THE DOUBLE BROKER BOUNTY HUNTER'S FRAUD PREVENTION GUIDE

For Carriers, Dispatchers, and Brokers

This service brought to you by:

Vigilant Transportation Services LLC, home of the Double Broker Bounty Hunter (DBBH) program, designed to help carriers, brokers and dispatchers defend themselves against present day threats to the transportation industry relating to fraudulent actors. Contact dbbh.hotline@vigilanttransport.com for info.

John A. Cantera, Jr.
Jcantera@vigilanttransport.com
912-346-8456

Introduction

Vigilant Transportation Services (VTS) was started in 2021 as a dispatching service that specialized in the dispatching of box trucks, hot shots, and new authorities. During the course of 2022, we encountered a huge increase in the occurrences of double brokering in our operations. In September of 2022, we began keeping count of each double brokered load we defeated and the amount of money recovered for our clients. Between September 2022 and April 2023, we stopped 73 instances of double brokering, and recovered over $23,000 in funds that double brokers have tried to steal from our carriers. We began to refer to the recovered funds as “bounties”.

In December of 2022, we formally launched the Double Broker Bounty Hunter (DBBH) program. Our goal is to directly impact the revenue stream of illegal double brokers in an effort to drive them out of the trucking industry. As of December 2023, we have stopped 322 double brokered events, recovering over $90,000 in additional revenue for our customers.

In April of 2023, VTS was approached by the National Owner Operators Association (NOOA), and have been asked to head up the Department of Fraud Prevention (DFP) using the DBBH model to help any carrier that finds themselves unwillingly entangled in transportation fraud.

With this new visibility VTS and NOOA have developed a strategy for identifying and addressing scams that impact the transportation industry, and are also developing tools to help all legitimate actors in the industry defend themselves and their operations from the scammers.

This educational resource is by no means a final solution to dealing with fraud in the industry. Our intent is to regularly update this document and make it readily available as a resource for any industry stakeholder (shippers, carriers, dispatchers, or brokers) trying to improve the industry and reduce the impact of scammers in daily operations.

The fact of the matter is that the scammers are too deeply entrenched and are not going to go away. It is because stakeholders don’t understand the scams or how to beat them, or would rather not deal with it at all, that these scammers have grown to a magnitude where they have effectively driven down the industry to its breaking point. Only as a community can we succeed against fraudulent actors, restore rates to their true levels, and begin to prosper as we have before.

This document will identify the types of fraud active in the industry, and explain, if possible, how these scams are perpetrated. We will also identify best practices that help stakeholders defend their operations from these scams. We will also outline the successes and failures of current anti-fraud strategies, and make recommendations on how to tailor those tools to impose maximum challenges on scammers and minimum barriers to true industry stakeholders. This is a living document that will undergo regular updates and be reposted on the VTS websites as updated to ensure the most current information is readily available to stakeholders.

Active Forms of Fraud in the Transportation Industry

There are many forms of fraud in the industry, however our focus is on forms of fraud that have a sweeping impact on the industry as a whole. Here we will list and briefly describe these forms of fraud, and we will individually break them down to show how the fraud works. Finally we will list recommended countermeasures that specific stakeholders can use to mitigate the impacts of any fraud attempt.

This is the list of the most common forms of fraud in the industry today:

1. Double Brokering - the illegal practice of using a carrier authority to book loads from the broker of record for the explicit purpose of re-brokering those same loads under a separate brokering authority without the permission or knowledge of the broker of record. A more in-depth discussion of this form of fraud is contained within this document.

2. Cargo Theft – the illegal practice of diverting cargo from its intended destination to a location that is unknown to the cargo owner or broker of record, usually with the intent of the cargo to be sold on the black market. A more in-depth discussion of this form of fraud is contained within this document.

3. Carrier/Broker/Shipper Identity Theft – the illegal appropriation of a legitimate carrier, broker or even shipper identity and information for the purposes of booking cargo with the broker of record under an assumed name or booking a carrier to illegally haul cargo to deflect attention from the scammer's true intentions. A more in-depth discussion of this form of fraud is contained within this document.

4. Predatory Brokering – The legal, yet unethical, practice of a broker intentionally maximizing profit by forcing carriers to take unreasonably low rates for cargo when shippers are paying normal or elevated rates to the brokers. Further, predatory brokers are known for issuing freight guards and negative reviews against carriers as a form of retribution for any carrier that questions the actions of such brokers.

5. Dispatch Fraud – The legal yet unethical practice of forced dispatching (pushing carriers to accept unfair rates for their work or forcing carriers to accept loads to destinations that they do not want or cannot legally operate in. It also includes forcing carriers to violate Hours of Service (HOS) regulations while not accepting responsibility for any violations the carrier may be cited for as a result of improper dispatching.

6. Carrier Fraud – The illegal act of retribution against shippers, receivers or brokers for any action the carrier deems unfair. The carrier is not allowed to change the terms of a carrier/broker agreement as a form of retribution. Examples of this form of fraud is intentionally delaying delivery (holding a cargo hostage), intentional late delivery, false location reporting, and misrepresentation of the carrier's record.

What is Double Brokering?

Double Brokering is the illegal practice of using a carrier authority to book loads from the broker of record for the explicit purpose of re-brokering those same loads under a separate brokering authority without the permission or knowledge of the broker of record.

“Co-brokering” is an “industry accepted” practice, disguised as legal double brokerage, by which a broker of record authorizes another with a brokering authority to act as broker of record in finding a carrier for a given load. Such practices are authorized by contract, and are done with the full knowledge of all parties, and consent of the original broker of record. This is most often utilized when goods are being shipped internationally across the US northern or southern borders. Some domestic freight brokers utilize these agreements to provide additional brokering capacity when there is too much freight for one brokerage house to handle but they don’t want to expose this shortfall to their customers.

Why is Double Brokering Illegal?

There is a great deal of debate on what makes the practice illegal, and there are no specific laws that define the action of double brokering and denote penalties for violation of such laws. There are REGULATIONS in DOT policy that prohibits the practice. These regulations have been in place for nearly 20 years, and are focused on carriers re-brokering to other carriers. A perceived legal loophole exists that is being actively exploited by bad actors who are using carrier authorities to book loads but then are re-brokering the loads on a different broker authority. In general, 49 CFR and MAP-21 laws are interpreted to prohibit the act of double brokering as we have defined it here.

What makes this practice illegal under US criminal code is the element of FRAUD. The Double Broker (DB) is fraudulently promising to brokers of record that they are hauling the loads as legitimate carriers. The DBs then enter into broker/carrier agreements with real carriers to haul the load for either a reduced rate or an overly inflated rate. This is a fraud against carriers because the carrier is doing the work promised by the DB to the broker of record, and is not getting paid properly for the work, or possibly not getting paid at all for the work. The “profit” a DB gets from these loads are actually a theft of funds intended for the carrier, which is a crime under LARCENY statutes. Each event of double brokering involves two counts of fraud, and one count of larceny.

Though 49 CFR governing the transportation industry does not specifically identify this practice as a crime, criminal statutes covering the intent of the actions and the resulting theft from such actions are a crime under US law, punishable under federal statutes as the crime takes place across state lines.

How Does Double Brokering Work?

Because the practice of double brokering is punishable under US criminal code, there are far fewer instances of the practice occurring by US based brokers. Foreign actors make up a majority of all double brokering events that take place against US carriers. Foreign actors are

impervious to prosecution by the federal government and therefore have little reason to not engage in this practice. Understanding how the scam works leads us to clues on how to defeat the scam.

DBs operations can be simple or very sophisticated. There are individual DB operations managed by one or a handful of individuals where they have a ready pool of cash to operate independently, and ensure payments promised to carriers while collecting from brokers of record. There are also large scale DB rings that operate around a single financial arm that funnels all of the funds from the scam through a single entity, usually associated with international organized crime syndicates, and distributes the gains across the network.

Step 1: Obtain a Carrier Authority and a Broker Authority with FMCSA.

This is not an easy or cheap feat. Carriers know that to get a carrier authority, one must have a corporate entity, have ownership of at least one commercial vehicle (title or lease agreement), and insurance for that equipment in the name of the corporate entity. Setting up the organization is fairly cheap to do. Obtaining the title of a commercial vehicle is usually done by black marketeers selling titles to trucks that may or may not exist, usually in a scrap yard. The scammers then need to obtain insurance for the vehicle that meets the minimum requirements of FMCSA to be granted a carrier authority. An FMCSA certified mechanic is then needed to sign off on an inspection of the vehicle. The scammer then needs to maintain the insurance to keep the authority active for the duration of their operations. Because all of this is usually faked, these “carriers” usually only exist for up to one year. After one year, they will be called upon by state DOT for a new entrant audit, and the entity will suddenly cease to exist. When the “carrier” fails to report for their audit, their authority is revoked. The bulk of the scam is using this “carrier’ perpetrated for a period of 6-10 months on average, before the scammer needs to establish a new carrier authority that will allow them to continue DB operations.

The DBs also need to obtain a valid broker authority. To do this, they purchase a bond in accordance with FMCSA regulations, and must maintain that bond in order to obtain a broker authority. These bonds are intentionally expensive to discourage individuals who are not serious about being brokers from obtaining bonds.

These actions require startup capital. Where the funds to launch these DBs come from is still unclear, but once a DB is operational, they can generate large amounts of revenue in a very short period of time. If for any reason their authority is revoked, they can start the process over again without additional outlay of funds. The reality of this situation is what makes FMCSA’s only defense against such an enterprise, revocation of the authority, a meaningless weapon. The DBs can easily get a new authority and start over very quickly.

FMCSA is powerless to stop the application and awarding of these authorities. The Motor Carrier Act of 1980 removed all barriers to entry (ability to obtain a carrier or broker authority) to those who meet all of the basic requirements for such authorities.

Since April of 2023, DBs have employed IMPERSONATING valid carriers, brokers and even shippers for the purpose of Double Brokering and even Cargo Theft. It is important for all industry stakeholders to monitor their SAFER email addresses to watch for possible freight guards when a real stakeholder is victimized by ID theft. We are actively working to develop defensive countermeasures for the impersonation of stakeholders by scammers.

Step 2: Find Freight

Brokers of record sell their services to all kinds of shippers and consignees all over the country. They usually have a salesman or sales team whose only job is to get new clients and maintain relationships with current clients, much like any business. This is how brokers of record get freight to arrange transportation for. Many brokers will tell you that earning a shippers' business is very challenging work and usually is only successful based on established connections.

DBs go around this daunting process, and find freight by using their carrier authorities to book freight that belongs to another broker. Once the DB has the rate confirmation from the broker of record, the DB treats the load as if it is their load to broker out.

Step 3: Broker the Load to a Real Carrier

The DB made a promise to the broker of record to make sure the cargo is picked up and delivered by a specific day and time. The clock is counting down against the DB to find a real carrier to take the load. The DB uses their broker authority to then repost the load on a public load board, usually for 25%-50% less than what the DB is being paid by the broker of record. A real carrier then bids on the load, and books it with the DB, thinking the DB is the broker of record, and is issued a rate confirmation to memorialize the arrangement between the DB and the real carrier.

Step 4: Customer Service and Coordination

The DB must maintain a good relationship with the broker of record in order to be able to book more loads with them in the future. DBs want to send regular updates to the broker of record so that they appear to be responsive to the real brokers and build a positive rapport with them. To do this, the DBs then makes regular update requests of the real carrier. A broker of record usually only wants to know when the load is picked up and when it is delivered. Sometimes they are looking for intermediate updates, but they are usually infrequent. DBs, however, insist on constant updates. DBs want to know when the real carrier arrives, when loading is started, when loading is complete, regular ETA updates, etc.

Additionally, there is intense coordination of documentation on double brokered loads. The brokers of record do not usually ask for a copy of the BOL at pickup from the carrier. They don't ask for it because they usually provided it to the shipper. Under FMCSA rules for formatting BOLs, brokers are supposed to be listed as the 3rd party (or bill to party) on the BOL. The broker of record is also required to list their appointed carrier on the BOL. This does not always happen, and is not actively enforced by FMCSA or DOT. As a shortcut, some brokers list themselves as the carrier, and their customer as the 3rd party. This is not proper under the rules that govern BOLs but is also not enforced by authorities and is therefore generally accepted across the industry.

The DB wants a copy of the BOL at pickup as an insurance policy against the real carrier in case the real carrier gets wise to the scam. The DB will send the BOL after pickup to the broker of record as "proof" they (the DB) are in possession of the load. Brokers of record will believe them in the short term because they never asked for the BOL, and they can see it is the same BOL they provided the shipper in the first place.

Step 5: Cargo Delivery and Payment

The race is exceptionally desperate for the DB when the cargo is delivered. A broker of record usually asks for the POD to be provided within 24 hours of delivery. A DB wants the POD

immediately after delivery. The minute the real carrier gives POD to a DB, the DB will claim the load delivered to the broker of record, and file for immediate payment, usually by quick pay from the broker of record. Once the DB has the funds from the broker of record, then the DB has won the scam. The DB has a vested interest in keeping real carriers happy, so the DB will usually make good on their promise to the real carrier and pay as promised if the load was a load listed for less than what the DB listed that load for.

There are some instances where the DB will not pay the real carrier and keep all of the money for themselves. This usually happens when the DB has over inflated the rate, never intending to pay the final mile carrier so that they can profit 100% from the load. At this point, the DB cancels their bond, and tries to collect as many payments as they can before their authority is revoked. This is usually the time when real carriers are left without being paid for the load, and they do not have a bond that they can go after since the bond was cancelled. If the bond is still in place, there could be MILLIONS of dollars against the bond, and the resulting payout from the bond to carriers could be pennies on the dollar, or even less.

Another tactic designed to beat the real carrier is that if the scammer thinks that they are being pursued by the real carrier or an agent of the real carrier, they are attempting to get the POD from the RECEVIER instead of waiting for the carrier to send it. This is why it is so important to act as soon as you think a load may be impacted by a scammer.

In both cases, the DB has won, and has successfully taken carriers' money from them. Once the load is delivered, there is little a carrier can do to defeat the scam or recover funds without resorting to legal means or the use of debt collection agents who will act on double payment liability against the real broker and their customer for the load under 49 CFR 377 which states that the final mile carrier must be paid for the load.

The Impacts of the Scam

There are many direct and indirect impacts of the scam on carriers, brokers, and the industry as a whole. These impacts are the reason why all legitimate actors in the industry must unite against the DBs and drive them out.

The direct impact is the theft of funds from the real carriers. The broker of record determines the rate awarded to the carrier. This is based on the amount of money the broker's client pays, the brokers' target margin, and negotiation between the carrier and the broker. In the end, the rate confirmation issued by the broker of record is the official rate of that load. When a DB issues a rate confirmation for the same load to a carrier for less money, that "profit" for the DB is being directly stolen from the carrier. The carrier is unknowingly being taken for hundreds or even thousands of dollars on the load.

One indirect impact is the overall artificial deflation of rates in a given market. Rates in a region or market are determined by rate trends, fuel prices, availability of cargo, availability of carrier capacity, and other factors. When a DB publishes a load to the boards for less money, the average rate for the market begins to trend downward making sure that every load in the market gets cheaper to move, and carriers make less money in that market.

Another indirect impact is in perceived capacity. Every load a DB books with a broker of record artificially demonstrates an increase of capacity in the market, again, affecting overall market rates to carriers by reducing them. Remember, the "trucks" that DB's are using don't usually exist, thus there is an artificial increase of available capacity.

It is fair to say that with DBs skimming anywhere from 25%-50% of a load's revenue off the top, that rates across the industry have been artificially depressed by a minimum of 10% industry wide. DBs are one of the largest market influencers driving down rates. When fuel prices increase, logic dictates that rates should also increase. In the last few years, we have seen the opposite effect. DBs are a significant part of the economic equation and are driving rates in directions that are unexpected by those who study market impacts.

Aside from financial impacts, there are liability impacts as well. Most carrier cargo and liability policies are only in effect if the carrier is in legal possession of the cargo. Legal possession is defined as being listed as the carrier on the BOL. There are cases where insurance companies have denied carrier insurance claims in accidents or cargo damage because the carrier was not in legal possession of the cargo. An insurance company has a legal ability to deny a claim in such cases. If there is cargo damage or an accident, the liability falls on the carrier. If the carrier is not in legal possession, they will seek liability relief from the broker they booked the load with. Since the DB is not the broker of record, they can deny all knowledge of the load, and there is no official documentation tying the DB to the load. The rate confirmation from the DB to the real carrier can be called a forgery to deflect liability away from the DB, leaving the carrier with the full weight of liability of the damages, without coverage from insurance. This will lead to financial ruin for any small carrier, and big legal issues for a major carrier, especially if there was a death as a result of the accident.

For the broker of record, there is a business liability from the practice of double brokering. A broker's customer could view the broker as incompetent for allowing a DB to get control of a load, and the broker may lose their customer. The reality is that brokers do not usually know nor can know if their loads have been double brokered. Remember, the DB is using their carrier

authority to book the load in the first place and is regularly publishing updates to the broker of record. This keeps brokers of record from becoming suspicious of the matter. Unless the real carrier reaches out to the broker of record, the broker will usually never know their load has been double brokered. Knowing this is an issue, brokers of record have taken significant steps in screening carriers through a variety of compliance standards. These standards will catch some, but not all DB attempts.

We have observed a new evolution where scammers book loads using their own MCs or stolen MCs, and then instead of posting the load themselves, they would hire small or medium brokerages to re-broker the cargo. The danger is that the scammer gets to hide when the scam is taking place. The second legit broker doesn't know that they are illegally double brokering, and end up doing this for upwards of 30 days. The danger with this scam, is that the second broker pays the real carrier, expecting the shipper (scammer) to pay them inside of 30-60 days. The thing is that when the second broker sends the paperwork to the "shipper" for payment, the scammer send the paperwork to the real broker, and the scammer gets paid. The scammer does not pay the second broker at all. The second broker can wind up being out over $100k and will likely fail if they do not have a strong cash position.

There is also a variant of this scam where the scammer, acting as a shipper, creates a load out of thin air, and has a real broker organize transportation for this fake load. The scammer will require the carrier be approved by the "shipper". The catch is that the scammer has control of the "carrier" that is booked. There is no real cargo, so it is an exercise in paperwork. When the load "delivers", the scammer will submit forged BOLs as POD. The "carrier" is paid, and the "shipper" disappears after about 30 days. The resulting impact is the same as before with 6-figures worth of economic damage to the broker hired by the scammer.

How Does Cargo Theft Work?

Another indirect impact of the DB scam is how it leads to Cargo Theft. For high value cargos, or cargos of high importance, a scammer may use DB tactics to gain control of the load from the broker of record. Instead of providing constant updates to the broker of record, the scammer will break off all contact. Once the scammer has control, they can instead of issuing a RC to the intended destination, the scammer can issue their RC to take the cargo to another destination. In these cases, the scammer will tell the real carrier that the cargo is a "BLIND SHIPMENT".

Blind Shipments are used by brokers of record to legally consolidate freight for cheaper movement. The scammer, however, will convince the carrier that the load is a consolidation, and direct the carrier to dispose of the BOL received at the shipper and use a scammer provided BOL instead. The destination for stolen cargo is usually a pre-arranged warehouse rented by the scammers for the off-load or transload of the cargo. Once the cargo is dropped by the real carrier, the scammer may or may not make payment to the real carrier.

Once the broker of record determines that the cargo has not yet delivered as the scammer promised to the original intended destination, the broker of record will begin to search for the scammer carrier. With no paper trail to go from, the broker of record is forced to report the cargo stolen.

By this time, the scammer will have already transloaded the cargo delivered by the real carrier into another truck and the cargo will disappear into the black market. If the original BOL signed

by the real carrier is ever discovered by the broker of record through the shipper records, the real carrier will disclose where they dropped the cargo, but by then it could be too late.

The resulting damages are that the real carrier is now a suspect in a cargo heist, the broker of record is on the hook financially for the cargo, and the cargo owner must arrange for a new shipment likely delaying the project the cargo was intended to support.

What Role Does Identity Theft Play in Transportation Scams?

Identity theft is a fairly new phenomenon in the industry, beginning to be seen with more regularity in the Spring of 2023. At this time, cargo prices have been dropping at such a rapid rate that scammers were not "profiting" as much from DB scams as they were in 2022. Additionally, the exponential increase in DB activity in 2022 has led many brokers to change their carrier requirements to include a level of authority maturity that is unobtainable by most scammers since their "fleets" were fictitious as discussed in Step 1 above. In an attempt to reduce costs and dodge stricter broker requirements for authority maturity, scammers have abandoned their fake carriers, and are turning to stealing the identities of carriers that meet broker of record requirements.

Carriers who are most likely to have their identities stolen are small carriers and owner operators. Scammers are looking for the following traits when selecting an authority to steal:

1. Authorities with greater than six (6) months of maturity, and have documented roadside inspections. Since a recent broker anti-fraud defense is increasing the required maturity of a carrier authority to levels beyond where scammers can maintain their own authorities, scammers are combing FMCSA records to identify carriers with well-aged authorities.

2. Carriers at some point may have done a setup through any of the scammer's many brokerages, or with any brokerage that was part of a massive DB ring. DBs have been operating unchecked for over a decade. During that time, DB rings have been gathering data on carriers including insurance information, W9s, banking info for ACH deposits, and authority certificates. Most of this information is available from data storage sites on the dark web so that a scammer can cross reference an active carrier on an FMCSA search and find that carrier's information in the massive database the scammers have built of carrier information. Examples of this include the Kissflow and RIGZ platforms (also known as Crossroad Services). These are known DB setup platforms and the data can easily be sold off to fellow member DBs. There are also known DBs that have begun using RMIS and MyCarrierPackets for carrier setups, which usually give member brokers access to current information and documentation of carrier credentials. It is also conceivable that scammers may have an unknown method of getting up to date information like current insurance documents that we are unaware of.

3. Scammers appear to be targeting carriers who use public domain email platforms such as Gmail, Yahoo, and Hotmail for official email traffic. A scammer will create a very similar email address to the address listed in SAFER and fake that they are affiliated with the carrier. For example, the carrier's email may be XYZ@gmail.com. The scammer may use XYZ.Dispatch@gmail.com. It is easy for a less experienced broker to

assume that it is a valid company email address, and issue a load under the stolen ID MC.

A recent carrier ID Theft investigation revealed the following chain of events:

1. Carrier email was impersonated by scammer using a slight modification from the carrier's Gmail address.

2. Scammer used likely stollen DOT PIN for the carrier (likely stolen in FMCSA data breach in March of 2023) to issue an updated MCS-150 impersonating the carrier owner on the FMCSA SAFER site.

3. Scammer successfully changed carrier official email and phone number on SAFER to reflect those that the scammer has sole control of.

4. When the changes went live in SAFER (usually 24 hours later), the scammer contacted RMIS and AssureAssist to report a change to the carrier company contact info so that any verification codes or phone calls would only go to the email address the scammer set up.

5. Scammer began booking loads using brokers that subscribe to RMIS and MyCarrierPackets. Since all company docs are stored in these systems, the scammer does not need to produce them to complete setups.

6. Once loads are booked, the scammer can double broker the loads or modify broker rate confirmations for the purpose of stealing the cargo.

<u>These are the steps to restore control of your carrier authority:</u>

1. Notify appropriate authorities. Contact Offices of Inspectors General at the Department of Transportation (State and Federal). Advise them that the authority has been compromised by scammers. Ask them for current guidance for damage control measures.

2. File an updated MCS-150. Be sure to update your email and phone numbers to restore control of your authority to you. This can take up 48-72 hours to go into effect.

3. Contact your insurance provider. Have them place a fraud alert on your account. Since the insurance company does not refer to SAFER contacts to verify information, this will prevent unauthorized parties from obtaining COIs, including RMIS and AssureAssist. Ask them to verify the most recent COIs issued. Make sure that the COIs match recent approved broker setups. If you use a dispatch service, ask your dispatcher to conference in with the insurance company because they will better know what recent setups they have done on the carrier's behalf.

4. Contact RMIS and AssureAssist. These agencies can tell you what brokerages have recent activity on your account. If you have not hauled loads for those brokers, this

gives you a list of brokers that may have issued a load to the scammer in your name. Do this daily until the SAFER information is corrected.

5. Contact all brokers who are suspected to be victims of the scammer. Speak to broker dispatch and explain the situation. Ask them if they have any active loads under your MC. If they do, and you know they are not currently being hauled by your company, have the brokers mark the load as fraudulent activity. The broker will take the necessary steps to secure the cargo and identify the carrier at delivery, or report the cargo stolen if it never arrives at its intended destination. If you report this before the cargo is set to deliver, you are likely not to be held liable for any cargo issues on these loads.

6. Monitor company email very closely. If a freight guard is posted for fraudulent activity, you have only 72 hrs to respond. Before publishing a response in the Carrier411 response tool, call the broker and explain the situation. The broker is most likely to remove the freight guard. If they do not, contact the DBBH Hotline and we will fix that situation for you.

7. Watch email for rate confirmations and setup packages that were not requested. Contact the associated brokers immediately so that they are informed about the situation and can cancel the load on the scammer and protect the cargo from potential theft or double brokering.

8. When your SAFER information is updated, contact RMIS and AssureAssist and change back all contact information to match SAFER.

9. If you have not yet done so, get a company specific email domain, and update SAFER email address to one with your new domain name. This will reduce the odds that you will be targeted again by scammers for ID theft.

10. When it is clear that the danger is past, request a new PIN from FMCSA by mail. Keep this in a secure location when received.

We know that broker authorities are being stolen as well. The large brokers identities are stolen very easily as there are many copies of their rate cons floating around on the internet. This makes the rate cons very readily available, and therefore easy to access and change the information on while still looking like a legit rate con. These entities are so well known that people rarely look at the rate con for detailed content which makes it easy to get the rate con past an unsuspecting carrier, shipper, or receiver. For small brokers, stealing the identity could come after the scammer used a stolen carrier ID to book with. This will give the scammer a rate confirmation that they can then forge using photoshop or other image graphics tools. The scammer can then change the destination details using the format of the original broker of record, and direct a real carrier to deliver the cargo to a location that is unknown to the broker of record. Once the broker figures out the cargo never delivered to its intended destination, the broker will try to reach the dispatcher for the stolen carrier authority. Not getting a response from the dispatch email, they will reach out to the owners of the carrier authority using information from the Secretary of State or an official authority site such as the FMCSA SAFER. Other sites such as Carrier411 and SaferWatch pull the same info from the FMCSA database

and may be used as well. The answering carrier will usually have no idea what the broker of record is talking about. This begins the frantic calls to the police and FBI in a vain attempt to locate and recover the stolen cargo.

As we have described these individual scams, one can see how they are often tied together as elements of each scam are needed to pull off the larger scams. It is now appropriate to get into defensive strategies for both real carriers and real brokers of record to employ that can help mitigate exposure to these scams and allow both to work in concert with each other to help them to facilitate corrective actions after the scam has taken place or during the scams actual movement.

What are some Defense Strategies to help Defeat the Scammers?

The scammers hold all the cards, and are in control of the game. They know who the real broker of record is, and they know who the real carrier is, and they will do anything to prevent one from discovering the other. The smoke and mirrors a DB uses to keep both the carriers and brokers in the dark must be maintained even after load completion, so that the DB can continue to book more loads with real brokers and sell them to real carriers. In cases of cargo theft, the smoke screen must only be maintained for about 24 hours after cargo delivery to give the scammer time to get away with the cargo.

FMCSA and DOT are powerless to stop the DBs from doing their work. Federal agencies have tried to make it more difficult to obtain authorities as a carrier and as a broker over the last 20 years. The only real weapon FMCSA has in policing brokers and carriers is revocation of the authority. In theory, FMCSA and DOT have the power to better screen new authority applications by forcing a physical visit to the new applicant's business address. If the new applicant is nowhere to be found or the address is a virtual address, FMCSA has the ability to deny the authority. FMCSA and DOT do not dedicate any resources to this purpose so if an applicant appears to meet the requirements on paper, the authority is granted in accordance with the Motor Carrier Act of 1980. Once granted, they wash their hands of the matter until there are so many reports of fraud against a single authority that they are compelled to act. It is not public information as to how many reports of fraud must appear before FMCSA and DOT before they act.

As discussed before, cost of authority establishment is not a viable deterrent to DB organizations. DBs can easily get the funds needed to establish new organizations and authorities between the time that FMCSA puts them on notice of revocation, and when the revocation actually takes place.

The only real weapon that exists against scammers is to block their cash flow. DBs exist because there are loopholes in the transportation industry that allow them easy access. Once the carrier and broker authorities are established, the DBs are free to operate at will, usually for months at a time, before constant reports to FMCSA force regulators to revoke the DB's authority. Stopping the scam while in progress is the single best way to impact the cash flow of the DB. To do this effectively, a carrier must discover who the broker of record really is and convince the broker of record that they are the real carriers and have possession of the cargo.

Only then can a broker of record, provided with proof of fraudulent activity, cut out the scammers and issue a new rate confirmation with the real carrier.

It is critical to reiterate that the BEST time to attempt to expose the DB and any other fraudulent actor is when the real carrier has the cargo in their truck. If the DB is exposed to the broker of record before the truck is loaded, the broker of record can cancel the load. This is an elegant solution for the broker, but it leaves the carrier without a load, and certainly no TONU. If it is exposed after delivery, the broker of record may have already paid the DB, and the real carrier is at the mercy of the DB to be paid, or must employ legal forms of representation such as an attorney or a debt collector. Of course, the broker of record will flag future loads that the DB attempts to book, but the real carrier will only be quickly paid by the broker of record for exposing the DB if the load is in their truck, or before POD is given to the DB.

Signs that Your Load Is Double Brokered or Scammed

There are many clues that a carrier can observe that should lead them to suspect a load has been double brokered or scammed. If any of these clues are encountered, the carrier must act immediately to prevent any money from being stolen from them by the DBs, or to return control of the cargo to the broker of record before the cargo is stolen. Below is a list of signs that a load has been double brokered or scammed. After the list, we will break down each of the signs and what they mean. No one sign proves double brokering or scamming, but it should arouse suspicion.

- Load is not factorable
- Broker setup through Kissflow or RIGZ platforms (also known as Crossroad Services)
- Broker explicitly forbids carrier from contacting shipper or receiver.
- Broker explicitly directs carrier to check-in for pickup as a different carrier.
- Rate confirmation is exceptionally vague on cargo details.
- Broker is aggressive in tone and frequency in requesting updates.
- Broker demands a copy of BOL immediately upon pickup and delivery.
- Broker does not appear to have a grasp on US geography.
- English is not the broker's native language, or operates outside the US.
- Irregularities on the BOL.
- Rate for the cargo is abnormally high or abnormally low compared to market rates.

Let's break each of these down and explain why it is a sign of potential scam.

<u>Not Factorable –</u>

Most factoring companies screen brokers under certain criteria to factor their loads. They need to be certain that the broker will pay the invoice in a timely manner. Brokers must meet credit score and days to pay criteria to be factorable. Additionally, and this is the most important clue, the broker must have been in business for a certain amount of time before they can be considered for factoring. If a broker has been in business for less than a year, but has an excellent credit rating, they are most likely a new broker and trying to establish themselves. On the other hand, if the broker has been in business for a long time, had a good credit score and is still not factorable, it is often due to claims of double brokering in their history. This is usually a strong first indication that the load is being double brokered.

Setup Through Kissflow or RIGZ Platforms –

The larger DB rings centralize data flow in the production of the scam. Gathering data on real carriers gives DBs an edge and gives the appearance of legitimacy. It can also open the door to scammers using the collected data to steal the identities of carriers later down the line.

Kissflow setups are a standardization tool, that functions similar to MyCarrierPackets or RMIS, but have no data collection point to list your factoring company as a payment option. They only show quick pay and 30-day checks as payment options. At the end of the process, it will let you upload a NOA, but there is no option for factoring on the form.

RIGZ takes the scam to a new level. All brokers affiliated with RIGZ use the RIGZ financial group, Crossroad Services, to run all financial transactions. RIGZ has the appearance of a legitimate platform, with knowledgeable support staff that answers the phone when you call. They do not screen affiliated brokers and allow for these brokers to operate however they want as long as RIGZ gets their cut. Use of these platforms have a very high probability of a load being double brokered.

Directed No Contact to Shipper or Receiver –

There are two issues here. First, no broker agreement forbids contact with the shipper or receiver. Broker agreements protect brokers from back-solicitation (carriers trying to leverage knowledge of who a broker's customer is for the purpose of seeking direct work from the customer). A broker can sue a carrier under this agreement provision if the carrier was trying to steal the customer. Second, the broker cannot abridge a carrier's First Amendment rights. A carrier can talk to any shipper or receiver they want to, and is encouraged to do so when it is to support the efficient loading and unloading of the cargo. Yes, the broker would prefer that carriers not bother their customers, but brokers understand the difference between back-solicitation and effective customer service. This is where the mantra of TRUST BUT VERIFY comes into play. Again, broker may not like any interaction between the carrier and their customer, but if that interaction does no damage the broker's relationship with the customer, there is usually no issue. Our hunters are trained so that if they need to contact a shipper or receiver to learn the identity of a broker, that they are to announce themselves, the nature of our investigation, and advise the customer that the level of sophistication of the scammers is so high that most brokers will never know that the load has been scammed. Under no circumstances do our hunters attempt to sell services of any kind to a shipper or receiver. No contact orders tend to indicate a strong probability of double brokering.

Directed to Check In as a Different Carrier –

Sometime a legitimate broker will ask the carrier to check in as the Broker's name, as a contractor of that broker. If the broker is an agent of a larger brokerage, the broker may want you to check in as a contractor of the agent using the agent's name or the parent brokerage's name. Such directions are not in accordance with FMCSA standards on BOLs, but it is not necessarily a sign of double brokering. If the broker asks you to check in as an entity that is not the broker or a parent brokerage, and is not the identity of the real carrier, then you must be

very suspicious. In such cases, there is a very high probability the load has been double brokered.

Broker Aggression in Tone and Frequency of Updates –

DBs know that to pull off the scam, they must be communicating updates regularly with brokers of record in order to build trust and to increase the chance of getting more loads from the broker of record in the future. There are all kinds of personalities working as legitimate brokers, and a broker having a bad day may be verbally aggressive toward a driver. That is not the indicator we are talking about. Brokers of record usually ask for an ETA for pickup and delivery, and a heads up when you have completed loading or unloading. Only on special loads that are high visibility will a broker be more frequent with update requests.

DBs make constant update requests. If you find that a broker is calling a driver every 10 min for an update while approaching pickup or delivery, you should be concerned of possible double brokering. In such cases there is a moderate probability the load is double brokered.

Broker Demands Copy of BOL Immediately After Pickup and Delivery –

Brokers of record are the ones who usually develop the BOL and send them to the shipper. Unless they have no trust in the carrier, they will not ask for a copy of the BOL on pickup. Most rate confirmations also give the carrier 24 hours to submit POD after delivery. Most brokers will not ask for the POD on delivery unless it is an expedited load for them.

DBs want that paperwork immediately to wave around as proof to the broker of record that they are in possession of the load after pickup. The want the POD immediately after delivery so they can invoice the broker and get paid as quickly as they can. If you are asked for a copy of the BOL after pickup, there is a strong probability the load is double brokered.

Broker Tends to Not Know US Geography –

Experienced drivers and dispatchers know how far it is from point to point inside the US. Most Americans will not know the location of an obscure town in the middle of nowhere, however most know it's a long distance between certain major cities. They know that New York and Miami are a very significant distance from each other. If a broker seems to think you can do a same day delivery between Boston and Chicago in just a couple of hours, there is clearly something wrong there. Such cases have a significant chance of being double brokered depending on how ridiculously wrong the broker is in terms of geography knowledge.

English is not the Broker's Native Language –

This is a controversial sign, however the active DB rings are mostly overseas in Eastern Europe, Asia, and India, or natives of the aforementioned regions. There are legitimate brokers overseas (military spouses, retired transportation professionals, etc) who operate overseas, legally, and adhere to the standards of conduct befitting a professional in our industry. Foreign accents do not alone cause concern for suspicion of double brokering, but when combined with

any of the other signs, there could be a problem worth investigating. Such cases are a moderate chance of double brokering when no other signs are immediately present.

Irregularities on the BOL –

As previously discussed, FMCSA standards on BOLs (not enforced) require the BOL to list the broker of record as the 3rd Party (or Bill To party), while the actual carrier should be listed on the BOL as well. If this not the case on your BOL, then there is certainly room for suspicion. That suspicion should be dramatically increased if you don't recognize the organization listed as the 3rd party or carrier, and especially if you know the third party listed is another major brokerage. In such instances you have a high probability of double brokering.

Rate for the Cargo is Abnormally Low or Abnormally High –

For double brokering scams, this is an indicator of the type of DB scam being employed. If the rate appears to be abnormally low, this is indicative of the "skim off the top scam" where the DB is likely taking a percentage of the total value of the load off the top, and effectively stealing that percentage from the real carrier. The INDUSTRY STANDARD in dealing with this type of scam is for the real carrier to provide proof of the scam to the broker of record (BOL and scammer RC), and the broker of record will respond with a new RC cutting out the scammer, and giving the real carrier the full amount that was offered to the scammer. This usually means a net gain for carrier revenue, and zero sum gain for the broker of record, but the broker of record regains control of the cargo which has its own value in protecting liability.

If the scam rate is higher than normal, then this is indicative of the "too good to be true scam". This scam is used when the scammer has no intention of paying the carrier in any way, and offers any amount they need to in order to ensure they find a carrier to haul the load. They only need to maintain the illusion long enough get paid by the broker of record, and then they disappear leaving the real carrier holding the bag without any compensation whatsoever. If it is caught before the load delivers, the carrier will be in a shock as they will only be entitled to whatever the broker of record agreed to the scammer for compensation. If the scammer promises the real carrier $2000, and the load only really paid $1000, then the carrier will only be paid $1000 by the broker.

It is important for the real carrier to understand what the market rate is in order to determine what type of scam they may be opening themselves up to. When there is a significant deviation from the normal market rate, usually greater or less than 20%, then the load has a significant probability of being double brokered.

How to Confirm Double Brokering

When trying to beat a possible double broker, you must do two things: First you must act when the cargo is in your truck. Second, you must keep the DB in the dark about your suspicions.

The BOL is the key to determining if a load is double brokered. The first task is to determine the broker of record. Sometimes it is easy. If you recognize the listed 3rd party or carrier as a known broker, you can start by reaching out to them and asking about the load. The BOL number or a reference number on the BOL will allow a broker to trace the load and determine if it is actually their load or not. If not, and there are no more clues on the BOL, then we contact the shipper and/or receiver. If we can determine who paid for the load, we can ask who they used to broker the load.

Once you determine who the broker of record is, you may be requested by the broker to provide load documents including the BOL and rate confirmation. The broker will then do their due diligence regarding the load. They will most likely contact the carrier they booked to see if they have the load, try to verify from the shipper who actually picked up the load, and a host of other compliance checks. Once the broker is satisfied that the real carrier has the load and not the DB, then the broker will run their setup with the real carrier (if not already set up) and then issue a new rate confirmation.

It is very important that the DB is not made aware of any suspicions. Until the real carrier has the rate confirmation from the broker of record, we cannot consider the DB busted. This process takes time and effort as well as regular communication with the real broker.

In addition, the carrier must keep up appearances with the DBs long as possible. Give the usual updates, play nice, but whatever you do, DO NOT GIVE THE POD TO THE DB. Once the DB is alerted to the fact that they have been exposed, the real carrier will be subject to all kinds of harassment. They will verbally assault the carrier. They will threaten the carrier with calls to the police and declare the cargo stolen. They may even resort to death threats. THEY CAN'T DO A DAMN THING TO THE CARRIER ONCE THEY ARE EXPOSED. Calling the police will only alert authorities to the fraud aspect of the case and it will backfire because the carrier has the BOL and the cargo. Verbal assaults are designed to scare and fluster a carrier. Ignore them. Though terroristic threatening is a serious crime, these DBs are overseas and would not dare to set foot on US soil. The threats are empty and should be ignored. In fact, when our team is threatened in such ways, we usually laugh at the DBs.

Additional Defenses Against DBs

DBs, like other scam artists, are always working to find innovative ways to appear more legitimate and eliminate suspicion while at the same time reinforcing their procedures to ensure the scam is successful. For every double brokered load that is intercepted, there are a dozen that are not. There are a couple of recommendations a recent working group of brokers and dispatchers have come up with to help carriers and brokers defend themselves.

Don't be afraid to book loads that are not factorable.

DBs operate by minimizing the number of real individuals they need to involve. Getting qualified for factoring is a test that has a high risk of exposing the DB. Most DBs would rather use Quick Pay with the broker of record rather than factor the load. If they factor the load under their carrier authority, the broker of record has 30 days to issue final payment to the factoring company. Usually in that 30 days, the broker of record will detect a pattern of a sloppy DB, and freeze payments to the MC. Using Quick Pay with the broker of record allows them to get paid quickly and the accounting dept of the broker of record then only has a couple of days to identify a fraudulent pattern. The DB also offers Quick Pay to the real carrier, since once the real carrier is paid, there is no reason for the real carrier to act on any suspicions.

As long as the carrier is smart enough to act when they still have the cargo in their truck, then the DB is immediately exposed and the real carrier can be paid directly by the broker of record.

Some will argue that the broker agreement and rate confirmation from a double broker is legally binding. Any agreement entered into where at least one party has fraudulent intent is null and void by legal precedent and is a matter of settled law. The DB cannot take legal action against the real carrier nor against the broker of record as their intent was fraudulent from the start. This is why once a broker of record researches a real carrier's double brokering claim against a DB, the real carrier is rewarded with a rate confirmation for the original value of the load that was promised to the DB.

Once the DB is exposed, it is most likely that the broker of record is factorable, and then there is little reason to avoid the load.

It is admirable for a real carrier to strictly honor their agreements, but if they do not act against the DB and seek out the broker of record, the DB is still stealing money from the real carrier. There is no honor among thieves, and the DB will not be so accommodating to an over-trusting carrier that they just stole from. In fact, they will call that carrier repeatedly to offer them loads because they know they can successfully steal from them.

If a Load is Too Good To Be True, Stay Away!

If you have been in the industry for any length of time, you have a decent idea of what the market rate is for a load. If you are being offered a rate that is significantly higher than market rate, and there is no aspect of the load that justifies it (multiple stops, overweight or over dimension, driver load or unload) then stay away from the load. If other indications of double brokering are present, it is likely a load that is a trap set by a DB to lure in a carrier with the promise of a great rate, but then not pay the carrier at all. If the DB is exposed during such loads, the real carrier needs to be ready to find out that the broker of record is really paying less than the DB offered. The real carrier has no choice but to accept the original rate of the load, even if it means losing thousands of dollars in promised income by the DB. Brokers of record are not obligated to pay what a DB promises. If the DB is not exposed until after the real carrier realizes they are not getting paid, the broker and shipper have an obligation to see that the final mile carrier is paid. This is called double payment liability. Case law and the support of 49 CFR 377 requires the final mile carrier to be paid for the load. Generally, we reach out to the original broker to give them a chance to indemnify their customers. This helps protect their relationship

with the customer, and as such, those brokers may pay the delivering carrier a settlement but they are not legally liable. The best thing to do in these cases is to not book the load, and if you do, expose the DB while the load is still in the truck to ensure the carrier will at least get paid something for their trouble. If all else fails, and the carrier is not paid over a scammed load, the carrier has 18 months to present their claim to the real broker of record to obtain payment for interstate loads. Intrastate loads have larger statutes of limitation but vary from state to state.

Carriers Should Carry a Stamp for BOLs, and Sign and Print Their Names on BOLs.

Carriers are required by FMCSA BOL standards to sign the BOLs. Many do not. Brokers of record who review invoices tend to look to see if the carrier signature matches the name of the driver reported when the load was originally booked. If there is no carrier signature, there is no way to match the driver to the load, thus no way to suspect that the carrier was a victim of double brokering. If a carrier (driver) signs and prints their name on the BOL, the broker of record can quickly notice that the driver's name does not match the name provided when booking. This gives the broker of record a reason to withhold payment until they can resolve who the real carrier is.

One way to help brokers of record and lead them to the real carrier is if the driver for the real carrier uses a stamp when signing the BOL. The driver should sign and print their name, and then use the stamp, which should have the carrier's MC number and carrier company name. If such a mark were on a BOL that a broker of record found to be suspicious, the broker of record can easily identify who the real carrier is and make sure they are the ones to get paid for the load.

The investment of a stamp for the driver to use on the BOL is a security measure to protect carriers and is a small price to pay to ensure they are credited with every load they haul. Carriers could even issue their drivers stamps that include the driver's name, so that the driver only needs to stamp the BOL and then sign it, since their name is legible from the stamp. This one recommendation has overwhelming support and can quickly expose DBs before they are paid, assuming the brokers are watching for this.

Carriers and Brokers Should Have Their Own Email Domains.

As discussed before, brokers and carriers using GMAIL or other public domain email addresses can be susceptible to having their identity stolen. By registering for a domain that matches your company name or is similar, you can make it much harder for a scammer to impersonate you via email. It is critical however that you alert FMCSA of any change to your contact information by submitting an updated MCS-150. You need for your information to match between the carrier vetting sources (like Carrier 411 and Carrier Watch who draw directly from the FMCSA database) and your advertised business information so that customers can contact you when needed, and brokers can verify dispatchers that work for you. This one suggestion can thwart current identity theft trends among carriers. It helps for brokers also, but your customers and carriers need to know that any information that comes from any domain other than your business domain is at risk of being fraudulent and should require the recipient of a possible fictitious communication to reach out to the alleged sender to verify the authenticity of the message.

Get Help If You Don't Have the Time to Fight Scammers On Your Own

We have laid out the way to fight these scammers, but the process takes time and patience. Carriers need to do research, make calls, and send emails to try to discover who the broker of record is, and then to prove they have the cargo. This process can take as little as 30 minutes of effort, or as much as a few hours of effort and even more hours of waiting on responses.

The DOUBLE BROKER BOUNTY HUNTER is a service sponsored by VTS, designed to help carriers and dispatchers who lack the time to research these loads on their own. Our staff is trained to identify double brokered loads in just a quick review of the load documentation. We have a database of cooperating brokers who advise tell-tale markers as to when loads belong to their brokerages, giving us an edge on quickly identifying the broker of record, and then alerting them to the matter. Our program is recognized in the carrier compliance groups with several dozen major brokerage houses and our requests for resolution are usually pushed to the front of the line among carrier issues.

To take advantage of this service, simply email DBBH.hotline@vigilanttransport.com

We will send you a Service Agreement to protect your business and limit distribution of load documents to only necessary parties on your behalf. We charge $50.00 to fund the investigation. We would temporarily serve as your appointed dispatcher to speak on your behalf for the duration of the case. The carrier will then be asked to send us their load documents, and one of our Hunters will work the case. Once we identify the broker of record, we will reach out to them and inform them of the case. We may need to setup the carrier to ensure a new rate confirmation is issued, so we may ask for a copy of the carrier's setup documents for this purpose. Once the difference between the DB rate confirmation and the broker of record confirmation is known, the carrier will be charged a service fee of 25% of the increase in revenue, and the investigation fee of $50.00 is waived.

Example: If the DB rate confirmation was $1,500, and the broker of record rate confirmation is $2,000 (an increase of $500), we will charge the carrier 25% of the increase ($125.00) for the service.

Once the fee is paid (we accept payments online by credit card and electronic bank drafts), we will turn over the new rate confirmation to the carrier and close the case file. With our program, the real carrier only needs to send a couple of emails to get the money they are supposed to receive and get it for very little effort.

If you do not wish to pay for the service, the ways to fight the DBs are in this document. We don't care if you use the service or not. We really care about the community standing up together to fight scammers. As long as there are carriers who are willing to be victims, the scammers will continue to prey on them.

Stay informed on new trends in transportation fraud by subscribing to our weekly podcast, The DBBH's Stop the Scam!. It airs live every Monday at 5pm central time on our YouTube channel, @DoubleBrokerBountyHunters.

This version was published on 3/28/24.