

Classifying Behavioral and Registry-Based Fraud Indicators Used in Carrier and Broker Vetting

 **Kholmatjon Gofurov**¹

¹ CEO, Fastmover Express Inc Mason, Ohio, United States

ABSTRACT: Fraud in United States freight transportation has shifted from opportunistic theft to schemes that exploit the vetting process itself, including double-brokering, non-payment, and impersonation of established intermediaries. Carriers and brokerages without an in-house analytical function face these schemes with limited tools, and the warning signs described in the practitioner literature remain scattered across formats that are not operational. This review organizes those warning signs into a classification built on two dimensions, the verifiability of the underlying signal and the stage of the load lifecycle at which the signal becomes actionable. The classification separates registry-based indicators, which can be checked against records maintained independently of the counterparty, from behavioral indicators, which surface only in the conduct of the transaction. Each family is mapped onto a documented dispatch procedure in which credit verification through a factoring provider and the retention of a time-stamped verification artifact precede the release of any load. A risk-scoring framework is proposed based on classification, with four signal groups feeding into a weighted score and three escalation outcomes. The framework has not been implemented or validated and is presented as a construction whose weights and thresholds function as management parameters. Two boundary conditions are identified, post-verification double brokering and impersonation of a vetted counterparty, both of which pass through registry checks and remain detectable through behavioral signals alone.

KEYWORDS: freight fraud, carrier vetting, broker vetting, double brokering, fraud indicators, supply chain risk management, third-party logistics

1. Introduction

Freight transportation in the United States rests on a chain of intermediated transactions in which a carrier commits equipment, fuel, and driver hours to a counterparty whose reliability has been assessed in a few minutes. The structure of that market, with tens of thousands of licensed brokers and load boards that lower the cost of entry to a few filings, has created conditions in which deception offers a favorable reward-to-exposure ratio. Losses attributed to double brokering alone have been estimated at hundreds of millions of dollars each year, and industry reports have recorded rising numbers of fraud complaints across brokerage operations.

The structural conditions behind these schemes have been examined in the operations literature. Supply chains whose participants are separated by information

gaps create positional advantages for parties willing to exploit them, and the same gaps that make intermediation profitable also make fraud difficult to observe from any single vantage point (DuHadway et al., 2022). Digital freight platforms have compressed search costs while leaving information asymmetry between shippers and carriers largely intact, which sustains opportunistic conduct alongside efficiency gains (He et al., 2025). Cargo theft has followed a parallel trajectory, with deception-based methods displacing physical interception in a growing share of incidents (Cedillo-Campos et al., 2024).

Regulatory design contributes to the same picture. Operating authority in the United States is granted based on filings, insurance evidence, and a surety instrument, and the process establishes eligibility to operate at a given point in time. Continuing oversight focuses on safety performance, leaving commercial

conduct toward carriers and shippers to private ordering through contracts, credit assessment, and industry reputation systems. A counterparty can therefore hold valid authority while accumulating a record of non-payment, and a carrier seeking to assess that risk consults sources outside the regulatory record. This division explains why credit assessment through a factoring provider occupies a central place in the classification developed here, since the factoring company prices the payment risk it assumes, thereby producing an assessment that the public record does not contain.

Detection research has concentrated on modeling. Supervised learning has been applied to transactional records to distinguish fraudulent from legitimate activity in supply chain data (Seify et al., 2022). Broader treatments have assessed the contribution of machine learning and artificial intelligence to fraud prevention across procurement and order processes (Lokanan & Maddhesia, 2025). Such approaches presuppose labeled histories, engineering capacity, and data volumes that a carrier operating 100 trucks lacks. The gap between what the modeling literature assumes and what a mid-sized carrier can execute defines the problem addressed here.

Four schemes account for most of the exposure discussed in this article. Double brokering describes the re-tendering of a load by a party that presented itself as the carrier, which leaves the original broker with an unknown party in possession of the freight and the performing carrier with no contractual path to payment. Non-payment describes acceptance of transportation services followed by refusal or inability to settle the invoice, a scheme whose losses fall on carriers that have already spent fuel and driver hours. Identity theft is the use of a licensed and reputable entity's credentials by a third party, thereby defeating verification directed at the record rather than the person. Cargo theft by deception involves acquiring physical custody through fraudulent tender, after which the freight disappears. The four differ in mechanism and converge on a single moment of exposure, namely the point at which a load is released to a counterparty whose identity and intent have been assessed on the basis of incomplete information.

A second gap concerns the object of study. Fraud in supply chains has been examined at the level of products, procurement, and network structure, while the specific transaction through which a load is tendered

from a broker to a carrier has received attention almost entirely in practitioner publications. To the best of the author's knowledge, no peer-reviewed classification organizes the warning signs used in carrier and broker vetting according to how each signal can be verified and when in the load lifecycle it can be acted upon.

This article addresses that gap for a defined audience, namely carriers and brokerage companies that lack a dedicated analytical function and must conduct any vetting through dispatchers in the ordinary course of a working day. Three contributions follow. The first is a classification of fraud indicators along two dimensions, verifiability and timing. The second is a mapping of that classification onto a documented dispatch procedure, which converts the classification into an ordered sequence of checks, each with a required artifact. The third is a proposed risk-scoring framework derived from the classification and expressed in the vocabulary of operational risk management, together with an explicit account of the schemes the framework cannot cover.

2. Review Approach and Classification Framework

The work reported here is a narrative review with an author-developed classification. Its purpose extends beyond enumerating documented fraud schemes toward organizing known indicators into a structure that a carrier or brokerage without analytical staff can apply as an ordered vetting procedure. The term systematic is avoided throughout, since the search protocol did not meet the requirements of that method.

Three strands of source material informed the classification. The first consists of regulatory and registry documentation of the Federal Motor Carrier Safety Administration, covering operating authority registration, reinstatement, insurance filings, and complaint mechanisms. The second consists of industry publications and loss-prevention reporting on double-brokering, identity fraud, non-payment, and cargo theft in the United States truckload market. The third consists of academic work on counterparty risk, fraud detection, and supplier assessment in supply chain and transportation management. Two lines within that strand carry direct relevance. The first covers multicriteria models developed for the selection of logistics providers (Luyen & Thanh, 2022). The second covers empirical work on the risk factors applied during supplier evaluation (Urbaniak et al., 2022). Sources were

entered into the review when they described either the mechanism of a scheme or a verification practice that is executable at the level of an individual dispatch. Coverage of the literature is partial, and the contribution lies in the classification and its operational mapping.

Two dimensions organize the classification. The first is the verifiability of the underlying signal. An indicator counts as registry-based and verifiable when it can be checked against an external record maintained independently of the counterparty, such as a government registry, a factoring company's credit assessment, an insurance filing, or a complaint database. An indicator counts as behavioral when it becomes observable only through the counterparty's conduct during the transaction, including the pace and pressure of negotiation, requests regarding payment or communication channels, and inconsistencies between what is offered and what the counterparty's profile would predict. The second dimension is the timing of the check within the load lifecycle, which is divided into the period before booking, the period after booking and before the load is released for execution, and the period running through delivery. The dimensions are orthogonal. Registry-based indicators concentrate in the first two periods, while behavioral indicators can surface at any point, including after every registry check has been passed.

Calibration of the classification draws on a dispatch standard operating procedure documented at the author's company. Two controls in that procedure serve as reference points for what an operationalized registry check looks like in practice. Under the first, a dispatcher who has booked a load verifies the broker's credit standing through the factoring provider, captures a screenshot showing the broker's name, the check date and time, and the credit status, and uploads it to the transportation management system. No load proceeds without the verification artifact on file. Under the second, the dispatcher obtains the broker's track-and-trace contact and enters it into the system before the load is released for full execution, thereby establishing a verified channel to the counterparty's tracking function. These controls convert counterparty vetting from a discretionary judgment into a documented, auditable step. The procedure sits within a broader set of

documented operating policies at the same company covering driver management and performance standards, indicating a control environment that is operational and beyond declarations. Details of this kind are reported as the author's documented practice, and no operational performance figures are claimed.

The selection of the two dimensions followed from a property of the vetting problem that distinguishes it from fraud detection in settings with abundant labeled data. A carrier deciding whether to accept a load holds two kinds of information about the counterparty, and the kinds differ in where they come from and in when they arrive. Information held in records exists before the conversation begins and remains available for as long as the record persists, which makes it verifiable by a third party and reproducible across dispatchers. Information carried by conduct exists only inside the exchange and disappears unless someone writes it down. Any classification that mixes the two loses the ability to determine whether an indicator can be built into a procedure, since a check against a record can be mandated and audited, whereas an observation of conduct can only be trained and recorded. Timing enters as the second dimension because an indicator that cannot be acted upon at the stage where it appears has no operational value, and several of the strongest behavioral signals arrive after every registry check has concluded.

The scoring framework set out in section 4 is described in the vocabulary of operational risk management. Indicator groups function as sources of signals, weights and thresholds function as parameters of a management escalation decision, and the framework as a whole function as a structured vetting procedure. The framework has not been built, deployed, or validated against realized outcomes.

3. Results

The classification distinguishes two families of indicators, each divided into four constituent signals. Figure 1 presents the resulting structure, with the source of verification recorded beneath each signal and a dashed connector marking the pair of indicators that together address impersonation of a counterparty whose record is clean.

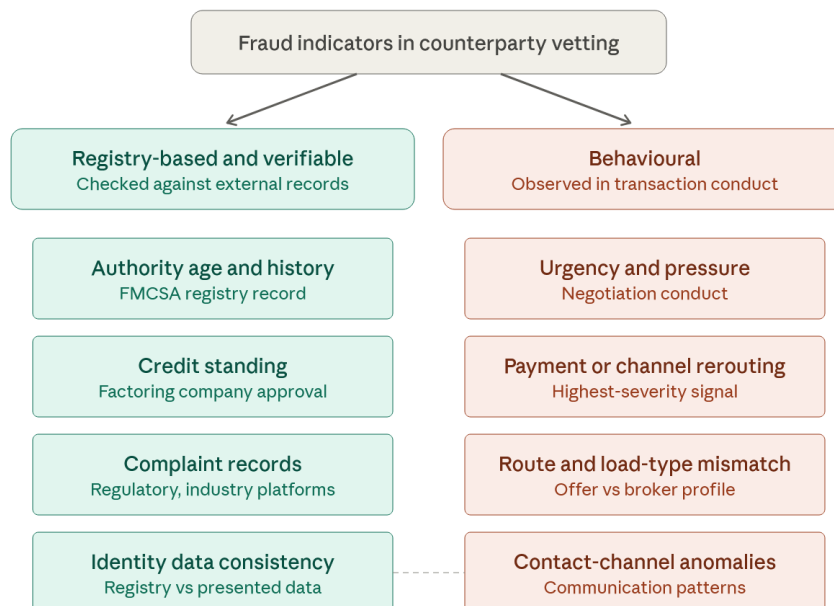


Fig. 1. Taxonomy of fraud indicators in carrier and broker vetting

The first family comprises indicators that can be checked against external records. Its opening component concerns the age of the counterparty's operating authority and the history of its registration record, covering the initial grant date, reinstatements, revocations, and changes to legal name, address, or insurance provider. Newly granted authority, the solicitation of high-value freight, authority reinstated after revocation, and a pattern of frequent changes to registered identity data all place a counterparty in a category that warrants additional verification. None of these observations proves fraud, since legitimate new entrants exist in every market cycle, and the indicator's function is to allocate scrutiny.

The second component concerns credit standing verified through the factoring company. Because the factoring provider assumes payment risk on the invoices it purchases, its approval decision aggregates payment behavior information that an individual carrier cannot assemble at a reasonable cost. A declined or conditional approval, or a credit status that has declined since the last transaction with the same broker, carries weight beyond what any single carrier could establish on its own. This indicator anchors the documented procedure described in section 2, and the artifact it produces, a time-stamped screenshot filed in the transportation management system, makes the check auditable and prevents the control from decaying into an informal habit.

The third component draws on complaint and

payment dispute records available through regulatory channels and industry platforms. Recurring non-payment complaints, allegations of double brokering, and recent, dense complaint patterns carry more diagnostic weight than sparse historical entries. The fourth component concerns identity and contact data consistency, which compares the contact information presented during the transaction against the data on file in the registry for that counterparty. An email domain that departs from the registered corporate domain or resolves to a free mail service, phone numbers absent from the registry record, and an insurance certificate at odds with current filings all indicate that the party in the conversation may differ from the party in the record. Identity consistency checking is the primary registry-based defense against impersonation of a legitimate, well-rated broker, a scheme in which every other registry check passes because the identity being presented has a clean record.

The second family comprises indicators observable through conduct. Artificial time pressure opens the group, expressed through insistence on immediate commitment, discouragement of verification steps, and unusually accommodating terms offered to accelerate agreement. Urgency functions as an instrument of fraud because every verification step in the first family takes time, thereby making the compression of the timeline an attack on the vetting procedure itself.

Requests to reroute payment or communication constitute the second component and carry the highest

severity within the family. Such requests cover changes to remittance details, the movement of payments outside the established channel, and the migration of correspondence to personal email or messaging applications. These requests precede the extraction of funds or the severing of the audit trail, and the mechanism resembles business email compromise, where deception directed at an individual replaces technical exploitation as the vector of loss (Papathanasiou et al., 2023). The countermeasure is procedural. Any change to payment or contact details is verified through a separate, previously established channel before it is acted upon, a control that applies regardless of how routine the request appears.

The third component concerns inconsistency between the offered load and the counterparty's profile, including freight categories the broker has not handled, lanes at odds with its operating footprint, and rates materially above market without an explanation grounded in the load. Above-market pricing recurs in theft-oriented schemes, where the economic loss falls on the cargo, and the rate serves only to secure acceptance. Route and drop-off characteristics carry independent risk information, and quantitative work has shown that the interaction of route type, cargo value, and driver behavior shapes the probability of a theft incident (Liang

et al., 2022). The fourth component covers contact channel anomalies, meaning communication patterns inconsistent with a functioning brokerage operation, including a single individual answering every function, unavailability through the registered main line, and activity concentrated outside business hours. Each of these signals is weak in isolation but gains weight when combined with any indicator from the first family.

The behavioral family carries properties that invert those of the first. Its indicators resist reproduction, since the same exchange, when read by two dispatchers, may yield different assessments, and their evidentiary value depends on whether anyone recorded the observation while it was fresh. Their compensating strength lies in coverage, since conduct remains observable when records have been satisfied and when the record itself has been appropriated. A carrier that treats the behavioral family as a secondary layer discards the only signals available for the schemes that defeat verification, and the two families operate as complements, with a division of labor determined by what each can reach.

Table 1 maps both families onto the stages of the load lifecycle and records the artifact that evidences each check.

Table 1. Fraud indicators mapped to stages of the load lifecycle

Stage of the load lifecycle	Registry-based checks	Behavioural observation	Mandatory control point
Pre-booking	Operating authority age and registration history, complaint records, and identity consistency at first contact	Negotiation urgency, mismatch between route and load type	Lookup results recorded with the load file
Post booking, before release	Credit standing verified through the factoring company	Contact channel anomalies	Time-stamped screenshot uploaded into the TMS, tracking contact entered
Execution through delivery	Identity re-check on any change of details	Requests to reroute payment or communication	Out-of-band verification before any change is acted upon

The mapping expresses the classification's central practical claim. Each family of indicators has a stage at which it becomes actionable, and each stage carries a documented artifact that evidences performance of the check. A vetting procedure that produces artifacts can be audited, taught to new dispatchers, and enforced against

drift. A procedure resting on dispatcher intuition offers none of these properties, and its failures leave no record for the organization to learn from. Figure 2 presents the same mapping in process form, with the two families and the required artifact shown inside each stage.

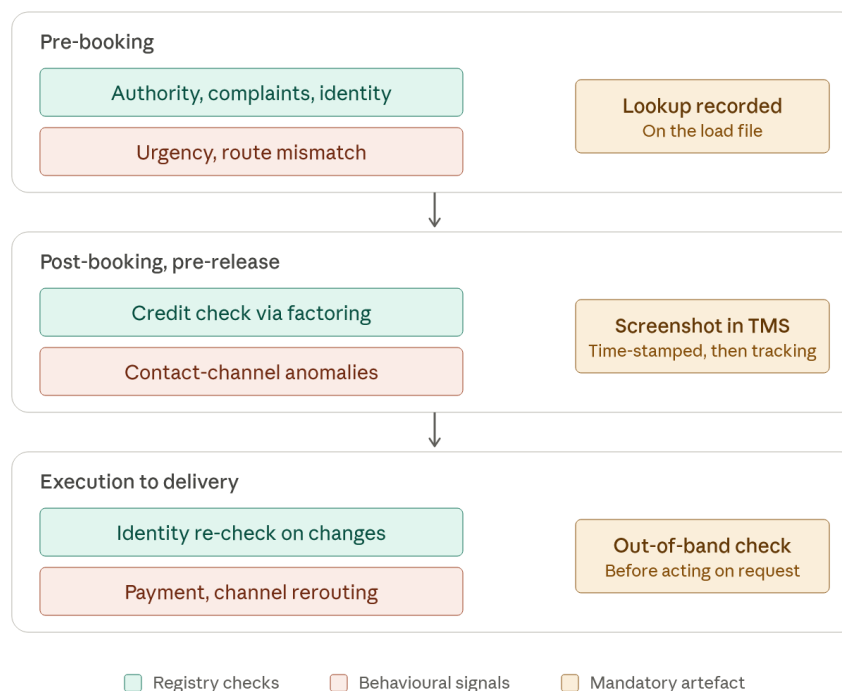


Fig. 2. Vetting checks and control points across the load lifecycle

Building on the classification, a structured risk-scoring framework is proposed as a construct awaiting implementation and validation. The framework accepts four groups of inputs that mirror the signal structure developed in Section 3. The first group covers payment history as aggregated through factoring approval and dispute records. The second covers operating authority age and registration behavior. The third covers

complaint records held on regulatory and industry platforms. The fourth covers behavioral red flags observed during the transaction. Each group contributes a weighted score, and the weights express a management judgment about the relative severity of signal types, subject to revision as case experience accumulates. Figure 3 sets out the resulting architecture.

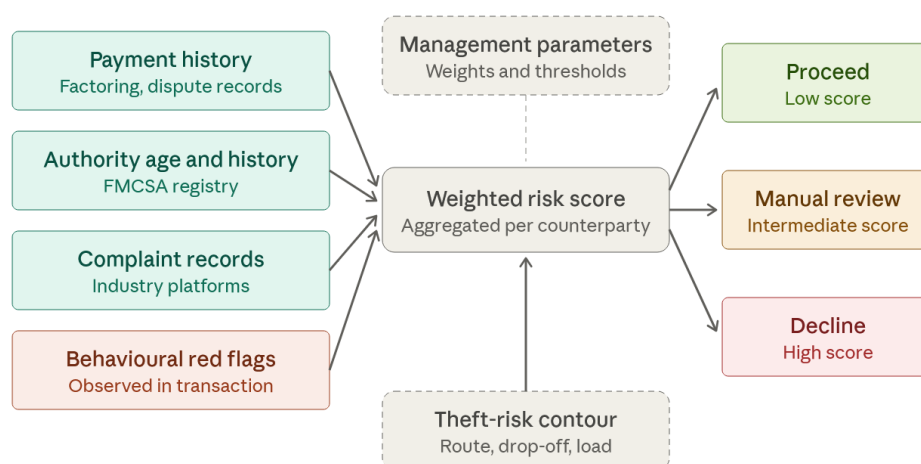


Fig. 3. Proposed risk scoring framework for counterparty vetting

The aggregate score maps to a three-level escalation decision, which results in proceeding with the load, referring the counterparty for manual review, or declining the transaction. Thresholds separating the levels operate as management parameters set to balance fraud exposure against the commercial cost of refusing legitimate freight. Weighted multicriteria evaluation of this kind has an established record in logistics provider

assessment, where criteria of unequal importance are combined into a single ranking used for a selection decision (Luyen & Thanh, 2022). The framework shifts that logic from provider selection to counterparty screening, with the difference that the decision concerns exposure to deception rather than service quality.

A related contour of the same construction addresses cargo theft exposure in place of counterparty fraud. It

evaluates the route, drop-off location, and load type against known theft-risk patterns and flags high-risk lanes and shipments for additional safeguards. Analytical work on road transportation has demonstrated that the theft risk can be estimated for a given product-route combination and that thresholds can be defined beyond which a shipment becomes attractive to organized groups (Cedillo-Campos et al., 2024). The theft contour and the counterparty score feed the same escalation decision, since a load that is safe on counterparty grounds may remain exposed on lane grounds.

Three design questions govern whether such a framework produces value in operation. The first concerns the calibration of weights. Assigning equal weight to the four signal groups would understate the severity of requests to reroute payment, which precede loss more directly than a complaint filed several years earlier, and would overstate the diagnostic value of authority age taken alone. Initial weights express severity judgments held by management and require revision as case outcomes accumulate. The second question concerns the treatment of the middle escalation band, since a framework that refers a large share of counterparties for manual review transfers cost onto the staff it was meant to assist. The width of that band determines the operating cost of the procedure and warrants monitoring as a performance measure in its own right. The third question concerns decay, since a counterparty screened at the time of booking may change in ways the score does not capture, thereby returning the analysis to the behavioral signals available during execution.

The intended effect of the framework is a shift in the timing of fraud handling. Discovery of loss after the fact gives way to identification, before commitment, of the transactions that warrant either refusal or hardened controls. Validation of the framework, meaning empirical establishment of weights and thresholds together with measurement of discrimination against realized fraud outcomes, remains outstanding and is treated in section 4 as the principal direction for further work.

4. Discussion

Three implications follow from the classification and its operational mapping. The first concerns the value of documentation over judgment. The credit verification

control described in section 2 owes its effectiveness to the artifact it produces: a screenshot filed in the transportation management system converts an act of diligence into evidence that can be reviewed after a loss and audited during ordinary operations. Firms that observe fraud in their networks vary in whether they intervene, and organizational conditions shape that response as much as knowledge of the underlying facts (DuHadway et al., 2026). A procedure that generates artifacts reduces the room for that variation, since it removes the option of quiet inaction at the level of the individual dispatcher.

The second implication concerns the symmetry of vetting. The dispatch procedure that anchors this classification requires accurate representation of the truck's location, realistic pickup and delivery times, and immediate communication of any delays. Read against the behavioral family, these requirements govern the same signals from the opposite direction, since a carrier that misrepresents its position or conceals a delay produces exactly the behavioral pattern that a broker screening for risk would flag. Vetting therefore operates in two directions at once, and a carrier managing its own observable conduct performs the mirror image of the screening it applies to counterparties. The behavioral family supplies a transaction-level account of how reliability and information sharing become visible to the other side, qualities through which trust in third-party logistics arrangements has been characterized (Valashiya & Luke, 2023).

The third implication concerns the limits of registry-based control. Two scheme types pass through a fully executed registry procedure. Post-verification double brokering occurs when a broker who is legitimate and creditworthy at the time of the check re-brokers the load afterward. No pre-booked registry signal exists for this sequence, so detection shifts toward execution-stage behavioral signals and tracking discipline. Impersonation of a verified counterparty is the case in which the identity presented has a clean record, so that every check against it passes. Defense here rests on identity-consistency comparison and out-of-band verification, both of which lie outside the registry record. These boundary conditions explain the two-family structure, since behavioral indicators constitute the only detection surface available to schemes that registry checks cannot structurally reach.

The practical output for the target audience is an ordered procedure with four properties. Checks occur at defined stages of the load lifecycle. Each check produces an artifact. Behavioral observation continues after registry checks conclude. Any request to change payment or contact details triggers verification via a separate channel before any action is taken. A carrier without analytical staff can adopt this sequence using tools already present in most operations, meaning a transportation management system capable of storing documents against a load and a factoring relationship that supplies credit decisions.

Adoption raises questions that the classification alone does not settle. Dispatchers are compensated and evaluated against revenue production, and a verification step that delays acceptance of a load competes with that objective at the moment of the decision. A procedure that relies on individual diligence erodes under commercial pressure unless the artifact requirement makes omission visible. Placing the credit check after booking and before release reflects this tension, as it preserves the speed of acceptance while retaining hard control before the carrier assumes physical exposure. Training carries a parallel requirement, since behavioral indicators are conveyed through worked examples rather than definitions, and a dispatcher who has never seen a rerouting request will not recognize the first one.

Four limitations qualify these results. The review is narrative in character, and its source coverage reflects the judgment of a single author working from a defined but incomplete search. The scoring framework remains a proposal without empirical weights, measured discrimination, or evidence of false-positive rates, so its commercial cost is unknown. The operational grounding derives from documented practice at one carrier, which provides illustration but falls short of evidence of effectiveness across firms of different sizes and market positions. Open data on the frequency of the schemes discussed here remains sparse, since victims underreport and industry estimates rest on samples of uncertain representativeness.

Further work follows from each limitation. Empirical validation of the weights and thresholds against realized fraud outcomes would establish whether the four signal groups carry the relative severity assumed here. A comparative study across carriers would test whether the artifact-based procedure withstands exposure to

different dispatch cultures and volumes. Integration of the classification with data already resident in transportation management systems would allow the behavioral family to be captured as structured records rather than dispatcher recollection, which is a precondition for any subsequent quantitative treatment.

5. Conclusion

Fraud in carrier and broker vetting resists a single countermeasure because its warning signs differ in kind. Some can be verified against records held independently of the counterparty, and others become visible through conduct during the transaction. Organizing the indicators along verifiability and the timing of the check produces a classification with an operational consequence, since each family acquires a stage of the load lifecycle at which it can be acted upon and an artifact that evidences the action. The classification converts scattered practitioner knowledge into an ordered procedure available to carriers and brokerages without analytical staff.

The risk-scoring framework proposed on this basis combines four groups of signals into a weighted assessment, yielding three escalation outcomes, with weights and thresholds serving as management parameters. The framework awaits construction and validation, and its value at present lies in the structure it imposes on the vetting decision. Two schemes fall outside the reach of registry verification: double brokering that occurs after the check, and impersonation of a counterparty whose record is clean. Both remain detectable through behavioral observation and verification conducted through a separate channel. The classification treats behavioral indicators as a necessary component of counterparty screening, with a detection surface that registry records cannot supply.

References

1. Cedillo-Campos, M. G., Flores-Franco, J. E., & Covarrubias, D. (2024). A physical internet-based analytic model for reducing the risk of cargo theft in road transportation. *Computers & Industrial Engineering*, 190, 110016. <https://doi.org/10.1016/j.cie.2024.110016>
2. DuHadway, S., Carnovale, S., & Kaufmann, L. (2026). Supply chain guardianship: Why some firms intervene when other firms commit fraud. *Journal of*

- Operations Management, 72(3), 439–461. <https://doi.org/10.1002/joom.70035>
3. DuHadway, S., Mena, C., & Ellram, L. M. (2022). Let the buyer beware: How network structure can enable (and prevent) supply chain fraud. *International Journal of Operations & Production Management*, 42(2), 125–150. <https://doi.org/10.1108/IJOPM-05-2021-0310>
4. He, C., Xu, Q., Xu, X., Kong, F., & Shen, F. (2025). Data-driven mechanisms for network freight platforms: An evolutionary game perspective. *PLOS ONE*, 20(6), e0319842. <https://doi.org/10.1371/journal.pone.0319842>
5. Liang, X., Fan, S., Lucy, J., & Yang, Z. (2022). Risk analysis of cargo theft from freight supply chains using a data-driven Bayesian network. *Reliability Engineering & System Safety*, 226, 108702. <https://doi.org/10.1016/j.ress.2022.108702>
6. Lokanan, M. E., & Maddhesia, V. (2025). Supply chain fraud prediction with machine learning and artificial intelligence. *International Journal of Production Research*, 63(1), 286–313. <https://doi.org/10.1080/00207543.2024.2361434>
7. Luyen, L. A., & Thanh, N. V. (2022). Logistics service provider evaluation and selection: Hybrid SERVQUAL–FAHP–TOPSIS model. *Processes*, 10(5), 1024. <https://doi.org/10.3390/pr10051024>
8. Papathanasiou, A., Lontos, G., Liagkou, V., & Glavas, E. (2023). Business email compromise (BEC) attacks: Threats, vulnerabilities and countermeasures—A perspective on the Greek landscape. *Journal of Cybersecurity and Privacy*, 3(3), 610–637. <https://doi.org/10.3390/jcp3030029>
9. Seify, M., Sepehri, M., Hosseinian-far, A., & Darvish, A. (2022). Fraud detection in supply chain with machine learning. *IFAC-PapersOnLine*, 55(10), 406–411. <https://doi.org/10.1016/j.ifacol.2022.09.427>
10. Urbaniak, M., Zimon, D., Madzik, P., & Šírová, E. (2022). Risk factors in the assessment of suppliers. *PLOS ONE*, 17(8), e0272157. <https://doi.org/10.1371/journal.pone.0272157>
11. Valashiya, M. C., & Luke, R. (2023). Enhancing supply chain information sharing with third party logistics service providers. *The International Journal of Logistics Management*, 34(6), 1523–1542. <https://doi.org/10.1108/IJLM-11-2021-052>