have visibility into unusual order patterns or suspicious customer behaviors from their vantage point in the supply chain. Collaborative fraud intelligence sharing where retailers and suppliers exchange information about fraud signals can improve detection for both parties. However, such collaboration requires trust and appropriate data sharing agreements that protect competitive information while enabling security cooperation. Industry consortia focused on fraud prevention provide neutral venues for sharing fraud intelligence without competitive concerns.

Coordination between fraud detection and other supply chain optimization initiatives prevents conflicts and creates synergies. For example, promotional campaigns that reduce prices or offer flexible return policies may inadvertently create fraud opportunities. Coordination between marketing teams planning promotions and fraud detection teams monitoring risk ensures that fraud controls adapt to accommodate legitimate promotional surge while maintaining protection against fraud exploitation. Similarly, inventory optimization initiatives that reduce safety stock levels increase the cost of fraud-related inventory misallocation, potentially justifying more aggressive fraud detection thresholds during periods of tight inventory.

The integration perspective also applies to organizational structure. Rather than housing fraud detection exclusively within loss prevention or security organizations, supply chain organizations should consider shared ownership models where supply chain operations, IT, and loss prevention collaborate on fraud detection as a shared capability. This cross-functional ownership ensures that detection systems balance fraud prevention with operational efficiency and customer experience rather than optimizing solely for fraud detection without considering broader business impacts.

This chapter has analyzed the implications of the fraud detection research for supply chain management practice and theory. The findings demonstrate that fraud detection implemented through the proposed network-based approach delivers substantial value through both direct fraud prevention and indirect supply chain performance improvements. Integration with broader supply chain operations and risk management strategies maximizes this value while positioning fraud detection as a strategic capability rather than a tactical security measure. The next chapter concludes the research by summarizing key findings, discussing limitations, and suggesting directions for future research.

**CHAPTER 6: CONCLUSION**

**6.1. Summary of Key Findings**

This research developed and evaluated a network-based fraud detection system for supply chain operations, integrating social network analysis with deep learning to identify fraudulent transactions in e-commerce supply chains. The study addressed a critical gap in both fraud detection literature and supply chain management practice by demonstrating how customer-product network features enhance fraud detection performance beyond traditional transaction-based approaches.

The empirical investigation used the DataCo supply chain dataset containing 180,519 transactions from a real-world e-commerce operation. A bipartite network with 20,770 nodes and 101,196 edges was constructed to represent customer-product relationships, enabling calculation of four network centrality measures: degree, betweenness, closeness, and PageRank. These network features were combined with 57 transaction-based features and processed through principal component analysis to create an optimized feature set of 45 components.

The fraud detection model employed a deep neural network architecture with three hidden layers containing 256, 128, and 64 neurons respectively, trained using a cost-sensitive focal loss function that explicitly penalizes false negatives more heavily than false positives. The model was trained on SMOTE-balanced data to address the 2.25 percent class imbalance in the original dataset. An ensemble of three independently trained models with simple averaging produced final fraud predictions, with a classification threshold of 0.20 optimized to maximize recall.

The AGGRESSIVE ensemble configuration achieved recall of 74.83 percent on the held-out test set, successfully detecting 214 out of 286 fraudulent transactions while generating 848 false positives from 3,845 legitimate transactions. This performance exceeded the industry-standard target of 70 percent recall by 4.83 percentage points, demonstrating practical viability for production deployment. The model achieved ROC-AUC of 82.16 percent, indicating strong discriminative ability across all possible threshold settings.

Network features provided substantial incremental value beyond transaction features alone. Models trained exclusively on 57 transaction features achieved 69.23 percent recall, falling short of the 70 percent target. Adding four network centrality measures improved recall by 5.60 percentage points to 74.83 percent, representing detection of approximately 16 additional frauds in the test set. This improvement demonstrates that customer purchasing patterns captured through network analysis contain fraud signals not visible in individual transaction characteristics.

Comparative analysis revealed that the proposed approach significantly outperformed alternative configurations. A single model baseline using standard binary crossentropy loss achieved only 41.61 percent recall, missing 58.39 percent of frauds despite higher precision. A stacking ensemble combining diverse base models achieved catastrophically low 32.87 percent recall, demonstrating that complex meta-learning approaches can optimize for the wrong objectives in cost-asymmetric problems. The AGGRESSIVE ensemble's simple averaging approach preserved cost-sensitive behavior while benefiting from variance reduction.

Cost-benefit analysis demonstrated positive business value under realistic assumptions. The detection system generated net benefit of 88,900 dollars on the test set, scaling to approximately 444,500 dollars annually. This benefit resulted from preventing 935,000 dollars in fraud losses while incurring 233,000 dollars in investigation costs and accepting 314,000 dollars in residual losses from undetected frauds. The system achieved payback in approximately 5 months against estimated development costs of 200,000 dollars, demonstrating strong return on investment.

Analysis of network structure revealed systematic differences between fraudulent and legitimate customer behavior. Fraudulent customers exhibited 57 percent higher degree centrality than legitimate customers, purchasing an average of 7.40 distinct products compared to 4.71 products for legitimate customers. This elevated purchasing diversity provided the strongest single fraud signal. Fraudulent customers also showed 8 percent lower PageRank, indicating they purchase less popular products than typical customers. This combination of high diversity and low popularity created a distinctive fraud signature that network features captured effectively.

The bullwhip effect analysis demonstrated that fraud creates information distortion that amplifies demand variability throughout supply chains. Products experiencing fraud in more than 3 percent of transactions showed 36 percent higher demand coefficient of variation than low-fraud products. By detecting and removing 74.83 percent of fraudulent transactions, the system reduced demand variability by an estimated 22 percent. This reduction translated to approximately 30 to 40 percent reduction in upstream manufacturer order variability through amplification effects, generating substantial cost savings from reduced inventory, production volatility, and capacity requirements.

Forecast accuracy improved significantly when fraud was removed from historical demand data. Models trained on fraud-contaminated history achieved mean absolute percent error of 32.4 percent, while identical models trained on cleaned history achieved 27.8 percent MAPE, representing 14 percent improvement. This accuracy gain enabled better inventory planning, reduced safety stock requirements, and improved service levels. The forecast improvement cascaded through multi-echelon supply chains as better retail forecasts enabled better wholesale inventory positioning and more efficient manufacturer production planning.

**6.2. Theoretical Contributions**

This research makes several contributions to the theoretical understanding of fraud detection and supply chain risk management. First, it extends social network analysis theory into the fraud detection domain by demonstrating that network centrality measures capture behavioral patterns relevant to fraud propensity. Previous research applied network analysis primarily to financial fraud detection in transaction networks or social fraud detection in online platforms. This research shows that customer-product bipartite networks in supply chain contexts contain fraud signals that complement transaction-level features.

The finding that degree centrality is the most important fraud predictor provides theoretical insight into fraudster behavior. High purchasing diversity among fraudulent customers suggests that fraudsters either deliberately purchase across categories to maximize extracted value or lack the coherent preferences that guide legitimate customer behavior. This behavioral pattern aligns with rational fraud models where fraudsters optimize for short-term gain before detection while contrasting with models that assume fraudsters mimic legitimate behavior to avoid detection. The theory implication is that fraud detection should focus on detecting anomalous diversity rather than only detecting individual anomalous transactions.

The research contributes to cost-sensitive learning theory by demonstrating the importance of explicit false negative penalties beyond standard focal loss. While focal loss addresses class imbalance by down-weighting easy examples, it does not directly encode the economic cost asymmetry between error types. The research shows that combining focal loss with explicit false negative cost terms significantly improves recall compared to focal loss alone. This finding suggests that cost-sensitive learning requires not just addressing class imbalance but also directly encoding cost structures into loss functions.

The ensemble learning findings contribute to understanding when simple averaging outperforms complex meta-learning. The research demonstrates that stacking ensembles with meta-learners can undo cost-sensitive learning from base models by introducing additional optimization that defaults to accuracy maximization. Simple averaging preserves the cost-sensitive behavior of base models while reducing prediction variance. This suggests theoretical principle that ensemble aggregation methods should match the objectives of base model training, with simple methods preferable when base models already optimize for desired objectives.

From supply chain management theory perspective, the research extends the operational hedging framework by quantifying how fraud detection implements the risk reduction strategy. Previous work on operational hedging focused primarily on diversification, pooling, and flexibility strategies for managing supply and demand uncertainty. This research demonstrates that risk reduction through root cause elimination can be more effective than other hedging strategies for certain risk types. The theoretical contribution is showing that operational hedging strategy selection should consider risk characteristics including detectability and prevention feasibility, not just risk magnitude and correlation structure.

The bullwhip effect findings contribute to information distortion theory by demonstrating fraud as a specific mechanism of information distortion. While previous research identified demand signal processing, rationing game playing, order batching, and price fluctuations as bullwhip causes, fraud represents an additional cause where completely false signals enter the supply chain. The research quantifies how fraud contributes to demand variability amplification and shows that fraud removal reduces variability transmission. This extends bullwhip theory to encompass intentional information distortion beyond the unintentional distortion emphasized in previous work.

The coordination theory contribution demonstrates how information quality affects trust and enables coordination mechanisms. Previous research showed that lack of trust impedes coordination but focused primarily on trust built through relationship history and contractual structures. This research shows that demonstrable information quality through fraud detection builds trust that enables coordination mechanisms like vendor-managed inventory and collaborative forecasting. The theoretical insight is that information quality is not just about accuracy but also about demonstrable quality assurance that creates partner confidence.

**6.3. Practical Contributions**

The research provides actionable guidance for supply chain practitioners seeking to implement fraud detection systems. The detailed methodology including network construction, feature engineering, model architecture, training procedures, and threshold optimization provides a blueprint that organizations can adapt to their specific contexts. The open description of techniques enables reproducibility and reduces barriers to adoption compared to proprietary commercial fraud detection systems that obscure methodology.

The cost-benefit analysis framework provides practitioners with tools to evaluate fraud detection investments quantitatively. By demonstrating how to estimate direct fraud prevention benefits, investigation costs, and residual losses, the research enables business case development that justifies detection system investments to organizational leadership. The framework extends to estimating indirect benefits from bullwhip mitigation, forecast accuracy improvement, and coordination enhancement, providing comprehensive value assessment beyond direct fraud prevention.

The comparative analysis of different model configurations provides practical guidance on design choices that matter most for performance. The finding that cost-sensitive loss and aggressive thresholds are more important than complex ensemble methods helps practitioners prioritize development efforts on elements that drive results. The demonstration that simple averaging outperforms stacking for imbalanced problems prevents practitioners from pursuing sophisticated ensemble approaches that may underperform simpler alternatives.

The feature importance analysis guides data collection and feature engineering priorities. By identifying degree centrality as the most important feature, the research directs practitioners to ensure their systems capture customer purchasing history across products. The finding that network features provide 5.60 percentage point recall improvement justifies investment in network construction and centrality calculation despite additional complexity compared to transaction-only approaches.

The implementation roadmap provides structured approach to deployment that balances speed to value against implementation risk. The five-phase approach from data preparation through pilot deployment to full-scale production provides realistic timeline expectations and identifies critical activities for each phase. Organizations can adapt this roadmap to their specific circumstances while following proven sequence that builds capabilities systematically.

The integration guidance helps practitioners position fraud detection within broader supply chain operations rather than as isolated security measure. By showing how detection outputs improve demand forecasting, inventory planning, and supplier coordination, the research helps organizations realize full value beyond direct fraud prevention. The governance recommendations ensure fraud detection receives appropriate cross-functional ownership rather than being confined to loss prevention departments.

The system design principles derived from the research provide concise guidance on architecture decisions. The emphasis on real-time operation, ensemble diversity through random initialization, hybrid automation with human review, and continuous model updating through feedback loops reflects lessons from both the research findings and industry best practices. These principles help practitioners avoid common pitfalls while focusing on elements that drive system effectiveness.

**6.4. Research Limitations**

Several limitations affect the interpretation and generalizability of the research findings. First, the study uses a single dataset from one e-commerce operation, limiting generalizability to other supply chain contexts with different product categories, customer demographics, fraud patterns, or operational characteristics. The DataCo dataset represents a specific mix of consumer products sold through online channels. Fraud patterns and network characteristics may differ significantly in business-to-business supply chains, pharmaceutical supply chains, or luxury goods markets. Validation on additional datasets from diverse supply chain contexts would strengthen confidence in the generalizability of findings.

Second, the fraud labels in the dataset reflect suspected fraud based on existing detection mechanisms rather than confirmed fraud verified through investigation and legal proceedings. This label quality limitation means the model learns to detect fraud patterns similar to those identified by previous detection methods rather than learning true fraud patterns independently. If the existing detection methods are biased toward certain fraud types, the model may inherit and perpetuate these biases. Access to datasets with confirmed fraud labels from completed investigations would improve label quality and model learning.

Third, the research does not account for fraudster adaptation over time as detection systems are deployed. The test set performance assumes fraud patterns remain stable, but real-world fraudsters actively adapt tactics when they discover detection mechanisms. The 74.83 percent recall achieved on the test set may degrade over time as fraudsters learn to mimic legitimate customer network behavior or exploit blind spots in the detection system. Longitudinal evaluation tracking model performance over extended periods with periodic retraining would better assess sustained effectiveness.

Fourth, the cost-benefit analysis relies on simplified assumptions about fraud values, investigation costs, and operational impacts. Real-world fraud values vary significantly across transactions, investigation costs depend on case complexity, and operational impacts include customer experience effects that are difficult to quantify. The analysis assumes constant costs and benefits per transaction type, but actual economics exhibit substantial variation. More sophisticated cost modeling incorporating distributions rather than point estimates would improve accuracy of economic assessments.

Fifth, the network features calculated from the complete dataset including both training and test customers create potential information leakage. In production deployment, network metrics for new customers cannot be calculated from future transactions that have not yet occurred. The research addresses this by calculating network features before train-test split, but a more rigorous approach would construct separate networks for training and test periods to fully eliminate leakage. This limitation may cause production performance to fall short of research results if network features derived from limited history provide less predictive power than those calculated from complete transaction history.

Sixth, the research focuses exclusively on customer-product bipartite networks and does not explore alternative network representations. Customer-customer networks based on shared purchasing patterns, product-product networks based on co-purchase patterns, or multi-layer networks incorporating both customer and product relationships might capture different fraud signals. The choice of bipartite representation, while justified by supply chain structure, may miss network patterns that alternative representations would reveal.

Seventh, the deep learning approach requires substantial training data and computational resources that may be unavailable to smaller organizations. The model architecture with approximately 50,000 parameters requires sufficient training examples to avoid overfitting. Organizations with lower transaction volumes or limited historical data may struggle to train effective models using the proposed approach. Evaluation of simpler model alternatives suitable for low-data regimes would improve accessibility for smaller organizations.

Eighth, the research does not address explainability and interpretability requirements that may be important for fraud detection in regulated industries or contexts where fraud determinations must be justified to customers or legal authorities. Deep neural networks function as black boxes whose predictions are difficult to explain in terms of specific features or decision rules. Organizations requiring explainable fraud determinations may need to sacrifice some performance to use more interpretable model architectures like decision trees or rule-based systems.

**6.5. Future Research Directions**

Several promising directions for future research would extend and strengthen the contributions of this work. First, validation on multiple datasets from diverse supply chain contexts would test generalizability and identify context-specific factors that affect fraud detection performance. Comparative studies across industries such as consumer electronics, fashion, groceries, and industrial supplies would reveal whether network-based fraud signals are universal or industry-specific. Cross-industry validation would also identify which model architecture choices and hyperparameter settings are robust versus context-dependent.

Second, exploration of alternative network representations beyond customer-product bipartite graphs could reveal additional fraud signals. Customer-customer networks where edges represent similar purchasing patterns might capture fraud rings where multiple accounts are controlled by the same fraudster. Product-product networks where edges represent frequent co-purchase could identify unusual product combinations favored by fraudsters. Multi-layer networks incorporating multiple relationship types simultaneously might capture interaction effects between customer behavior and product characteristics. Comparative evaluation of network representations would identify optimal approaches for different fraud types.

Third, development of explainable fraud detection models would address interpretability requirements while maintaining performance. Attention mechanisms that highlight which features and network patterns drive fraud predictions would improve model transparency. Rule extraction approaches that distill deep learning models into interpretable decision rules would enable explanation of fraud determinations. Counterfactual explanations showing how a flagged transaction would need to change to be classified as legitimate would help investigation processes. Research comparing performance-interpretability tradeoffs across model architectures would guide practitioners in selecting appropriate models for their governance requirements.

Fourth, investigation of dynamic network models that capture temporal evolution of customer behavior would improve detection of account takeover fraud and behavioral changes. The research uses static networks calculated from complete transaction history, but customer purchasing patterns evolve over time through learning, changing preferences, and life events. Graph neural networks with temporal attention mechanisms could model how customer network positions change over time and detect anomalous changes indicative of account compromise. Recurrent architectures processing transaction sequences could identify behavioral drift patterns that distinguish fraud from legitimate evolution.

Fifth, development of online learning frameworks that continuously update models as new transactions and fraud confirmations arrive would maintain effectiveness against adaptive fraudsters. The research uses batch learning where models are trained once on historical data. Production systems require ongoing learning to adapt to changing fraud tactics. Research on efficient online learning approaches that incrementally update model weights without full retraining would enable real-time adaptation. Active learning strategies that intelligently select which transactions to investigate for maximum learning value would improve learning efficiency.

Sixth, integration of external data sources beyond internal transaction history could enhance fraud detection. Social media data revealing account authenticity, shipping address validation against postal databases, device fingerprinting identifying reused devices across accounts, and email domain reputation scoring could provide additional fraud signals. Privacy-preserving approaches to external data integration that comply with regulations while enhancing detection would be particularly valuable. Research quantifying incremental value from different external data sources would guide data acquisition priorities.

Seventh, investigation of fraud detection in multi-channel supply chains where customers interact through multiple touchpoints would address increasingly common omnichannel operations. The research focuses on online transactions, but modern supply chains integrate online ordering with in-store pickup, returns across channels, and customer service through multiple contact points. Network representations capturing multi-channel interaction patterns might reveal fraud signals not visible in single-channel data. Cross-channel fraud where fraudsters exploit differences in fraud controls across channels represents an important practical challenge requiring research attention.

Eighth, development of frameworks for adversarial robustness against fraudsters who actively try to evade detection would improve system resilience. The research assumes fraudsters are unaware of detection mechanisms, but sophisticated fraudsters may probe systems to identify detection blind spots. Adversarial training approaches that expose models to synthetic fraud examples designed to evade detection would improve robustness. Game-theoretic frameworks modeling the strategic interaction between fraud detection systems and adaptive fraudsters would inform robust detection strategies.

Ninth, investigation of transfer learning approaches that leverage fraud patterns learned in one supply chain to bootstrap detection in another would reduce data requirements for new deployments. Organizations implementing fraud detection often lack sufficient historical fraud labels to train effective models. Transfer learning approaches that adapt models pretrained on public datasets or other organizations' data to new contexts with minimal labeled data would improve accessibility. Research on domain adaptation techniques accounting for differences in product categories, customer demographics, and fraud tactics would enable effective transfer.

Tenth, exploration of the broader implications of network-based fraud detection for supply chain visibility and collaboration would extend impact beyond fraud prevention. The customer-product network construction and analysis infrastructure built for fraud detection could support additional applications including customer segmentation, product recommendation, inventory optimization, and supplier performance monitoring. Research identifying synergies between fraud detection and other supply chain analytics applications would maximize return on network analytics investments.

**6.6. Final Remarks**

This research demonstrates that fraud detection represents not merely a security measure but a strategic supply chain capability that generates value through multiple mechanisms. By preventing fraudulent transactions, detection systems reduce direct financial losses and avoid operational disruptions from shipping products to fraudsters. By removing false demand signals from supply chain planning processes, detection systems improve forecast accuracy, reduce inventory requirements, and mitigate the bullwhip effect. By demonstrating information quality to supply chain partners, detection systems build trust that enables coordination mechanisms like vendor-managed inventory and collaborative forecasting.

The integration of social network analysis with deep learning provides a powerful approach to fraud detection that leverages both transaction characteristics and behavioral context. Network features capturing customer purchasing patterns across products reveal fraud signals that individual transactions cannot provide. The combination of transaction and network features enables detection performance that exceeds industry benchmarks while generating positive return on investment under realistic cost assumptions.

The emphasis on cost-sensitive learning through custom loss functions, aggressive classification thresholds, and recall-focused performance metrics reflects the fundamental asymmetry between false positive and false negative costs in fraud detection. Standard machine learning approaches optimizing for accuracy or F1-score fail because they treat all errors equally. Effective fraud detection requires explicit recognition that missing frauds costs far more than investigating false alarms, and this recognition must be embedded throughout the detection system from loss function design through threshold selection to performance evaluation.

The ensemble approach using simple averaging of independently trained models provides a straightforward method to improve detection robustness without complex meta-learning. The finding that simple averaging outperforms stacking ensembles in this application demonstrates the importance of matching ensemble aggregation methods to the objectives of base model training. When base models are trained with cost-sensitive learning to prioritize recall, simple averaging preserves this priority while reducing variance. Complex meta-learners that reoptimize predictions risk undoing carefully designed cost-sensitive behavior.

From supply chain management perspective, the research highlights fraud detection as an operational hedging strategy that reduces risk by addressing root causes rather than merely managing consequences. Compared to alternative hedging strategies like reserves, insurance, or diversification, detection provides more effective risk reduction at lower cost by preventing fraud from occurring. This superiority justifies positioning fraud detection as the primary fraud risk management mechanism, complemented by modest reserves for residual risk and appropriate insurance for catastrophic scenarios.

The bullwhip effect analysis reveals fraud as an important but previously underemphasized cause of information distortion in supply chains. While research has extensively studied how demand signal processing, rationing games, order batching, and price fluctuations create distortion, fraud represents intentional false signals that may amplify more severely than unintentional distortion. Recognition of fraud as a bullwhip driver suggests that fraud detection should be integrated with demand management processes rather than treated as separate security function.

The coordination theory implications demonstrate that information quality is not just about accuracy but about demonstrable quality assurance that builds partner trust. Effective fraud detection that visibly removes false signals from demand data creates confidence that enables suppliers to participate in collaborative planning arrangements that require mutual vulnerability. This trust-building benefit may generate value that equals or exceeds direct fraud prevention benefits, positioning fraud detection as enabler of supply chain coordination rather than merely cost avoidance.

Looking forward, the convergence of increasing supply chain digitization, growing availability of network data, and advancing machine learning capabilities creates opportunities for increasingly sophisticated fraud detection systems. As supply chains generate more granular transaction and interaction data, network representations become richer and more informative. As machine learning methods continue advancing, particularly in areas like graph neural networks and explainable AI, detection systems can leverage more complex patterns while maintaining interpretability. As organizations develop greater analytics maturity, fraud detection can integrate more deeply with supply chain planning and execution processes.

The challenge for practitioners is implementing fraud detection systems that balance effectiveness against practical constraints including development costs, computational requirements, investigation capacity, and customer experience impacts. The research provides a framework for navigating these tradeoffs through phased implementation that starts with high-value applications, proves benefits through pilot deployment, and scales systematically as capabilities and confidence build. Organizations that successfully implement network-based fraud detection position themselves to capture not just direct fraud prevention benefits but also broader supply chain performance improvements from reduced information distortion and enhanced coordination.

In conclusion, fraud detection represents an important but underappreciated opportunity for supply chain performance improvement. By integrating social network analysis with machine learning and embedding detection within supply chain operations, organizations can achieve fraud detection rates that exceed industry benchmarks while generating positive business value. The research demonstrates that network features provide incremental fraud signals beyond transaction characteristics, that cost-sensitive learning is essential for acceptable recall, and that simple ensemble methods are effective for robustness. These findings provide both theoretical insights and practical guidance for advancing fraud detection in supply chain contexts.

The implications extend beyond fraud detection to broader questions of how organizations should manage operational risks, maintain information quality, and build trust that enables supply chain coordination. As supply chains become increasingly complex and interconnected, capabilities for detecting and removing false signals become essential for operational excellence. Organizations that invest in these capabilities position themselves for competitive advantage through superior risk management, more accurate planning, and stronger partner relationships. The research contributes to this emerging capability area by demonstrating feasibility, quantifying benefits, and providing implementation guidance for network-based fraud detection in supply chains.